JET INFO

SINCE 1995

№ 1-2 (325-326) 2026 JETINFO.RU

АНТИХРУПКОСТЬ В ИТ

Зоны доступности

IT-архитектура непрерывности без единого центра: разбор по слоям

Поиск «черных лебедей»

Как мы сегодня пытаемся предсказать киберкатастрофы

Отказ от инженерных иллюзий

Манифест ИТ-инфраструктуры без стабильности — свобода вместо догм

Андрей Янкин,

директор дирекции информационной безопасности компании «Инфосистемы Джет»

Хорошая служба ИТ набила руку в решении типовых, каждодневных проблем. Работы ведутся четко, роли и планы прописаны заранее, значения SLA радуют глаз. Но порой случаются события катастрофического масштаба. Раньше для ИТ-инфраструктуры крупной компании это могли быть пожары, наводнения, беспорядки и отключения света. Сейчас к ним прибавились удары беспилотников, эпидемии и разрушительные хакерские атаки. Стремительный уход с рынка ключевых вендоров и отключение международных сервисов также стали для многих громом среди ясного неба. Каждое из таких бедствий казалось маловероятным, однако всего за несколько лет появилось немало компаний, которые столкнулись сразу со всем вышеперечисленным.

Нассим Талеб назвал такие события, труднопрогнозируемые и редкие, но имеющие серьезные последствия, «черными лебедями». Даже если что-то из череды катастроф можно было предсказать, на деле девять из десяти даже крупных компаний не делали ничего, чтобы к ним подготовиться. А значит, на мой взгляд, такие события можно смело отнести к «черным лебедям».

Лебеди эти прилетают к нам с невиданной ранее частотой, и логично предположить, что в ближайшем будущем нас ждут новые потрясения. Можно изучать прогнозы футурологов, а можно и признать невозможность предсказания новых катастроф. Как бы то ни было, жизненно необходимо так изменить подходы к построению ИТ-инфраструктуры, чтобы в ее ДНК была заложена способность переживать сокрушительные удары и быстро восстанавливаться после них.

Нассим Талеб ввел также понятие антихрупкости как ответ на появление «черных лебедей». Антихрупкость — это не неуязвимость. Антихрупкая система готова не только перенести катастрофическое воздействие с приемлемым для себя вредом, но и стать лучше на основе полученного опыта.

Антихрупкость невозможна без избыточности, постоянного анализа негативного опыта ***(лучше бы чужого, но все чаще своего)***, без регулярных тренировок на случай различных катастроф, без непрерывных доработок и изменений для адаптации к постоянно меняющимся условиям, без готовности принять ущерб и умения отделять зерна от плевел, чтобы спасти бизнес, а не ИТ или свою репутацию. Для построения антихрупкой ИТ-инфраструктуры требуется не только сменить подходы к техническим решениям и скорректировать процессы. Необходимо поменять и способ мышления. Авария должна восприниматься как что-то неизбежное и как возможность стать лучше. Надо переходить от парадигмы «если нас взломают» к «когда нас взломают», от «кто был виноват?» к «что мы можем теперь улучшить?».

Я сам отвечаю в том числе за киберустойчивость родной компании. И понимаю, что сделать все это куда сложнее, чем написать. А от упражнения «когда нас взломают» каждый раз по спине пробегает неприятный холодок. Однако и мы, и многие наши заказчики и партнеры постепенно движемся к этому почти недостижимому идеалу — антихрупкой ИТ-инфраструктуре. И на этом пути чрезвычайно полезно изучить чужой опыт и чужие ошибки. Дать читателям такую возможность — и есть главная задача этого номера.

12+

РЕДАКЦИЯ ЖУРНАЛА

Главный редактор: **Наталья Травова**
nv.travova@jet.su

Арт-директор: **Наталья Васильева**

Редактор: **Эвелина Кегелик**
ed.kegelik@jet.su

Выпускающий редактор: **Борис Конаков**

Куратор номера: **Андрей Янкин**

Корректор: **Ирина Карпушина**

Фотограф: **Карэн Эгнатосян**

Иллюстраторы: **Вера Подерская, Надежда Андрианова, Эвелина Кегелик, Мария Майдурова, Наталья Васильева**

Изображения: **Shutterstock, ChatGPT, Stable Diffusion, Midjourney, Nano Banana Pro, Seedream 4.5, Topaz**

Авторы и эксперты

Евгений Абакумов, Алексей Акопян, Максим Андрианов, Сергей Андронов, Александр Буланов, Илья Васильченко, Всеволод Воробьев, Сергей Вышемирский, Дмитрий Горохов, Александр Гостев, Владимир Гришанов, Станислав Громов, Игорь Дорофеев, Владимир Золотов, Анастасия Иванова, Дмитрий Казмирчук, Олег Кандальцев, Эвелина Кегелик, Анастасия Кисько, Борис Конаков, Александр Копылов, Анна Коробецкая, Станислав Котлячков, Александр Локтионов, Алексей Лукацкий, Алексей Малинский, Павел Михайлик, Александр Морковчин, Владимир Муравьев, Аскар Мусаев, Иван Мыздриков, Ольга Мягченко, Никита Осипов, Илья Панкратов, Юрий Пирогов, Георгий Руденко, Ринат Сагиров, Константин Сапронов, Юрий Семенюков, Кристина Сердюкова, Анна Теклина, Анна Терская, Павел Тесленко, Константин Титков, Наталья Травова, Дмитрий Унтила, Даниэль Халиулин, Анастасия Храмцова, Кира Шиянова, Игорь Шконда, Андрей Янкин

Адрес редакции

127015, Россия, г. Москва, ул. Большая Новодмитровская, д. 14, стр. 1,
бизнес-центр «Новодмитровский»

Отпечатано в типографии

ООО «ПОЛИГРАФСНАБ», 119421, г. Москва, ул. Обручева, д. 8, пом. 2/1

Тираж

4000 экз.

Дата выхода тиража из печати

17 апреля 2026 г.

Издатель

АО «Инфосистемы Джет»

Адрес издателя:

127015, г. Москва, ул. Большая Новодмитровская, д. 14, стр. 1

РАСПРОСТРАНЯЕТСЯ БЕСПЛАТНО

Оформить подписку на журнал:
jetinfo@jet.su

Сотрудничество и продвижение: **Наталья Травова**
nv.travova@jet.su

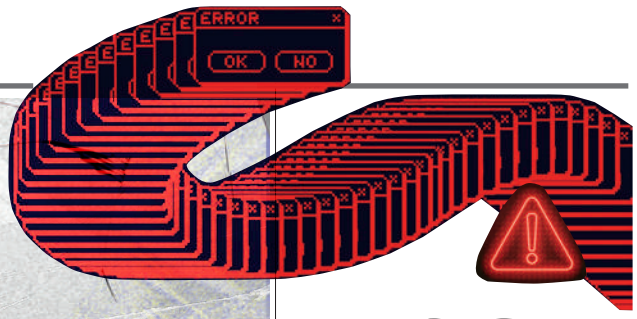
Журнал издается с 1995 г. компанией «Инфосистемы Джет»

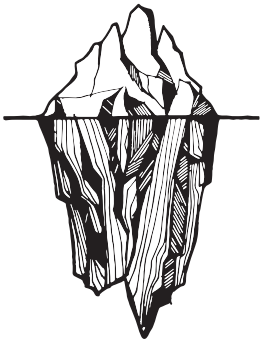
Учредитель: АО «Инфосистемы Джет»
Издание JETINFO зарегистрировано в Федеральной службе по надзору в сфере связи, информационных технологий и массовых коммуникаций (Роскомнадзор). Свидетельство о регистрации средства массовой информации ПИ № ФС77-77514 от 25 декабря 2019 г.

СОДЕРЖАНИЕ

СОДЕРЖАНИЕ

СОДЕРЖАНИЕ





«АНТИхрупкость.

КАК ИЗВЛЕЧЬ ВЫГОДУ ИЗ ХАОСА»: КНИГА НАССИМА ТАЛЕБА В 50 ЦИТАТАХ И ТЕЗИСАХ

«Антихрупкость. Как извлечь выгоду из хаоса» Нассима Талеба — философский бестселлер о том, как не просто переживать неопределенность, а использовать ее для роста. Автор вводит понятие антихрупкости — способности становиться сильнее под давлением кризисов, ошибок и непредсказуемости, превращая хаос из угрозы в инструмент развития.

Хаос неизбежен*

«Черные лебеди» — редкие и непредсказуемые события с серьезными последствиями. Их невозможно предугадать заранее, но по прошествии времени они кажутся очевидными из-за иллюзии объяснимости.

«Белые лебеди» — это ожидаемые, повторяющиеся и статистически предсказуемые события, последствия которых укладываются в привычные модели и не нарушают базовых представлений о мире.

Антихрупкость — это извлекать выгоду из повреждений**

Антихрупкость любит случайность и неопределенность***

Антихрупкость — это работать с неизвестностью и добиваться успеха**

---

* Мир по своей природе не линеен: редкие, неожиданные события оказывают решающее влияние. Игнорировать хаос — значит строить стратегии на иллюзиях.

** Речь не о выживании, а о росте: система становится лучше именно благодаря ударам, сбоям и стрессу.

*** В отличие от хрупких систем, антихрупкие выигрывают от непредсказуемости, потому что она создает возможности для роста и отбора лучших решений.

**** По мнению Талеба, успех не строится на точных прогнозах: антихрупкие системы принимают неизвестность как данность и выстраивают процессы так, чтобы выигрывать при любых сценариях. Они не пытаются угадать будущее, а готовятся к спектру возможных исходов, извлекая выгоду из неожиданностей и редких событий.

Антихрупкость позволяет нам лучше понять, что такое хрупкость.

Мы не можем стать здоровее, не борясь с болезнью, мы не можем стать богаче, не уменьшив потери. Антихрупкость и хрупкость зависят друг от друга.

Практика важнее объяснений*

Абсолютная неуязвимость недостижима, а значит, нужен механизм, посредством которого система станет непрерывно обновляться, извлекая выгоду из непредсказуемых событий, потрясений, стрессоров и переменчивости, а не только страдая от них.

Ошибки — это топливо**

Антихрупкость рождается под воздействием стрессоров.

Антихрупкие системы не боятся ошибок, а, столкнувшись со стрессами и неопределенностью, становятся только сильнее

Системы становятся лучше, если испытывают управляемую нагрузку.

Штиль убивает***

Иммунитет становится крепче, когда организм встречается с вирусами и бактериями. Вот почему стерильность вредна.

Выживают виды, которые меняются и становятся сильнее благодаря стрессорам из окружающей среды.

Без перемен нет стабильности

---

* Талеб противопоставляет «знание из опыта» абстрактным теориям: реальные действия и эксперименты дают больше пользы, чем красивые модели.

** Малые ошибки и неудачи позволяют системе учиться и адаптироваться, если цена каждой ошибки ограничена.

*** Отсутствие стресса ослабляет систему: как мышцы без нагрузки, она деградирует и становится уязвимой для резкого удара.

Когда вы действуете методом проб и ошибок, случайность уже не совсем случайна, поскольку появляется на рациональной основе: вы используете ошибку как источник информации.

Стартапы и малый бизнес часто выигрывают, адаптируясь к кризисам и неудачам, в то время как крупные корпорации могут быть хрупкими.

Хрупкое хочет спокойствия, антихрупкое развивается в условиях беспорядка, а неуязвимому попросту все равно.

Если неопределенность нельзя устранить, ее следует приручить

Если всякая проба дает вам сведения о том, что не работает, вы яснее видите правильное решение, а значит, каждая попытка становится более ценной и вы воспринимаете ошибки скорее как издержки. По пути к результату вы, конечно, совершаете массу открытий.

Антихрупкость несовместима с иллюзией полного контроля*

Антихрупкими не рождаются — антихрупкими становятся**

Стрессоры и сбои — источник информации, а не проблема***

Антихрупкость мобилизует нас, реагируя на стрессоры и травмы и порождая гиперреакцию и гиперкомпенсацию.

Сложные системы нельзя улучшить без риска их сломать****

Антихрупкость — это способность использовать хаос и неопределенность себе во благо.

---

* Попытка все предсказать и зарегулировать увеличивает хрупкость, потому что реальность всегда сложнее любой модели.

** Антихрупкость — это результат воздействия структуры и среды, а не врожденное свойство. Ее можно спроектировать.

*** Каждый сбой показывает, где система слаба, и дает сигнал, как ее улучшить, — если этот сигнал не подавлять.

**** Вмешательство в сложные системы часто имеет непредсказуемые побочные эффекты, поэтому оптимизация сверху опасна.

Информация антихрупка; попытка скрыть информацию делает ее более значимой, чем попытка донести ее до широких масс. Посмотрите, как люди теряют репутацию именно из-за того, что усиленно пытаются сохранить.

Локальные неудачи предотвращают глобальные катастрофы*

Наша антихрупкость не бесконечна. Многое зависит, например, от частоты стрессоров. Обычно люди лучше справляются с острыми стрессами, чем с хроническими, особенно когда после стресса у них есть время на восстановление, за которое стрессоры успевают выполнить свою работу передатчиков информации.

Антихрупкость нельзя спроектировать напрямую, ее можно только допустить

Свобода экспериментов важнее контроля**

Антихрупкость — это не просто средство от “черного лебедя”; понять, что это такое, значит перестать испытывать сильный интеллектуальный страх перед “черными лебедями” и принять их как нечто необходимое для истории, технологии, науки, для всего на свете.

Настоящая устойчивость проверяется не в спокойствии, а в кризисе***

Главное этическое правило формулируется так: не обладай антихрупкостью за счет хрупкости других.

Медленный рост надежнее быстрого расширения

Скажем, хакеры способствуют тому, что компьютерные системы делаются совершеннее. Или, как в случае с Айн Рэнд, навязчивая и агрессивная критика способствует распространению книги.

Будущее принадлежит не самым умным, а самым адаптивным системам

---

* Небольшие сбои действуют как предохранители: они снимают напряжение и не дают проблемам накапливаться.

** Децентрализованные эксперименты позволяют находить работающие решения быстрее, чем централизованное управление.

*** Пока нет стресса, нельзя понять, устойчива ли система на самом деле, — кризис всегда раскрывает правду.

Нашу жизнь существенно упрощает то обстоятельство, что неуязвимое и антихрупкое, в отличие от хрупкого, не нуждаются в точном понимании мира, а значит, и в предсказаниях тоже.

Антихрупкие системы не просто выживают под давлением — они становятся сильнее

Хрупкость проявляется там, где есть страх ошибок и стремление к стабильности

Антихрупкость — это сочетание агрессивности и паранойи: ограничьте потери, позаботьтесь о защите от крайнего риска, а приобретения, позитивные "черные лебеди", позаботятся о себе сами. Это асимметрия Сенеки: мы больше приобретаем и меньше теряем, когда попросту уменьшаем большие потери (эмоциональный ущерб), а не улучшаем ситуацию "посередине.

Часто лучшее решение — не вмешиваться*

Антихрупкость требует асимметрии: ограниченный ущерб и неограниченная выгода**

Потрясения приносят антихрупкой вещи больше пользы (и, соответственно, меньше вреда) по мере увеличения их интенсивности (до какого-то уровня).

Вы можете себе позволить большой риск в тех областях, которые неуязвимы для негативных "черных лебедей", и небольшой риск в тех сферах, которые открыты позитивным "черным лебедям", — так вы станете антихрупкими.

Уязвимость возрастает при попытке устранить всю неопределенность***

Чем больше защита от мелких проблем, тем сильнее будущий удар

Прогресс появляется через метод проб и ошибок, а не через планирование

Каково это — быть антихрупким? Сравните такого субъекта с человеком, который невозмутим и сохраняет хладнокровие в острых ситуациях, — считается, что это качество необходимо, чтобы стать лидером, командиром или крестным отцом мафии. Обычно он спокоен, мелкие неудачи его не волнуют, а когда дело пахнет жареным, он изумляет вас самоконтролем.

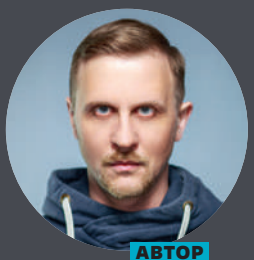
---

* Иногда отсутствие действий снижает риски эффективнее, чем активные попытки что-то исправить.

** Идеальная стратегия — когда потери заранее ограничены, а потенциальный выигрыш может быть многократно больше.

*** Чем сильнее систему «стерилизуют» от случайностей, тем болезненнее для нее редкий, но неизбежный шок.

ГОСТЬ НОМЕРА



АВТОР

Александр Гостев,

главный технологический эксперт «Лаборатории Касперского», автор Telegram-канала «Гостев из будущего»

«СЕРЫЕ ЛЕБЕДИ» ЦИФРОВОЙ ЭПОХИ

ПОЧЕМУ УСТОЙЧИВОСТЬ ИТ ОПРЕДЕЛЯЕТСЯ НЕ УГРОЗАМИ, А АРХИТЕКТУРОЙ ДОВЕРИЯ

- Цифровая инфраструктура может потерять устойчивость, если нарушится доверие к базовым элементам — времени, криптографии или данным
- Часть данных со временем перетекает на недосягаемые «цифровые архипелаги»
- Цифровая инфраструктура зависит от базовых предположений, которые считаются несокрушимыми
- «Серые лебеди» — возможные события, которые в будущем могут существенно изменить сферу кибербезопасности
- Антихрупкая ИТ-инфраструктура проектируется под неопределенность, а не против нее

Большинство прогнозов в сфере кибербезопасности строятся по понятной логике: существующие угрозы масштабируются, усложняются и автоматизируются. Такой подход полезен, но он не затрагивает более глубокого уровня — устойчивости самих технологических оснований, на которых построена современная цифровая среда. Сценарии, которые можно условно назвать «серыми лебедями», находятся между привычными прогнозами и маловероятными катастрофами. Это не попытка предсказать конкретное событие в конкретный момент, а анализ ситуаций, при которых перестают работать ключевые предположения: о надежности времени, неизменности криптографии, доступности данных или целостности инфраструктуры. Именно такие сдвиги способны радикально изменить правила игры.

Когда время перестает быть надежным ориентиром

Синхронизация времени — одна из фундаментальных основ цифрового мира. Для функционирования систем промышленного управления, механизмов аутентификации и средств реагирования на инциденты, выполнения финансовых операций требуются согласованные временные метки. Их согласованность обеспечивается иерархией источников времени и протоколом Network Time Protocol ***(NTP)***.

Компрометация первичных источников — например, спутниковых систем или атомных часов — может привести к появлению малозаметных отклонений, которые постепенно распространятся по всей инфраструктуре. Эти изменения могут быть настолько незначительными, что не вызовут немедленной тревоги, но их последствия окажутся системными.

Даже минимальные расхождения способны нарушить последовательность транзакций в финансовых системах, вызвать ошибки при проверке сертификатов шифрования и сбои в процессах клиринга. В такой ситуации проблема заключается не в потере самого времени, а в разрушении доверия к нему как к универсальной координате цифровых процессов.

Цифровое наследие, которое невозможно восстановить

Современная цивилизация накопила колоссальные объемы данных, начиная с конца XX века. Однако значительная часть этой информации хранится в устаревших форматах, проприетарных системах и на физических носителях с ограниченным сроком службы.

Со временем возникает риск появления недосягаемых «цифровых архипелагов» — массивов данных, которые формально существуют, но практически недоступны. Отсутствие совместимого программного обеспечения, специалистов и технической документации превращает такие архивы в недоступные фрагменты прошлого.

Физическая деградация носителей лишь усугубляет проблему. Даже современные инструменты анализа, включая системы на базе искусственного интеллекта, не гарантируют восстановления информации, если исходная среда утрачена. В результате человечество может столкнуться с постепенной, но необратимой потерей части собственной цифровой памяти.

Интеллектуальная собственность как барьер для прогресса

Искусственный интеллект ускоряет научные исследования и технологические разработки, но одновременно создает новые правовые риски. Компании все чаще регистрируют права не только на конкретные решения, но и на целые классы алгоритмов и методов.

Если различные системы искусственного интеллекта, обученные на схожих данных, приходят к аналогичным результатам, возникают проблемы с правами

на интеллектуальную собственность. Это особенно критично в областях с высокой научной и коммерческой значимостью — таких как медицина, химия или материаловедение.

Правовая неопределенность может привести к замедлению исследований, сокращению инвестиций и отказу от разработки перспективных направлений из-за риска судебных споров. В конечном итоге это поставит под вопрос саму модель защиты интеллектуальной собственности в условиях автоматизированного создания знаний.

Переоценка возможностей искусственного интеллекта

Инвестиции в искусственный интеллект растут на фоне ожиданий резкого повышения эффективности и появления универсальных интеллектуальных систем. Однако существует риск постепенного разрыва между ожиданиями и реальными результатами. Такой сценарий будет развиваться не как внезапный кризис, а как последовательность разочарований: проекты не достигают ожидаемой эффективности, затраты оказываются выше спрогнозированных, а экономическая отдача — ниже.

В этих условиях внимание инвесторов может сместиться с масштабных амбициозных инициатив на практические и прикладные решения. Искусственный интеллект останется важным инструментом, но его развитие станет более прагматичным и ориентированным на конкретные задачи.

Внезапный коллапс криптографии из-за математического прорыва

Современные системы безопасности базируются на вычислительной сложности математических задач. Именно она лежит в основе криптографических алгоритмов, используемых для защиты данных.

Наиболее обсуждаемая угроза — развитие квантовых вычислений. Однако «серым лебедем» может вполне неожиданно стать появление нового математического метода, позволяющего эффективно решать задачи, ранее считавшиеся трудными, даже с использованием обычных компьютеров.

Если подобное открытие произойдет, доверие к существующим механизмам защиты может быть утрачено практически мгновенно. В этом случае это поставит под угрозу инфраструктуру открытых ключей, цифровые подписи и защищенные соединения, на которых сегодня во многом основана безопасность современных цифровых коммуникаций.

КЛЮЧЕВАЯ ЗАДАЧА — НЕ ПОПЫТКА ПРЕДСКАЗАТЬ ВСЕ ВОЗМОЖНЫЕ УГРОЗЫ, А ПОСТРОЕНИЕ ИНФРАСТРУКТУРЫ, СПОСОБНОЙ ПРОДОЛЖАТЬ РАБОТУ В УСЛОВИЯХ НЕОПРЕДЕЛЕННОСТИ. ЭТО ОЗНАЧАЕТ ПРОЕКТИРОВАНИЕ СИСТЕМ С УЧЕТОМ ВОЗМОЖНЫХ ОТКАЗОВ И ПОТЕРИ ДОВЕРИЯ К ОТДЕЛЬНЫМ КОМПОНЕНТАМ

СО ВРЕМЕНЕМ ВОЗНИКАЕТ РИСК ПОЯВЛЕНИЯ НЕДОСЯГАЕМЫХ «ЦИФРОВЫХ АРХИПЕЛАГОВ» — ФОРМАЛЬНО СУЩЕСТВУЮЩИХ МАССИВОВ ДАННЫХ. ОТСУТСТВИЕ СОВМЕСТИМОГО ПО, СПЕЦИАЛИСТОВ И ТЕХНИЧЕСКОЙ ДОКУМЕНТАЦИИ ПРЕВРАЩАЕТ ТАКИЕ АРХИВЫ В НЕДОСТУПНЫЕ ФРАГМЕНТЫ ПРОШЛОГО

Кибератаки с долгосрочными последствиями

Не все кибератаки направлены на получение немедленной выгоды. Некоторые сценарии предполагают незаметное воздействие с накопительным эффектом. Например, вмешательство в системы управления промышленными объектами может постепенно привести к серьезным изменениям параметров работы оборудования. Такие изменения могут долго оставаться незамеченными.

Атаки на вспомогательные системы — включая инфраструктуру охлаждения или энергоснабжения — способны вызвать цепные сбои, затрагивающие облачные сервисы и критически важные цифровые платформы.

Фрагментация глобальной сети

Глобальный интернет традиционно рассматривается как устойчивая и децентрализованная система. Однако в действительности ключевые элементы инфраструктуры — корневые серверы DNS, сертификационные центры, магистральные кабели — представляют собой точки концентрации риска.

Скоординированное воздействие на эти элементы может привести к цифровой изоляции отдельных регионов. В таком случае организации будут вынуждены функционировать в ограниченных экосистемах с нарушенными международными связями. Последствия подобного сценария могут затронуть не только технологическую сферу, но и глобальную экономику, торговлю и научное сотрудничество.

Космическая инфраструктура как новая зона риска

Современная цифровая среда во многом зависит от спутниковых систем, обеспечивающих навигацию, связь и синхронизацию времени. Однако эта инфраструктура подвержена воздействию природных факторов.

Сценарий «серого лебедя» может возникнуть из-за экстремальных солнечных явлений, которые способны вызвать нарушения в работе спутников, сбои навигационных систем и перегрузку наземной инфраструктуры. Это приведет к цепным последствиям для отраслей, зависящих от космических сервисов. В таком случае космическая инфраструктура из надежного элемента превратится в источник системной нестабильности.

Когда проблема не в атаках, а в базовых предположениях

На первый взгляд перечисленные сценарии выглядят как набор отдельных угроз, но на практике у них есть общий источник — зависимость цифровой инфраструктуры от базовых предположений, которые считаются несокрушимыми. Системы предполагают, что время синхронизировано, криптография надежна, данные доступны, а инфраструктура всегда остается связанной и управляемой. Пока эти условия выполняются, цифровая среда функционирует предсказуемо. Но если нарушается хотя бы одно из них, последствия выходят далеко за пределы отдельной системы или организации.

Это принципиально другой уровень риска. В таких ситуациях перестают работать не отдельные механизмы защиты, а основа, на которой они построены. Именно поэтому устойчивость определяется не только способностью отражать известные атаки, но и готовностью работать в условиях, когда привычные точки опоры больше не гарантированы.

Эта логика требует пересмотра подхода к проектированию инфраструктуры: необходимо ориентироваться на предотвращение сбоев, а также на способность системы сохранять управляемость, даже если часть ее фундаментальных элементов перестает быть надежной.

Устойчивость начинается с признания неопределенности

Подготовка к будущим угрозам требует смещения фокуса — от реакции на известные сценарии до проектирования систем, способных адаптироваться к неизвестным. Именно этот подход создает основу устойчивости в условиях, когда сама природа цифровых рисков продолжает меняться.

Надежность цифровых систем формируется на уровне архитектуры, а не отдельных средств защиты. Чем больше инфраструктура зависит от единственных точек доверия — одного поставщика, одного механизма аутентификации или одного источника времени, тем выше риск масштабного сбоя и его цена. Чем более централизованной и оптимизированной становится инфраструктура, тем меньше ее запас прочности. В результате даже локальное нарушение может привести к цепной реакции и затронуть значительную часть системы.

Поэтому ключевая задача — не попытка предсказать все возможные угрозы, а построение инфраструктуры, способной продолжать работу в условиях неопределенности. Это означает проектирование систем с учетом возможных отказов, потери доверия к отдельным компонентам и необходимости работать в ограниченном режиме. Такой подход позволит снизить последствия даже тех событий, которые невозможно заранее предусмотреть, и сделает устойчивость не реакцией на кризис, а встроенным свойством цифровой среды.

АНТИХРУПКОСТЬ КАК СТРАТЕГИЯ: ПРОЕКТИРОВАНИЕ СИСТЕМ, ГОТОВЫХ К НЕИЗВЕСТНОМУ

ФИЛОСОФИЯ АНТИХРУПКОЙ ИТ-ИНФРАСТРУКТУРЫ

Проектируйте под неопределенность, а не против нее.

Планируйте не отдельные известные инциденты, а классы провалов: утрату доверия, рассинхронизацию систем, компрометацию поставщика, исчезновение данных или форматов, потерю физического доступа к инфраструктуре. Конкретные сценарии лишь примеры; структура уязвимости важнее симптомов.

Предпочитайте много маленьких отказов одному большому.

Монокультура — одно облако, один IdP, один CI/CD, один формат бэкапов — создает иллюзию простоты, но накапливает скрытый риск. Диверсификация неудобна в управлении, зато ограничивает масштаб любой аварии.

Ставьте обратимость и проверяемость выше оптимальности.

Сверхэффективность — минимальные буферы, агрессивная оптимизация, «все в real-time» — убирает запас прочности и ускоряет каскадные отказы. Избыточность и «потери» на дублирование — это не неэффективность, а страховка.

Стройте доверие как цепочку предположений и регулярно ее проверяйте.

Каждое «мы доверяем X» должно иметь альтернативу, способ верификации и понятную процедуру выхода. Доверие без плана отзыва — это зависимость.

Проектируйте деградацию, а не только отказоустойчивость.

Система должна продолжать функционировать, хотя и будет работать хуже. Плавная деградация — явное требование при проектировании.

Telegram-канал «Гостев из будущего»

ЗРЕЛОСТЬ РЕШАЕТ

ПОЧЕМУ УПРАВЛЕНИЕ ИТ-ИНФРАСТРУКТУРОЙ ВАЖНЕЕ ТЕХНОЛОГИЙ

ЭКСПЕРТ

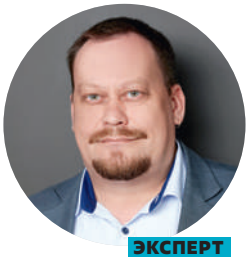
Павел Тесленко,

руководитель направления ИТ-аудита и бизнес-консалтинга компании «Инфосистемы Джет», куратор исследования

ЭКСПЕРТ

Илья Панкратов,

заместитель председателя наблюдательного совета itSMF, руководитель проекта «РИТМ»



ЭКСПЕРТ

Станислав Котлячков,

руководитель департамента инфраструктуры компании «Уралайтех»

64% российских компаний не используют системный подход в управлении ИТ

27% компаний выстроили зрелое взаимодействие между ИТ-отделом и бизнесом

61% организаций способны пережить локальный отказ оборудования

Для российского бизнеса неопределенность — уже привычный режим работы, и в нем важна не только киберустойчивость. На передний план выходит антихрупкость — способность компании использовать кризисные ситуации как возможность для дальнейшего развития. Но готов ли рынок использовать такой подход? Исследование зрелости ИТ в 120 российских организациях, проведенное компанией «Инфосистемы Джет» в 2025 году, показывает прямую связь между состоянием ИТ-ландшафта и умением бизнеса адаптироваться к непредсказуемым событиям. Решающим конкурентным преимуществом компаний в период перемен становится не наличие передовых технологий, а высокое качество управления и прочная связь ИТ-департамента с бизнесом.

Смена приоритетов: успех зависит от скорости изменений

В условиях постоянных киберугроз, технологических разрывов и высокой неопределенности бизнесу важно не только предотвращать сбои, но и быстро восстанавливаться, адаптироваться к изменениям и продолжать работать даже в нестандартных сценариях. Однако результаты исследования, проведенного компанией «Инфосистемы Джет», показывают, что более чем у половины российских организаций ИТ-инфраструктура по-прежнему ориентирована на стабильную работу, а не на быстрые изменения и восстановление после инцидентов.

Павел Тесленко, куратор исследования

«Основная задача ИТ сейчас — поддерживать бизнес и помогать ему зарабатывать больше за счет скорости, предсказуемости и управляемости процессов. В этом смысле управление ИТ — это не набор технологий и формальных документов, а способность компании быстро пересматривать приоритеты без роста рисков и простоев».

Ключевым фактором здесь становится зрелое взаимодействие между ИТ-отделом и бизнесом. Согласно результатам исследования, оно выстроено лишь в 27% российских компаний. В этих организациях ИТ-департамент системно собирает обратную связь от бизнес-подразделений и использует ее при формировании приоритетов дальнейшего развития.

В остальных компаниях связь между ИТ-департаментом и бизнесом остается фрагментарной. Планы формируются ситуативно, решения принимаются с запозданием, а ИТ-служба работает в режиме реакции, а не опережения. В такой модели ИТ-отдел поддерживает текущее состояние инфраструктуры, но редко становится точкой роста.

Рабочий подход выглядит иначе. Там, где управление ИТ встроено в регулярный управленческий цикл и опирается на постоянный диалог с бизнесом, оно соответствует темпу развития компании. Это снижает стоимость ошибок, ускоряет принятие решений и позволяет не воспринимать любые изменения как угрозу устойчивости.

Станислав Котлячков

«Зрелость ИТ — это когда руководители бизнес-направлений воспринимают ИТ-отдел не как техническую службу, а как партнера, понимающего производственные и финансовые задачи компании. Кроме того, зрелость проявляется в формализации процессов управления изменениями, инцидентами, конфигурациями, рисками. Именно процессная дисциплина, а не модные решения обеспечивает устойчивость инфраструктуры в крупной промышленной компании».

Не для галочки: стратегия как инструмент управления

Связующим звеном между бизнес-целями компании и развитием ее ИТ-ландшафта служит актуальная ИТ-стратегия. И 47% организаций на российском рынке уже ее сформировали, а еще 17% находятся в процессе разработки.

Наличие у компаний ИТ-стратегии

Илья Панкратов

«Сегодня заметна усталость топ-менеджеров от теоретических стратегий. Бизнес все чаще ожидает от ИТ-консультантов не деклараций, а четких планов достижения измеримых результатов. Стратегия перестает быть документом “для отчета” и становится рабочим инструментом управления».

Кстати, исследование подтвердило, что спрос на ИТ-консалтинг повышается, в том числе из-за тренда на импортозамещение: компаниям требуется экспертиза в области отечественных решений и их совместимости. В настоящее время 71% организаций обращаются за ИТ-поддержкой к внешним подрядчикам и только 25% активно наращивают внутренние ИТ-компетенции.

Такая ситуация во многом связана с дефицитом необходимых ИТ-специалистов: 84% респондентов признались, что в их организациях на подбор сотрудников уходит много времени — полгода и больше. Особенно это касается редких и узких специализаций *(архитекторы, ИБ-специалисты и инженеры)*. Вместе с тем длительное ожидание пополнения штата вызывает перегрузку уже работающих сотрудников. В 20% компаний переработки айтишников стали нормой, что увеличивает риски текучести кадров и ухудшения качества работы.

Илья Панкратов добавляет, что особенно важны выводы авторов исследования относительно управления ИТ: 64% компаний не имеют системного подхода, а 18% организаций вовсе не формализуют процессы. По мнению эксперта, в условиях ограниченной доступности зарубежных сводов знаний по управлению ИТ особенно возрастает значение российских методологических подходов.

Значимость качества управления ИТ отметили и в компании «Уралайтех».

Станислав Котлячков

«Зрелость ИТ определяется не стеком технологий, а предсказуемостью и управляемостью. Если ИТ-подразделение обеспечивает стабильность сервисов, выдерживает целевые показатели доступности систем, умеет прогнозировать загрузку мощностей и бюджет, системно предотвращает инциденты, а не “героически их тушит”, то это уже показатель зрелости. Важным критерием является прозрачность для бизнеса: понятные SLA, измеримые KPI, регулярная отчетность, связь инициатив с экономическим эффектом».

Аналитики компании «Инфосистемы Джет» оценивали зрелость ИТ-управления по 18 параметрам и учитывали размеры организаций и отрасли, в которых они работают. Наибольший разрыв между целевыми показателями и реальной картиной наблюдается в стратегии. Формирование ИТ-стратегии, работа архитектурных комитетов, а также использование модели аллокации затрат на ИТ остаются на низком уровне даже в крупных компаниях.

Кроме того, исследование показало, что ни одна отрасль не достигла целевой картины по всем параметрам. Это говорит о том, что рынок в целом пока только формирует зрелую ИТ-модель. Наибольших результатов достигли компании из сферы ИТ и финансового сектора.

Логика устойчивости: микросервисы требуют согласованной работы

Микросервисная архитектура приложений сегодня стала отраслевым стандартом. По данным исследования, такой подход в том или ином виде используют уже 75% компаний и эта доля продолжает расти. С учетом этого тренда работают и российские вендоры: большинство новых решений изначально проектируются для работы в микросервисной модели, то есть с расчетом на масштабирование и частые изменения.

Это радикально меняет подход к обеспечению устойчивости. Если раньше надежность ИТ определялась в первую очередь качеством оборудования и резервированием на уровне ЦОД, то сегодня она зависит от того, как устроено взаимодействие сервисов и насколько оно управляемо. Устойчивость

Оценка зрелости ИТ, отрасли

формируется не «снизу» *(на уровне ИТ-инфраструктуры)*, а на уровне архитектуры всего ИТ-ландшафта, включая логику приложений.

При использовании микросервисных приложений, в основе которых лежат горизонтальная масштабируемость и слабая связанность между модулями, классические подходы к отказо- и катастрофоустойчивости перестают работать. Репликация данных между ЦОД и зонами доступности все чаще переносится со слоя ИТ-инфраструктуры на уровень логики самого приложения, что снижает зависимость от дорогостоящих аппаратных решений и улучшает гибкость ИТ-ландшафта. Однако одновременно с этим резко повышаются требования к целостному проектированию архитектуры. Ошибки в архитектурных решениях, несогласованные изменения или отсутствие общего замысла начинают влиять не на отдельный сервис, а на всю систему в целом.

Павел Тесленко, куратор исследования

«Надежность в распределенной среде невозможно обеспечить, если компания не видит ИТ как единую систему. Исследование показывает, что 65% организаций применяют подход “единого взгляда на ИТ”, выстраивая централизованные или зонтичные системы мониторинга. Там же, где мониторинг остается фрагментарным, возникают “слепые зоны”. Отдельные сбои долго остаются незамеченными, а ИТ-инциденты проявляются уже на уровне бизнес-процессов».

По словам эксперта, параллельно меняются и подходы к управлению инфраструктурой. Для работы с распределенной средой компании внедряют практики DevOps *(объединение процессов разработки и эксплуатации)* и автоматизацию. Согласно результатам исследования, 36% организаций уже активно используют контейнеризацию и микросервисы, а еще 37% находятся в процессе перехода, внедряя CI/CD *(методологию разработки ПО, объединяющую непрерывную интеграцию и непрерывное развертывание)*. С другой стороны, почти половина опрошенных компаний не применяют оркестрацию контейнеров, что усложняет масштабирование.

Важно, что в распределенной ИТ-среде архитектура больше не формируется в рамках одного проекта. Она складывается из множества параллельных решений, принимаемых разными командами. В компаниях появляются разрозненные сервисы, растет число интеграций, усложняется слой промежуточного ПО *(middleware)* и инфраструктуры. Без согласованной работы команд, занимающихся инфраструктурой, прикладной разработкой, сетью, эксплуатацией и информационной безопасностью, такие решения начинают противоречить друг другу и снижают управляемость. При этом лишь в 30% компаний есть единый архитектурный комитет — команда архитекторов *(корпоративный, системный и solution-архитектор)*, отвечающая за согласованность архитектурных решений, выбор технологий и развитие ИТ-систем в связке с целями бизнеса.

Точка надежности? ЦОД меняет свою роль

Когда устойчивость формируется на уровне архитектуры и управляемости, неизбежно меняется и роль центров обработки данных. ЦОД перестает быть «точкой надежности» сам по себе и становится элементом более широкой системы непрерывности бизнеса.

Согласно исследованию, 48% компаний уже имеют резервный ЦОД, а еще 23% находятся в процессе его внедрения. Однако наличие второй площадки для обработки и хранения данных не гарантирует восстановления после серьезного инцидента.

Павел Тесленко, куратор исследования

«В распределенной среде с микросервисами, зонами доступности и активной репликацией данных классическая модель “основной ЦОД — резервный ЦОД” работает иначе. Непрерывность все чаще строится не вокруг физической площадки, а вокруг сценариев восстановления. Репликация данных, распределение сервисов и переключение нагрузок реализуются на уровне приложений и архитектуры. В этом отношении опасений добавляет тот факт, что, согласно исследованию, минимум четверть компаний не проводят регулярные проверки и тестовые переключения между основным и резервным ЦОД».

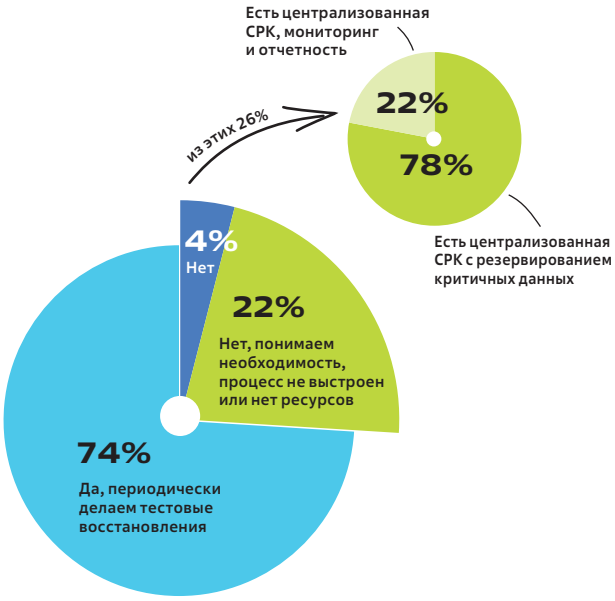
Отсутствие проверок и тестирования в течение шести месяцев может привести к тому, что в случае реального инцидента переключение на резервный дата-центр, скорее всего, окажется неуспешным из-за накопленного технического долга изменений и отсутствия тренировок у команд эксплуатации.

Это напрямую отражается на уровне реальной устойчивости. Исследование показало, что пережить локальный отказ оборудования способны 61% компаний. Однако 28% организаций остаются уязвимыми. Даже единичный сбой может привести к остановке процессов или потере данных.

Проверка готовности к сбоям

Реальная проверка архитектурной управляемости происходит в кризисных сценариях — при сбоях, атаках и потере данных, а также во время имитации этих событий. Однако 26% компаний даже

Проводятся ли тестовые восстановления данных из резервных копий

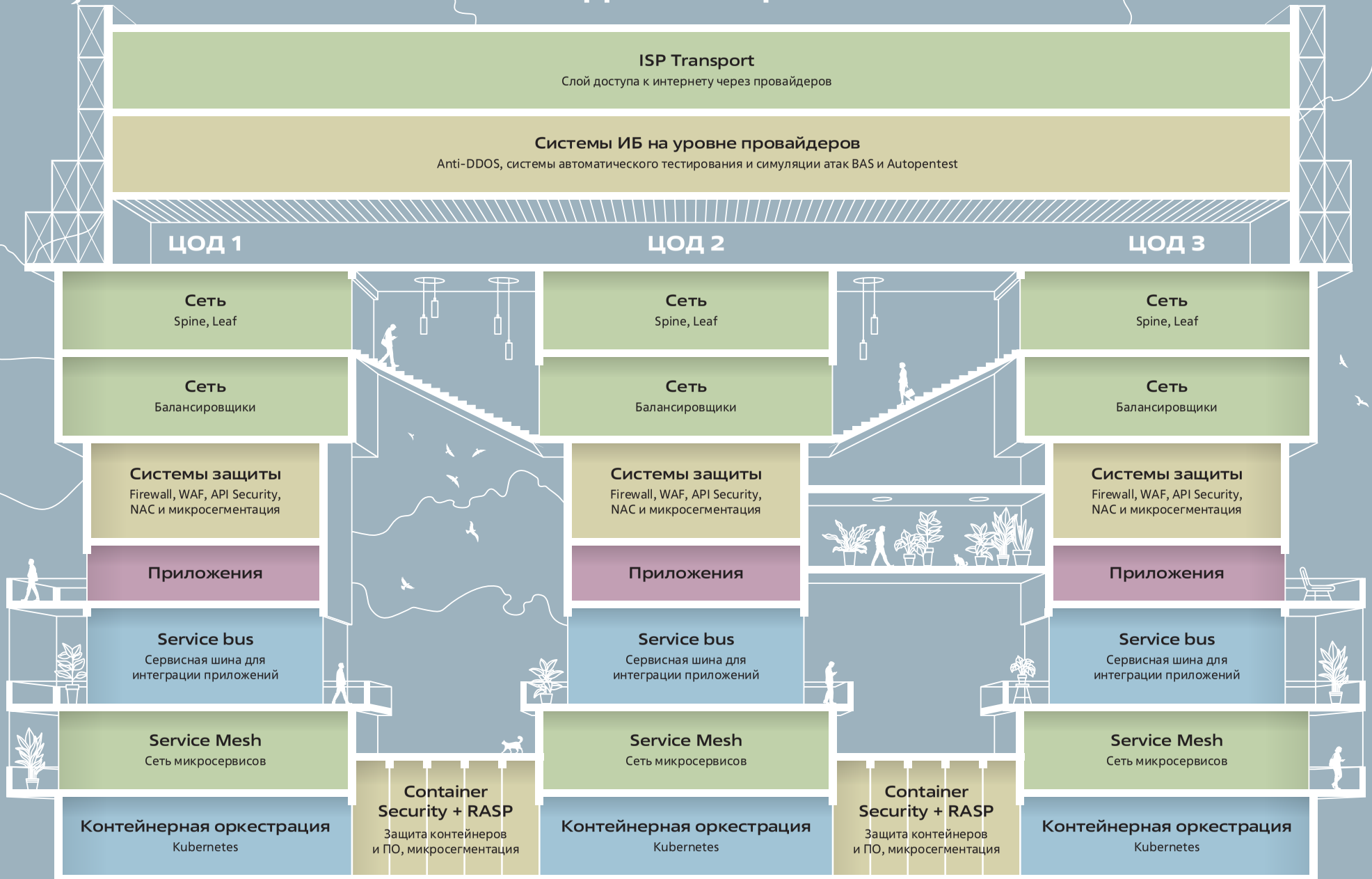


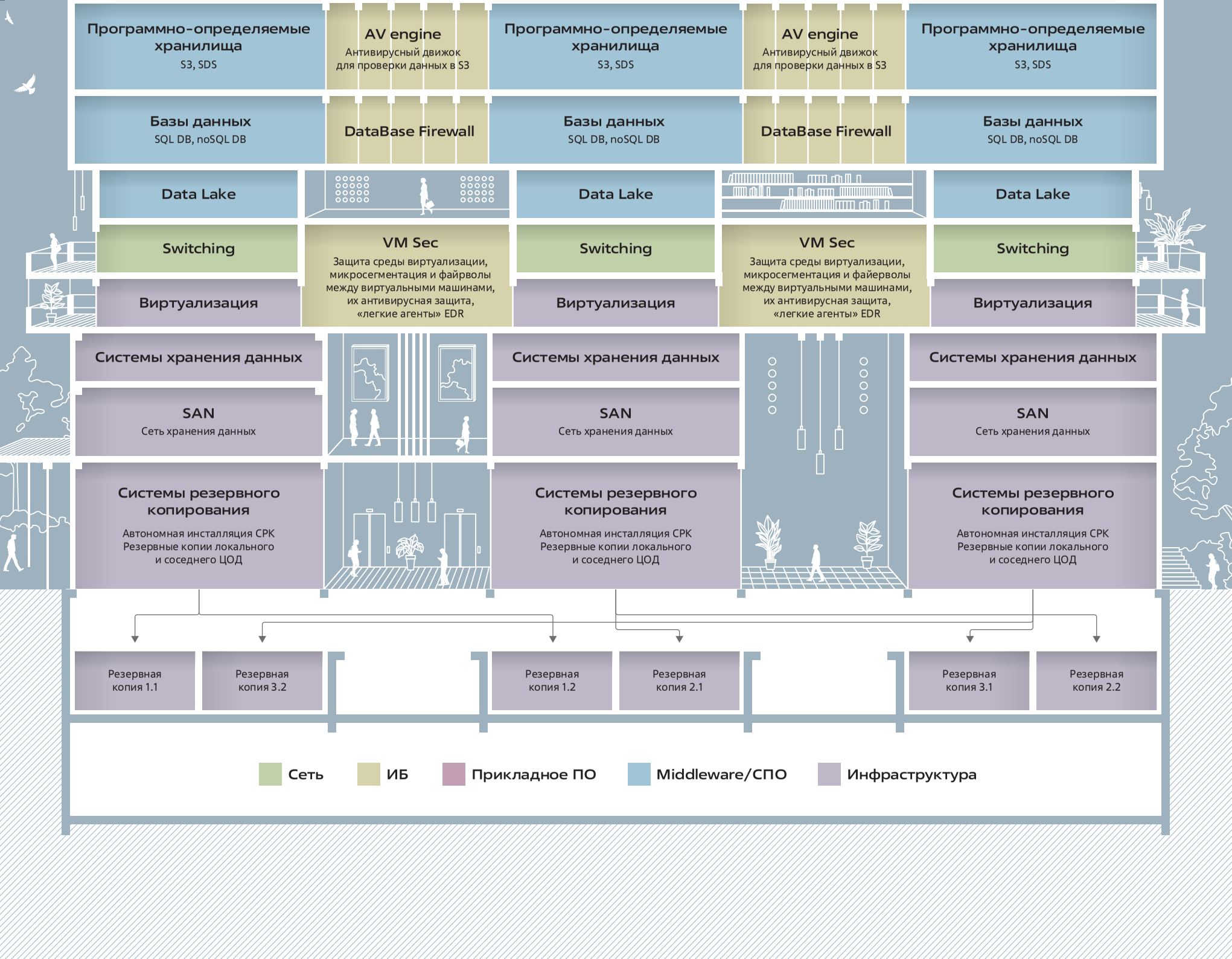
не проводят тестовое восстановление данных, несмотря на то что в большинстве этих организаций уже существует централизованная система резервного копирования *(СРК)*. В условиях роста кибератак и применения вирусов-шифровальщиков это повышает риск не просто потери информации, а полной остановки ключевых бизнес-процессов. Он особенно велик для 19% компаний, где нет централизованной СРК или резервируются не все данные.

Но даже там, где резервирование формально внедрено, уровень готовности к серьезным инцидентам остается ограниченным. Например, лишь 25% компаний для обеспечения полноценного контура защиты данных применяют правило «3-2-1», которое предполагает наличие трех копий данных на двух разных физических носителях и хранение одной из копий вне офиса/ЦОД.

Авторы исследования пришли к выводу, что компании могут быть гибкими только при одном условии: их инфраструктура управляется как целостная система, а не как набор разрозненных решений. Там, где архитектура согласована, изменения автоматизированы, а готовность к сбоям регулярно проверяется, служба ИТ перестает сопротивляться переменам: она начинает поддерживать эксперименты, масштабирование и эволюцию бизнеса без остановки процессов. Реализация именно такого сценария дает возможность спроектировать систему, которая в случае инцидентов будет выживать, адаптироваться и усиливаться.

АРХИТЕКТУРА НЕПРЕРЫВНОСТИ БЕЗ ЕДИНОГО ЦЕНТРА




Программно-определяемые хранилища
S3, SDS
AV engine
Антивирусный движок для проверки данных в S3
Программно-определяемые хранилища
S3, SDS
AV engine
Антивирусный движок для проверки данных в S3
Программно-определяемые хранилища
S3, SDS
Базы данных
SQL DB, noSQL DB
DataBase Firewall
Базы данных
SQL DB, noSQL DB
DataBase Firewall
Базы данных
SQL DB, noSQL DB
Data Lake
Data Lake
Data Lake
Switching
VM Sec
Защита среды виртуализации, микросегментация и файрволы между виртуальными машинами, их антивирусная защита, «легкие агенты» EDR
Switching
VM Sec
Защита среды виртуализации, микросегментация и файерволы между виртуальными машинами, их антивирусная защита, «легкие агенты» EDR
Switching
Виртуализация
Виртуализация
Виртуализация
Системы хранения данных
Системы хранения данных
Системы хранения данных
SAN
Сеть хранения данных
SAN
Сеть хранения данных
SAN
Сеть хранения данных
Системы резервного копирования
Автономная инсталляция СРК
Резервные копии локального и соседнего ЦОД
Системы резервного копирования
Автономная инсталляция СРК
Резервные копии локального и соседнего ЦОД
Системы резервного копирования
Автономная инсталляция СРК
Резервные копии локального и соседнего ЦОД
Резервная копия 1.1
Резервная копия 3.2
Резервная копия 1.2
Резервная копия 2.1
Резервная копия 3.1
Резервная копия 2.2
Сеть
ИБ
Прикладное ПО
Middleware/СПО
Инфраструктура

АРХИТЕКТУРА НЕПРЕРЫВНОСТИ

БЕЗ ЕДИНОГО ЦЕНТРА

РАЗБОР ПО СЛОЯМ

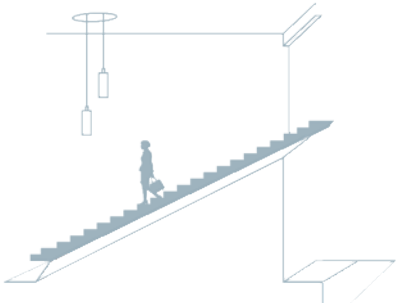
Современная архитектура непрерывности — это не про систему, которая «никогда не падает». Это про систему, которая продолжает работать, когда ее отдельные части выходят из строя. Для современных ИТ такая способность важнее формальной надежности, потому что изменения, отказы и атаки стали обычным режимом работы.

На схеме это сразу видно: параллельно работают три автономных ЦОД. Нет основного и резервного, нет центра, от которого зависит все. Каждая площадка — самостоятельная зона доступности, и отказ одной из них не должен приводить к остановке бизнеса и информационных систем.

АВТОР

Александр Локтионов,

руководитель отдела комплексных проектов компании «Инфосистемы Джет»



Слои доступа и внешнего трафика

(ISP Transport, Anti-DDoS, BAS, Autopentest)

Верхний слой схемы отражает работу каналов данных и внешних сервисов. Здесь показан доступ через провайдеров связи и представлены средства защиты от внешних воздействий. Этот слой выделен, чтобы разграничить внешние слои и внутреннюю архитектуру.

Рядом с Anti-DDoS находятся системы автоматического тестирования и симуляции атак — BAS и Autopentest. Внешняя среда рассматривается как нестабильная по умолчанию. Архитектура не опирается на оптимистичные допущения о характере трафика и не ограничивается установкой защитных механизмов «на всякий случай».

Anti-DDoS здесь — базовая гигиена. Он отсекает грубый шум, но сам по себе не делает систему устойчивой. Устойчивость обеспечивается тем, что намеренно и регулярно воспроизводятся синтетические негативные сценарии. Атаки и аномальные ситуации моделируются до того, как трафик попадает во внутренние слои, и система учится жить в этих условиях. Внешний стресс перестает быть неожиданностью и становится частью штатной эксплуатации.

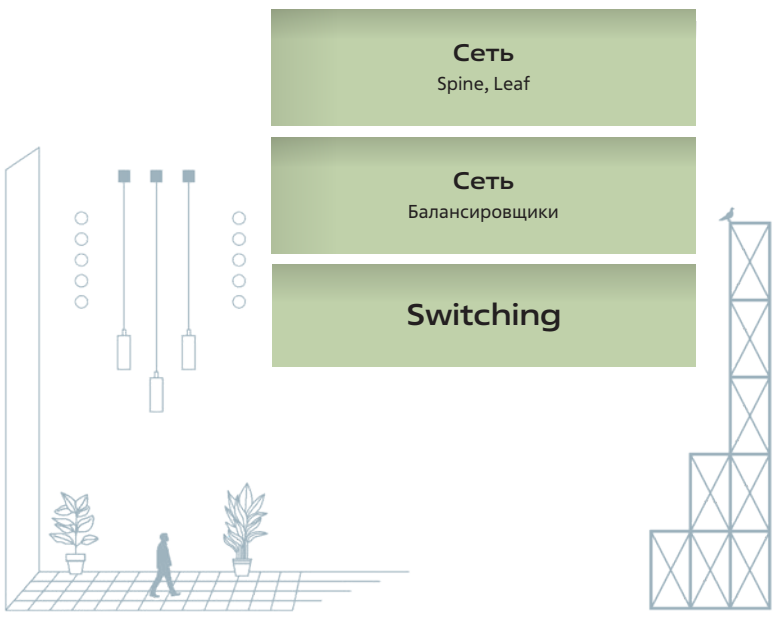
Внутренняя сеть ЦОД

(Spine-Leaf, Switching, балансировщики)

Ниже по схеме расположен сетевой слой каждого ЦОД. Он построен автономно и не предполагает растянутых L2-доменов между площадками. Это не частный пример технического выбора, а одно из ключевых архитектурных решений. Растянутая сеть создает между площадками жесткие зависимости, которые в штатном режиме могут не проявляться. Пока система работает стабильно, такая схема выглядит оптимальной: меньше маршрутизации, проще миграции, меньше логики на уровне приложений. Однако при сетевом сбое или деградации локальная проблема быстро выходит за пределы одной площадки и начинает влиять на работу всей системы.

В современной инфраструктуре такое размещение намеренно исключается. Каждый ЦОД имеет собственную сетевую топологию и собственные домены отказа. Это снижает вероятность каскадных отказов и делает поведение системы при деградации более предсказуемым.

Балансировщик нагрузки в этой части схемы выполняет роль управляемой точки балансировки трафика между сервисами. Он позволяет централизованно управлять маршрутизацией запросов и проверкой «здоровья» конечного сервиса и его компонентов.



Системы защиты

Firewall, WAF, API Security, NAC и микросегментация

Сетевой и прикладной контуры безопасности

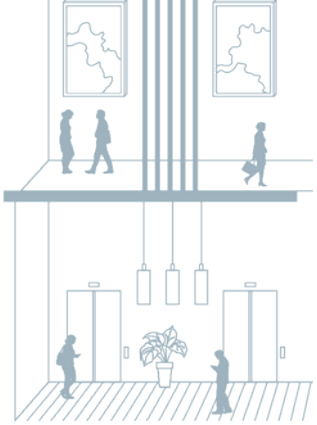
(Firewall, WAF, API Security, NAC, микросегментация)

Следующий слой схемы — сетевой и прикладной контуры безопасности. Межсетевые экраны, защита веб-приложений, API и механизмы микросегментации развернуты в каждом ЦОД автономно и не образуют единого растянутого контура.

Безопасность здесь не рассматривается как способ полностью исключить инциденты. Архитектура предусматривает возможность сбоев, ошибок конфигурации и компрометаций. Поэтому задача этого слоя — ограничить масштаб последствий.

Микросегментация и контроль доступа формируют внутри инфраструктуры набор изолированных зон. Если проблема возникает в одном сегменте, она не должна автоматически распространяться дальше.

Такой подход позволяет переживать инциденты без остановки всей системы и без экстренного вмешательства на уровне инфраструктуры. Важно, что все элементы данного слоя существуют автономно в каждом ЦОД. Это исключает ситуацию, когда сбой или перегрузка одного защитного компонента начинают влиять на работу всех площадок сразу.



Слой приложений и сервисного взаимодействия

(Applications, Service Mesh, Service Bus)

В центре схемы изображены приложения и компоненты их взаимодействия. Именно на этом уровне можно увидеть ключевое изменение в сравнении с классическими архитектурами.

Service Mesh отвечает за управляемое сетевое взаимодействие микросервисов: маршрутизацию, балансировку, контроль доступа и наблюдаемость. Service Bus используется для асинхронной интеграции и обмена событиями между системами. Оба компонента снижают связанность приложений и позволяют им взаимодействовать без жестких прямых зависимостей.

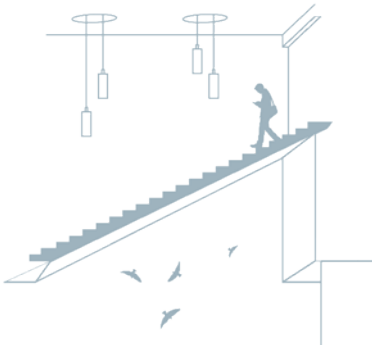
Принципиально важно, что приложения в этой архитектуре не воспринимают инфраструктуру как внешний механизм отказоустойчивости. Они проектируются с учетом того, что могут быть недоступны отдельные сервисы, происходить задержки и асинхронно приходить ответы. ИТ-инфраструктура в этом случае предоставляет правила и инструменты взаимодействия, но не пытается компенсировать архитектурные ограничения приложений за счет растянутых кластеров или сложных схем репликации. Такой подход требует большего внимания на этапе разработки приложений, но в результате система становится устойчивее. Частичный отказ перестает быть аварией, поскольку система остается управляемой.

Контейнерная платформа

(Kubernetes)

Под слоем приложений расположен Kubernetes — платформа, которая управляет жизненным циклом сервисов. Именно на этом уровне антихрупкость начинает проявляться не на уровне схем и документов, а в ежедневной эксплуатации. В работе Kubernetes изначально учитывается возможный выход из строя отдельных компонентов. Контейнер может быть остановлен, узел — стать недоступным, конфигурация — измениться. Это не аварийные сценарии, а штатные события. Благодаря декларативному подходу, согласно которому каждый компонент инфраструктуры описывается в виде манифеста его конфигурации, платформа следит за тем, чтобы фактическое состояние системы соответствовало описанному, и при необходимости автоматически приводит его в порядок.

В такой архитектуре компонент не рассматривается как ценность сам по себе. Если сервис ***(контейнер)*** перестал отвечать или начал вести себя нестабильно, он не анализируется и не «лечится» вручную. Он удаляется и создается заново в соответствии с заданной конфигурацией. Такой подход радикально снижает операционные риски и убирает зависимость от ручных действий в критических ситуациях. Система становится устойчивой не потому, что в ней нет отказов, а потому, что она умеет быстро и предсказуемо пересоздаваться.



Защита контейнеров и данных

(Container Security, RASP, AV engine для S3)

Рядом с контейнерной платформой на схеме показаны средства защиты контейнеров и проверки данных. Это важное изменение в подходе к безопасности: защита больше не сосредоточена только на периметре.

Container Security и RASP работают непосредственно в среде выполнения приложений. Они позволяют контролировать, что именно делает сервис во время работы, и реагировать на его аномальное поведение. Это особенно важно в микросервисных архитектурах, где классические средства периметральной защиты уже не дают полной картины происходящего.

Антивирусный движок для проверки данных в S3-хранилищах решает отдельную, критичную задачу. Объектные хранилища часто используются как точка интеграции между системами, и данные могут попадать туда из разных источников ***(информационных систем)***. Проверка на входе и выходе позволяет снизить риск распространения вредоносного контента внутри ИТ-инфраструктуры.

Слой данных

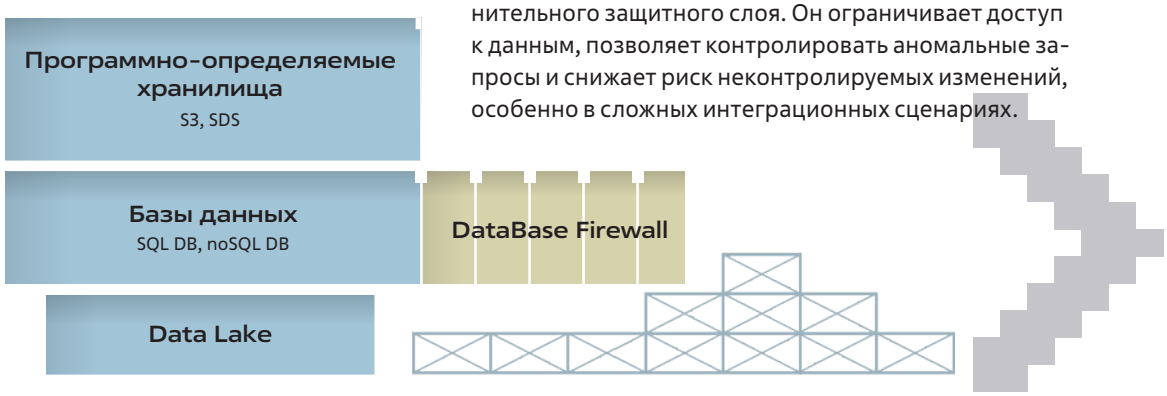
(SQL DB, NoSQL DB, Data Lake, S3/SDS, Database Firewall)

Слой данных — один из самых сложных и чувствительных в современной архитектуре. Именно здесь чаще всего возникает желание сделать всё устаревшими, но зарекомендовавшими себя способами с помощью инфраструктуры. На практике такой подход быстро приводит к снижению непрерывности.

При таком устаревшем подходе СУБД или другие данные растягиваются ***(реплицируются)*** различными средствами между несколькими ЦОД, что неизбежно приводит к потере их автономности и фактическому объединению ЦОД в одну зону доступности. Кроме того, наличие одной «основной» СУБД плохо сочетается с микросервисной архитектурой. В таких схемах переключение между экземплярами СУБД часто требует ручных операций ***(изменения конфигураций, переподключения приложений или их перезапуска)***, что приводит к простою сервисов.

Современный подход подразумевает, что разные данные имеют разную бизнес-ценность и разные требования к их доступности и согласованности. Для одних операций допустима задержка или асинхронная репликация данных, для других — нет. Попытка обеспечить одинаковые гарантии для разных данных приводит к появлению тяжелых и плохо управляемых решений, а также к значительному увеличению стоимости ИТ-инфраструктуры. Поэтому часть ответственности за согласованность данных сознательно переносится в логику приложений и промежуточных слоев. Это усложняет разработку, но делает архитектуру в целом более гибкой и масштабируемой. Инфраструктура «перестает притворяться», что может всеобъемлюще обеспечить консистентность данных бизнес-приложений, находящихся в разных ЦОД.

Database Firewall в этой схеме выполняет роль дополнительного защитного слоя. Он ограничивает доступ к данным, позволяет контролировать аномальные запросы и снижает риск неконтролируемых изменений, особенно в сложных интеграционных сценариях.



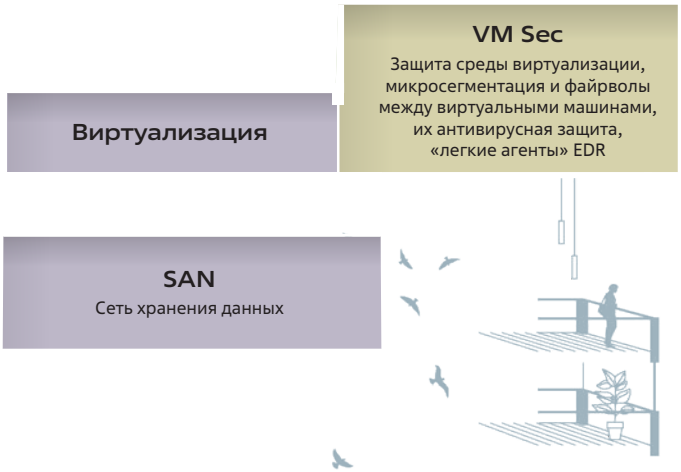
Инфраструктурный фундамент

(Виртуализация, SAN, VM Sec)

Ниже на схеме расположен инфраструктурный слой, включающий виртуализацию, системы хранения данных и средства защиты виртуальной среды. Эти технологии остаются важной частью архитектуры, но их роль принципиально меняется в сравнении с классическими подходами.

В такой модели ИТ-инфраструктура непрерывности перестает быть основным механизмом, обеспечивающим отказоустойчивость на уровне всей системы. От нее больше не ожидают, что она свяжет сервисы между площадками или обеспечит непрерывность работы за счет растянутых кластеров системы виртуализации и синхронной репликации на уровне СХД. Теперь инфраструктура отвечает за стабильную и предсказуемую работу ресурсов внутри одного ЦОД. Все компоненты этого слоя работают строго в пределах своей площадки и не образуют растянутых доменов между разными ЦОД. Такое ограничение намеренно снижает архитектурную сложность. Процессы виртуализации и работа систем хранения в аварийных сценариях становятся более понятными и управляемыми, а локальный сбой не перерастает в проблему сразу для нескольких площадок.

Благодаря этому можно обеспечить отказоустойчивость системы в целом, используя автономные зоны доступности, платформенные механизмы и логику приложений. Инфраструктура при этом остается надежным фундаментом, но перестает быть точкой концентрации рисков.

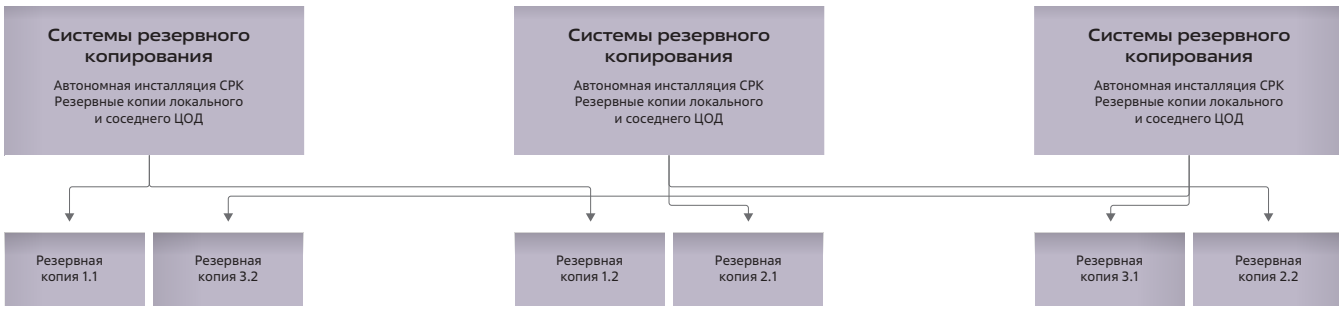


Резервное копирование как последний рубеж

(Автономная СРК, резервные копии между ЦОД)

Самый нижний слой схемы включает системы резервного копирования и восстановления данных. Он предназначен для восстановления системы в ситуациях, когда не сработали остальные механизмы: при воздействии логических ошибок, влиянии разрушительных ИБ-инцидентов, эффекте человеческого фактора. Именно поэтому системы резервного копирования развернуты автономно, а копии данных распределены между площадками.

Здесь разрушается иллюзия «абсолютной защиты», поскольку могут произойти события, после которых потребуются откат и восстановление. Наличие независимого, изолированного контура резервного копирования делает такое восстановление реальным, а не формальным, а соответствие правилу 3-2-1 с отчуждаемыми копиями данных в соседнем ЦОД повышает шансы на восстановление.



СОВРЕМЕННАЯ ИТ-ИНФРАСТРУКТУРА НЕПРЕРЫВНОСТИ НЕ ОБЕЩАЕТ ОТСУТСТВИЯ АВАРИЙ. ПРИ ИХ НАСТУПЛЕНИИ ОНА ОБЕСПЕЧИВАЕТ НЕПРЕРЫВНОСТЬ БИЗНЕС-ПРОЦЕССОВ

Почему система продолжает работать при отказах

Современная инфраструктура работает потому, что честно учитывает реальные условия эксплуатации современных приложений. Отказы отдельных компонентов, изменения конфигураций и обновления происходят постоянно, и архитектура рассчитана именно на это.

Ключевое решение — автономные зоны доступности без единого центра. В схеме используется конфигурация из трех ЦОД. Это практический инженерный компромисс. Система сохраняет работоспособность при отказе одной площадки и позволяет выполнять плановые работы. В схеме три независимых ЦОД, но количество зон доступности может быть и больше трех.

Второй важный принцип — наблюдаемость. В первую очередь важно видеть, что приложение корректно отвечает и выполняет свою бизнес-функцию, а не просто формально «работает». Мониторинг нижележащей инфраструктуры и сети в этом случае является вспомогательным инструментом, позволяющим быстрее диагностировать причины проблем, но не подменяет контроль за состоянием самого сервиса.

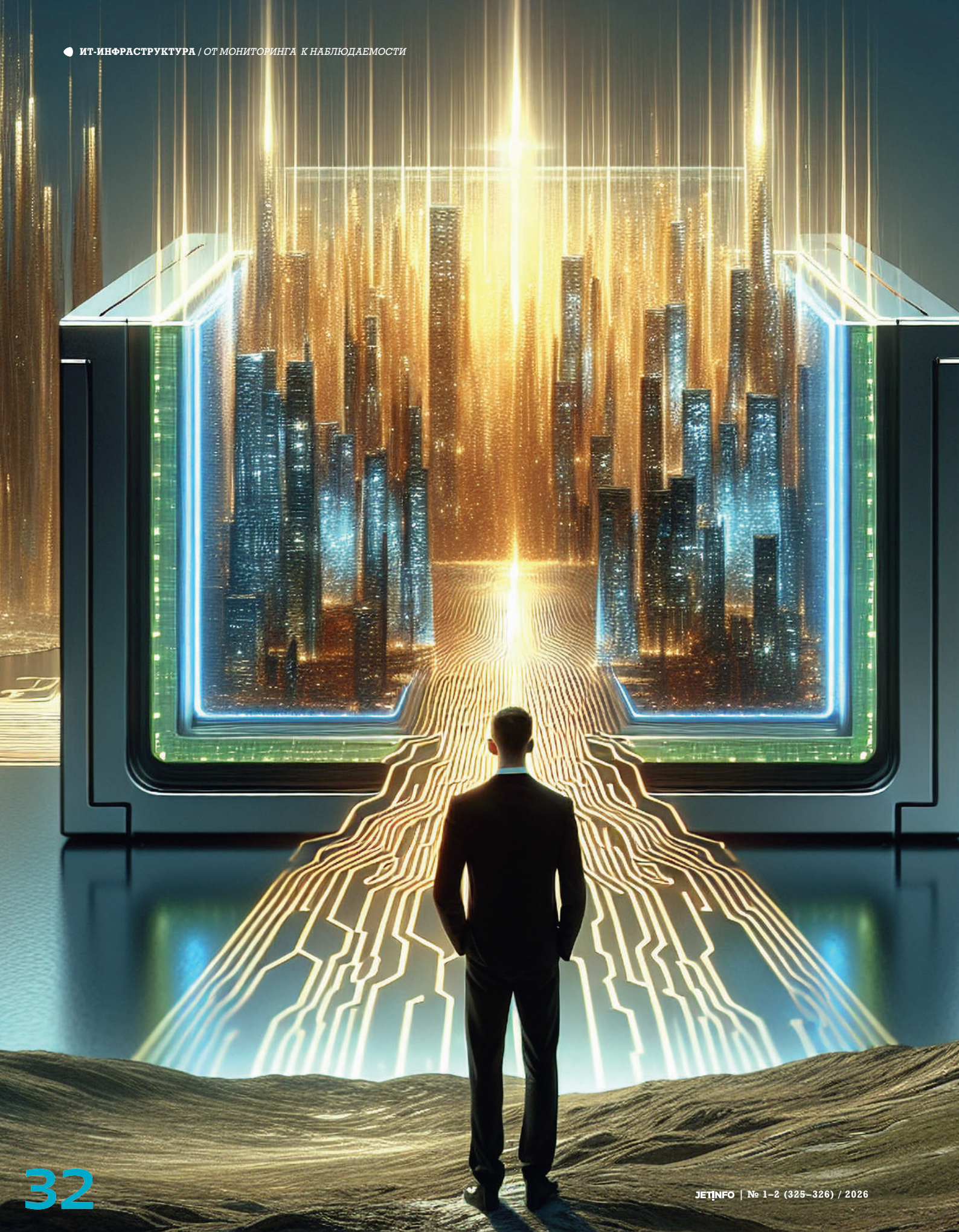
Отдельно стоит отметить адаптивность как ключевое свойство такой архитектуры. Сбой рассматривается не как катастрофа, а как источник информации. Команда сопровождения должна не только устранять аварии и писать post-mortem, но и проактивно учиться на этих инцидентах. Это предполагает внедрение в повседневную работу современных практик, таких как Chaos Engineering и SRE. Авария системы становится поводом для улучшения как технических решений, так и процессов эксплуатации.

Третий важный принцип — пересоздание вместо восстановления. Контейнерная оркестрация и подход Infrastructure-as-Code делают описание системы более важным в сравнении с конкретными экземплярами ресурсов. Потеря отдельного компонента перестает быть инцидентом, требующим ручного вмешательства, и обрабатывается автоматически в рамках заданной модели.

Немаловажным фактором является и киберустойчивость. Цель современных атак — не нарушение конфиденциальности, а остановка бизнеса путем удаления или шифрования данных. Поэтому для обеспечения киберустойчивости реализуются сразу две взаимодополняющие концепции. Первая — внедрение средств информационной безопасности на всех этапах жизненного цикла приложения ***(от разработки до эксплуатации в продуктивном ландшафте)***. Вторая — использование автономных, не связанных между собой систем резервного копирования в каждом ЦОД и дополнительная передача резервных копий данных в другую зону доступности в режиме «только чтение» ***(WORM)***.

Такой подход позволяет максимально защитить приложения и обеспечить оперативное и гарантированное восстановление сервисов в случае катастрофических сценариев.

Современная ИТ-инфраструктура непрерывности не обещает отсутствия аварий. При их наступлении она обеспечивает непрерывность бизнес-процессов. И поэтому такая архитектура постепенно становится базовой моделью для современных ИТ-систем.



ОТ МОНИТОРИНГА К НАБЛЮДАЕМОСТИ

КАК СДЕЛАТЬ ЧЕРНЫЙ ЯЩИК ПРОЗРАЧНЫМ

Чем крупнее бизнес, тем сложнее его ИТ-инфраструктура и серьезнее последствия инцидентов. В какой-то момент становится понятно: традиционный мониторинг работы систем не позволяет предотвращать нежелательные события. Требуется внедрять практику наблюдаемости: это кардинально повышает прозрачность процессов, что позволяет с легкостью находить и устранять ключевые проблемы. В каких случаях стоит использовать такой подход и как сделать это правильно, оправдав необходимые затраты? Ответы — в нашей статье.

- Системы усложняются — мониторинг не справляется
- Три столпа наблюдаемости: метрики, логи, трейсы
- Без мониторинга невозможно вовремя узнать о существовании проблемы, а без наблюдаемости — понять, как ее решить

ЭКСПЕРТ
Дмитрий Унтила,
СРО «Пульта» и «Графини»

ЭКСПЕРТ
Алексей Акопян,
руководитель отдела систем мониторинга компании «Инфосистемы Джет»

ЭКСПЕРТ
Юрий Пирогов,
руководитель направления Observability X5 Digital

ЭКСПЕРТ
Даниэль Халиулин,
технический менеджер платформы Monium (команда Yandex Infrastructure)

Инструменты не успевают за объемами?

Мировой объем генерируемых данных уже давно растет двузначными темпами, что стимулирует активное расширение ИТ-инфраструктуры. К тому же новая информация все чаще создается за счет использования распределенных сред, а их контроль требует иных методов в сравнении с традиционными монолитными приложениями.

Алексей Акопян

«Привычные инструменты уже не в состоянии обрабатывать такой объем данных и не предоставляют достаточной информации о состоянии приложений, позволяющей быстро понять, как исправлять возникающие проблемы. Как правило, традиционный мониторинг может оперативно зафиксировать нарушение, но сегодня этого уже недостаточно. Важно не только обнаружить поломку, но и предупредить ее возникновение, а также скорректировать системы, чтобы ситуация не повторилась».

Такая проактивность обеспечивается благодаря подходу, который получил название «наблюдаемость» ***(англ. — observability)***.

Здесь могут возникнуть вопросы:

- Где проходит граница между мониторингом и observability?
- В каких случаях нужна наблюдаемость, а когда достаточно мониторинга?

Последовательно разберемся с каждым из этих двух подходов.

Мониторинг оперирует неким набором критериев, которые заведомо известны, и именно поэтому их можно отслеживать, а еще решает целый ряд задач:

- обнаруживает отказы и деградации;
- контролирует состояние сервисов и инфраструктуры в реальном времени;
- сигнализирует о проблеме;
- сокращает время до обнаружения инцидента.

Норма инцидентов

Мониторинг также позволяет понять, какую работу сервисов можно считать приемлемой. В этом помогают три составляющие: SLA ***(обещанный уровень работы сервиса)***, SLO ***(целевые показатели)*** и SLI ***(конкретные измеряемые показатели)***.

Алексей Акопян

«Мониторинг системы задает норму качества через SLA, SLO и SLI. Недостаточно сказать, работает система или нет. Через SLO определяются конкретные показатели, показывающие насколько хорошо она функционирует. И именно на основе SLO рассчитывают бюджет ошибок (допустимое количество сбоев за определенный период) и приоритизируют работу инженеров по устранению аварий».

Благодаря правильно настроенному мониторингу удается максимально быстро обнаружить и локализовать проблему, а также получить общий срез работы системы, что дает возможность составить картину для проведения диагностики. В результате специалисты могут минимизировать время восстановления ***(MTTR — Mean time to repair)***.

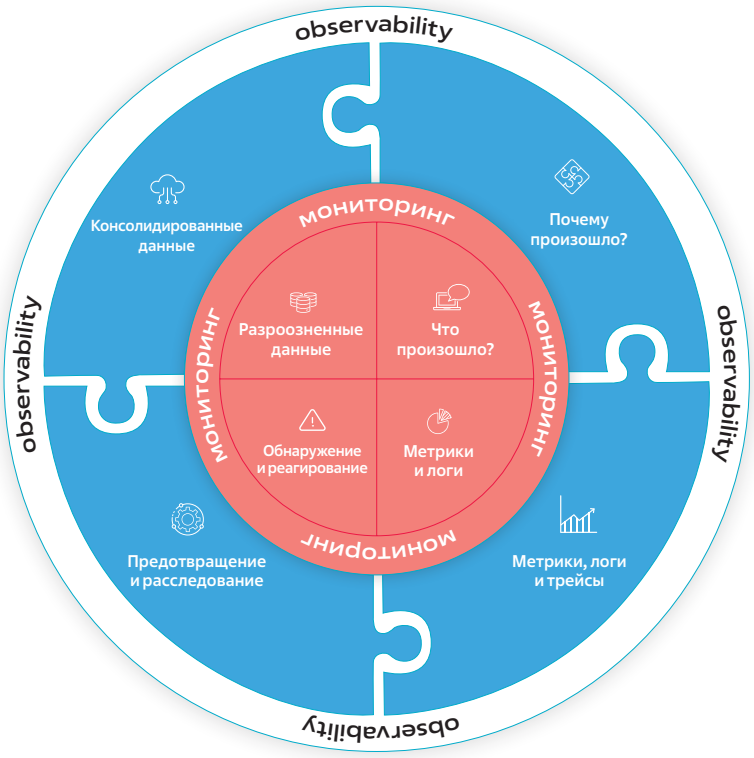
Алексей Акопян

«Верная настройка мониторинга позволяет управлять алертами, снижая уровень “шума” за счет сокращения количества бесполезных показателей и повышения точности сигналов. Это одно из условий эффективности мониторинга. Избыток информации (система постоянно сигнализирует об опасности тогда, когда ее в действительности нет) может привести к тому, что по-настоящему опасный сигнал на этом фоне будет проигнорирован».

«Почему это сломалось?»

Наблюдаемость принципиально отличается от мониторинга. Здесь тоже не обойтись без отслеживания данных, но основа метода другая: система, анализируя эту информацию, способна «рассказать» о своем внутреннем состоянии так, что инженер может понять, что с ней происходит.

То есть, имея некий черный ящик, куда невозможно проникнуть, мы должны делать выводы о его работе на основании того, как он реагирует на входящие в него сигналы. По этим реакциям предстоит понять, что находится внутри, как это работает, правильно ли оно функционирует и как исправить нарушения.



Не инструмент, но подход

Как правило, observability внедряют не ради собираемых данных, а для решения конкретной проблемы. И в этом отличие наблюдаемости от мониторинга. Мониторинг отвечает на вопросы, сломалось или нет, что сломалось, когда сломалось, сколько раз сломалось. А observability позволяет выяснить, почему это сломалось. Причем наблюдаемость дает возможность найти проблему даже в случае, когда в компании не знают, где она может быть локализована и что собой представляет.

Именно поэтому наблюдаемость позволяет решить проблему до того, как она станет инцидентом. Такую проактивность позволяют обеспечивать следующие функции:

- выявление деградации до момента отказа благодаря контролю изменений в поведении сервисов;
- предоставление контекста вместо разрозненных сигналов — за счет корреляции метрик, логов, трейсов и привязки сигналов к бизнес-контексту;
- прогнозирование поведения сложных систем при обнаружении неожиданных состояний и новых типов сбоев до того, как они станут массовыми;
- обеспечение автоматизации действий *(runbook automation)* на основе сигналов.

Юрий Пирогов

«Понятие observability шире, чем только метрики, логи и трейсы. Это методология работы с телеметрией процессов и их автоматизацией. В ее рамках обеспечиваются управление алертами, инцидент-менеджмент, инвентаризация и планирование ресурсов серверов. При этом телеметрия должна предоставляться в виде, удобном для каждого из потребителей — от инженеров и аналитиков до кибербеза».

Реализация observability позволяет видеть любые отклонения в работе систем, поскольку фиксируются все события и изменения. Благодаря этому удается выстроить зрелый процесс инцидент-менеджмента и сократить потери бизнеса.

Методология наблюдаемости широко применяется в компании «Яндекс». Сетевые инженеры и аналитики с помощью observability-платформы Monium в реальном времени отслеживают динамику конверсий и оценивают эффективность ключевых бизнес-сценариев. В компании отмечают, что практики observability внедрялись постепенно и прошли путь от базовых инструментов к единой платформе, которой сегодня пользуются более 16 тысяч сотрудников «Яндекса». Развитием платформы занимается команда Yandex Infrastructure — подразделение, отвечающее за дата-центры, сетевую инфраструктуру, распределенные хранилища данных, платформы разработки и деплоя, а также решения для машинного обучения.

Даниэль Халиулин

«Наша платформа observability помогла компании обрести “глаза”: инженеры и бизнес-команды научились лучше понимать работу распределенных систем. Новая информация значительно обогатила контекст, на основе которого принимаются решения о развитии наших продуктов. Такие концепции, как SLO (целевой уровень обслуживания, service level objective) и бюджет ошибок, позволили на уровне всей компании сделать понятными ожидания бизнеса и инженерных команд относительно ключевых показателей работы систем».

Единая observability-платформа и выстроенные практики повышают надежность систем: сбои удается обнаруживать и устранять быстрее. Снижается и нагрузка на инженеров — теперь им реже приходится переключаться между разрозненными инструментами

МЕТРИКИ

- Дают представление о форме и масштабе проблемы
- Используются как инфраструктурные, так и прикладные/пользовательские метрики
- Сигнализируют «что-то пошло не так», но не объясняют почему

БИЗНЕС-КОНТЕКСТ

- Дает возможность выделить важные для наблюдаемости факторы путем оценки таких параметров, как успешность транзакций, потери дохода или затронутые сегменты пользователей
- Позволяет понять реальный ущерб от инцидента

ТРЕЙСЫ

- Позволяют увидеть узкие места, понять, где возникает задержка, отличить причину от симптома
- Самый ценный тип данных для неизвестных проблем

ЛОГИ

- Обеспечивают наличие контекста (trace_id, user_id, order_id и т. д.)
- Отвечают на вопрос: что именно произошло в коде в конкретный момент?

СОБЫТИЯ

- Дают временной и причинный контекст
- Представляют собой деплои (англ. deploy — «развертывание», размещение программного обеспечения), конфигурационные изменения, масштабирование, аварийные переключения и пр.
- Позволяют оценить, совпадают ли «неизвестные» проблемы с изменениями

ИНСТРУМЕНТЫ ДЛЯ OBSERVABILITY

С открытым исходным кодом

OpenTelemetry — стандарт и набор инструментов для сбора и передачи телеметрии

Prometheus — система мониторинга для работы с временными рядами данных

Zabbix — система мониторинга состояния серверов, сетевого оборудования и приложений

Grafana — платформа для визуализации данных и алертинга

Loki — система агрегации и хранения логов

Tempo/Jaeger — инструменты для трассировки распределенных систем

Коммерческие российские продукты

«Пульт» — система мониторинга ИТ-инфраструктуры

«Графиня» — платформа для сбора, мониторинга и визуализации данных

Gmonit — универсальная система мониторинга, управления метриками, событиями, логами и трейсами с использованием ИИ

Proto Observability Platform — платформа наблюдаемости и аналитики операционных данных

Smart Monitor — универсальная платформа для сбора и анализа машинных данных

Monq — all-in-one — платформа наблюдаемости, мониторинга и автоматизации

мониторинга, что дополнительно ускоряет реакцию на инциденты. «Яндекс» использует платформу Monium не только для внутренних задач: решение проходит апробацию и у внешних пользователей, включая «ОТП Банк» и одну из крупных FMCG-компаний.

За хлебом на джипе?

Дмитрий Унтила

«Главное для построения проактивной работы с ИТ-инфраструктурой — взаимодополняемость мониторинга и observability. Эти подходы не являются альтернативными или конкурирующими. Они представляют собой части одного процесса: мониторинг фиксирует проблему, observability позволяет расследовать инцидент и предотвратить его повторение».

Однако применять observability следует далеко не всегда, поскольку это более сложный, а значит, и более дорогостоящий подход по сравнению с базовым мониторингом. Их стоимость может различаться на порядки, поэтому необходимо вовремя уловить момент, когда мониторинга становится недостаточно.

Дмитрий Унтила

«Это как с автомобилями: если машина вам нужна, чтобы пару раз в неделю

закупаться в гипермаркете, до которого полчаса езды по ровной городской улице, то использовать для этого Land Rover или Geländewagen нерационально. Ну а там, где вместо асфальта ямы и буреломы, без внедорожника не обойтись. Как правило, observability требуется в случаях, когда цена ошибки перекрывает стоимость самой наблюдаемости».

Как же определить, что уже пора «брать джип»? Самое время — если:

- корпоративная ИТ-инфраструктура построена не как монолитное приложение с ограниченным набором серверов, а включает микросервисы и сервисно-ориентированные архитектуры, облачные платформы и гибридные среды, контейнеризацию и оркестрацию;
- в компании активно используются интеграция внешних сервисов, API сторонних поставщиков, SaaS-сервисы, платежные шлюзы, сервисы аутентификации и облачные хранилища;
- бизнес требует быстрой доставки новых функций, высокой доступности, отказоустойчивости, безопасности и соответствия стандартам.

ПОШАГОВАЯ СХЕМА ВНЕДРЕНИЯ OBSERVABILITY

ШАГ 1. Определить, что считается нормой для бизнеса

Чтобы понять, какую работу сервисов можно считать приемлемой, необходимо:

- выявить 3–5 критических пользовательских сценариев *(login, checkout, search, API call)*;
- понять, что для них означает «работает хорошо»;
- использовать критерии этого «хорошо» как основу для observability.

ШАГ 2. Ввести SLI/SLO — это основа observability

- Требуются минимум 1–2 SLI на сервис. Например: время отклика *(p95/p99)* и уровень ошибок.
- Начните с простого SLO. Например: «99,9% запросов выполняются быстрее 300 мс за 30 дней».
- Корректные SLO формируются на основе опыта и требуют постоянной адаптации с учетом изменений бизнеса.

ШАГ 3. Стандартизировать сбор данных — без этого алерты не будут связаны между собой

Например:

- использование OpenTelemetry;
- единый формат логов *(JSON)*;
- единые система наименования и разметка метрик.

ШАГ 4. Построить базовую «тройку»: метрики, трейсы, логи

Пример их конфигурации:

Метрики:

- RED/Golden Signals *(ключевые метрики: rate, errors, duration)*;
- p95/p99 *(процентили времени отклика)*;
- насыщенность ресурсов *(saturation: очереди, пулы)*.

Трейсы:

- end-to-end *(сквозные трассировки)*;
- минимум: вход → ключевые зависимости;
- разумная выборка *(sampling)*.

Логи:

- структурированные;
- баланс между длительностью хранения, скоростью получения данных и утилизации хранилищ.

ШАГ 5. Сделать алерт точкой входа в observability

Признаки хорошего алерта:

- основан на SLO;
- содержит данные о том, что сломалось, кого затронуло и куда смотреть дальше;
- содержит ссылки на SLI-дашборд, проблемную трассировку, логи.

Если алерт нельзя исследовать за 2–3 клика, он неэффективен.

Шаг 6. Алертить симптомы, а не причины

Причины следует искать через observability.

Плохие алерты:

- загрузка CPU выше 80%;
- перезапуск подов.

Хорошие алерты:

- у checkout замедлилось время отклика (p99 выше SLO);
- ошибки 5xx возникают у 5% пользователей.

Шаг 7. Встроить observability в процесс релизов

Каждый релиз — потенциальный инцидент. Observability должна отвечать на вопрос: этот релиз ухудшил систему или нет?

Практики:

- сравнение метрик до/после;
- корректировка SLI/SLO.

Шаг 8. Использовать инциденты для улучшения

Каждый инцидент должен приводить к аудиту observability.

Пример разбор инцидента:

- каких сигналов не хватало;
- какой алерт должен был сработать раньше;
- какой контекст был потерян.

Шаг 9. Назначить владельца процесса

Observability — это процесс, у которого должен быть ответственный.

В управление процессом входят:

- регулярный пересмотр алертов;
- адаптация SLO с учетом изменений бизнеса;
- введение общих принципов для всех команд.

Оценивать эффективность работы системы эксперты советуют от противного — исходя из отсутствия перечисленных ниже признаков:

- Специалисты не могут за пять минут понять, почему количество ошибок выросло в несколько раз.
- Логи разрознены, а также нет trace-id *(либо они не совпадают между сервисами)*.
- Существующие дашборды не удается полноценно использовать — на них отображаются данные, которые не имеют особой ценности.
- При наступлении инцидента команда предпринимает хаотичные действия, пытаясь попасть в цель.
- Специалисты не понимают, что делать с получаемыми алертами.
- Команде неизвестны структура системы и назначение ее компонентов.
- Главная цель ИТ-команды — не решить задачу, а найти сотрудника, на которого можно возложить ответственность за провал.

Разумеется, необходимо соотносить затраты на построение системы наблюдаемости с отдачей от ее использования. В «Яндексе» придерживаются схожего подхода: в качестве ключевых ориентиров используют метрики семейства MTTx *(Mean Time To X)* — показатели, отражающие время прохождения основных этапов работы с инцидентами: от обнаружения *(MTTD)* до восстановления *(MTTR)* и других стадий. Среди основных издержек выделяют расходы на инфраструктуру, а также затраты на работу инженерной команды, которая отвечает за поддержку и развитие observability-системы.

Даниэль Халиулин

«По нашему мнению, подходы observability превосходят традиционные как с точки зрения получаемой ценности, так и в плане затрат. Бизнес повышает надежность

ИТ и усиливает прозрачность процессов, получая дополнительный контекст для принятия решений. Затраты при этом оптимизируются: больше не нужно поддерживать зоопарк разных решений».

Одна из наиболее сложных задач, с которыми столкнулись специалисты X5 Digital при внедрении observability, — незаметная для пользователей смена стека. Для ее решения требовалось выстроить работу в трех направлениях:

1. Управление сбором телеметрии, которое производится в компании с помощью инструментов непрерывной доставки и развертывания ***(continious delivery & deployment)*** и клиентских библиотек для продуктовых сервисов. При этом большая часть алертов и дашбордов создается в автоматическом режиме.

2. Контроль жизненного цикла правил алертов, за что отвечает отдельный сервис, с помощью которого происходит автоматизация управления правилами и аудита изменений в них ***(к этому процессу в том числе подключаются автогенераторы)***.

3. Высокая точность срабатывания алертов, которая достигается за счет собственной разработки компании — инструмента, динамически изменяющего уровни их срабатывания на основе собранных метрик нагрузки на сервисы в конкретное время.

Собственные решения в X5 Digital, в частности, используют для того, чтобы снизить риск попадания чувствительных данных в хранилища логов, а также заменить часть зарубежных компонентов open source в соответствии с требованиями кибербезопасности. После внедрения observability у сотрудников появился более полный обзор происходящего с сервисами во время инцидентов: стали доступными данные об изменениях, релизах, срабатываниях алертов и других событиях.

Юрий Пирогов

«Мы применяем превентивный подход — заранее прорабатываем алерты, срабатывание которых предупреждает инциденты, а не реагируем на них постфактум. Затем покрытие сервисов такими алертами автоматизируется и контролируется поддержкой и инцидент-менеджерами. При этом мы предоставляем разработчикам библиотеки и средства автоматического создания дашбордов по шаблонам алертов. В результате внутренняя команда не тратит время на ручную настройку».

Все только начинается

Выстраивая систему наблюдаемости, необходимо понимать, что ее работа подразумевает гибкую, постоянно меняющуюся архитектуру. Например, искусственный интеллект все активнее внедряется в мониторинг и observability. Платформы используют ИИ для анализа телеметрии: умной корреляции событий и снижения шума алертов, автоматического выявления аномалий и прогнозирования проблем, помощи в поиске первопричин аварий.

По мере усложнения распределенных систем и интеграций все больше внимания уделяется безопасности: системы сигнализируют об аномалиях, нарушениях политик, уязвимых маршрутах и т. д. Ожидается, что в ближайшие годы мониторинг будет эволюционировать, усложняться, становиться более эффективным и постепенно переходить в наблюдаемость.

Возможно, через несколько лет компании вовсе перестанут разграничивать два этих подхода, считая их составляющими единого процесса, необходимого любой ИТ-инфраструктуре.

Значимость темы observability для российского рынка подтверждается и интересом к ней профессионального сообщества. Так, в 2026 году впервые в России прошло отраслевое мероприятие, полностью посвященное вопросам построения наблюдаемости в организациях. Конференция Observability, прошедшая 19 марта в Москве, собрала 300 участников офлайн и более 2000 зрителей в олайн-формате.

В рамках события также была организована выставка ведущих производителей отечественного софта: Т-банк, Monq, Wisla, «Инфосистемы Джет» и «Лаборатория Числитель» с продуктом «Пульт» представили инновационные решения и провели живые демонстрации, позволив участникам на практике оценить их надежность и функциональность. Конференция имеет все шансы стать ежегодным событием и занять заметное место в повестке российского ИТ-сообщества.

ИЛЛЮЗИЯ БЕЗОПАСНОСТИ

ЗАЩИТА РОССИЙСКОЙ ПЛАТФОРМЫ ВИРТУАЛИЗАЦИИ ОТ КАТАСТРОФ И КИБЕРУГРОЗ

Платформы виртуализации — стратегическая основа каждой ИТ-инфраструктуры и цифровой экономики в целом. Именно поэтому чрезвычайно важно обеспечить им качественную защиту, причем с использованием отечественных решений. Изначально российские системы виртуализации уступали продуктам ушедших иностранных вендоров по функциональности, однако за последние четыре года наш рынок прошел путь, на который в иных условиях, возможно, потребовалось бы десятилетие.

ЭКСПЕРТ

Дмитрий Горохов,

директор департамента виртуализации и контейнеризации компании «Инфосистемы Джет»

Если в 2022 году компании стремились хотя бы просто запустить рабочие процессы на базе отечественного ПО, то сегодня приоритеты сместились: главной задачей стало обеспечить непрерывность бизнеса и создать для него глубокую эшелонированную защиту. Став основой критической инфраструктуры, Basis Dynamix, zVirt, SpaceVM и другие платформы виртуализации оказались приоритетной целью для киберпреступников и главными потенциальными жертвами техногенных катастроф. Сбой гипервизора, нарушение целостности данных на уровне репликации и другие неисправности чреваты остановкой сервисов и потерей данных с фатальными последствиями. Поэтому вопросы устойчивости, защиты и восстановления бизнес-систем требуют комплексного подхода и учета специфики российского ИТ-ландшафта.

Тем не менее многие компании до сих пор живут в иллюзии безопасности, полагая, что стандартный отказоустойчивый кластер полностью обеспечивает их защиту. Однако практика показывает иное: он спасает лишь при выходе из строя отдельного сервера. Обычных механизмов виртуализации окажется недостаточно в случае аварии на уровне всего дата-центра или проникновения в сеть вируса-шифровальщика. Именно поэтому успешная защита платформы виртуализации сегодня — это баланс между катастрофоустойчивостью и кибербезопасностью.

Три сценария аварийного восстановления

При пожаре, масштабном отключении питания, сбое ключевой системы хранения данных или ином катастрофическом сценарии, в результате которого «падает» весь ЦОД, главными метриками становятся RPO *(Recovery Point Objective — максимальный период времени, за который могут быть потеряны данные в случае сбоя)* и RTO *(Recovery Time Objective — максимальное время на восстановление системы до работоспособного состояния)*.

В своем выступлении на прошедшей конференции IT Elements Дмитрий Горохов, директор департамента виртуализации и контейнеризации компании «Инфосистемы Джет», представил три основных сценария построения инфраструктуры аварийного восстановления *(Disaster Recovery, DR)* для российских платформ в зависимости от критичности сервисов, бюджета и требований к RPO и RTO.

Первый сценарий — это **программная репликация**, которая реализуется безагентским способом на уровне гипервизора или с помощью агента, установленного внутри гостевой операционной системы. Такой подход применим для каналов с ограниченной пропускной способностью. К его ключевым преимуществам относятся независимость от аппаратного обеспечения в инфраструктуре *(например, от систем хранения данных)* и гибкость настроек для каждой виртуальной машины. Главными же недостатками являются невозможность

обеспечить сохранность данных в случае аварии и необходимость переключаться на резервную копию виртуальной машины.

По словам эксперта, сценарий программной репликации реализован в таких отечественных продуктах, как Mind Replication от компании Mind Software и Hystax Acura от одноименной компании. Также возможности платформы виртуализации zVirt от компании Orionsoft позволяют настроить асинхронную репликацию виртуальных машин между площадками.

Аппаратная репликация выполняется на уровне СХД и может быть как синхронной, так и асинхронной. Такой сценарий обеспечивает максимальную производительность и минимальный показатель RPO, однако для его реализации необходим ряд условий: одинаковые СХД в обоих ЦОД, установленная на них лицензия на функциональность репликации и поддержка управления со стороны платформы виртуализации. На российском рынке подобную интеграцию поддерживают платформы zVirt и HostVM, «РЕД Виртуализация», ROSA, функциональность которых находится в активной стадии развития.

Наконец, третий сценарий — **метрокластер** — предполагает использование «растянутой» инфраструктуры с синхронной репликацией данных в удаленных друг от друга СХД. Реализовать его можно как на аппаратных СХД, так и на программных *(например, в составе платформы виртуализации «Киберинфраструктура», «Росплатформы» или связки Proxmox + Ceph)*. В этом случае значения RTO и RPO можно свести практически к нулю, используя автоматическое переключение между площадками. Тем не менее внедрение метрокластера сопряжено со сложностью настройки и строгими требованиями к каналам связи, включая поддержку L2-связности между серверами и задержку передачи данных менее 5 мс.

Дмитрий Горохов

«Правильно настроенный метрокластер позволяет отрабатывать множество отказов вплоть до автоматического перезапуска нагрузок в резервном ЦОД. Split-Brain —самый частый и одновременно самый сложный сценарий отказа, при котором две площадки теряют связь друг с другом, но продолжают работать. Чтобы система корректно восстановила свою работу, критически важно подключать внешнего “свидетеля” (Quorum/Witness). Это виртуальная машина или сервер с установленным ПО на третьей независимой площадке, которые решают, какая из сторон останется активной, а какая перестанет функционировать».

Эксперт напомнил, что пока существует лишь одна отечественная система хранения данных с поддержкой метрокластера — AeroDisk. Кроме того, отсутствует поддержка Fibre Channel, что сужает выбор протоколов передачи данных — преимущественно до iSCSI. Технология NVMe over TCP, которая позволяет использовать стандартные Ethernet-каналы для доступа к быстрым SSD-массивам на обеих площадках, также пока не получила широкого распространения в России. И общий выбор СХД с полной функциональностью для построения сложных DR-сценариев остается ограниченным.

Когда враг уже внутри

Ландшафт угроз стремительно меняется: сегодня злоумышленники не ограничиваются попытками прорыва периметра, а целенаправленно атакуют саму среду управления виртуализацией. Успешное похищение учетных данных администратора

Многие компании до сих пор живут в иллюзии безопасности, полагая, что стандартный отказоустойчивый кластер полностью обеспечивает их защиту. Однако практика показывает иное: он спасает лишь при выходе из строя отдельного сервера

фактически обеспечивает преступникам контроль над всей ИТ-инфраструктурой.

Дмитрий Горохов подчеркнул, что все более актуальными становятся атаки трех типов. Ключевым и наиболее популярным методом проникновения остается компрометация учетных данных администратора, что открывает злоумышленнику прямой путь к сервисам централизованного управления. Однако не менее опасным является сценарий попадания внутрь гостевых операционных систем, после чего атакующий начинает скрытое перемещение между виртуальными машинами. В этой ситуации платформа виртуализации должна выступать не просто как среда исполнения, а как активный инструмент защиты, предоставляя механизмы микросегментации для блокировки подобных перемещений. При этом важно помнить и об атаках на системы резервного копирования *(СРК)*: шифруя или удаляя бэкапы, злоумышленники лишают компанию возможности быстрого восстановления.

Для противостояния угрозам необходим комплекс мер. Во-первых, это харденинг российских платформ, которые часто базируются на Linux-дистрибутивах *(Astra Linux, РЕД ОС, Rosa)*. В этом случае отключают все неиспользуемые сервисы и применяют механизмы контроля целостности и мандатного управления доступом, чтобы минимизировать поверхность атаки. Для гарантии неизменности исполняемых файлов и конфигураций не менее важен и контроль целостности виртуальных машин. Для защиты от низкоуровневых атак необходимо внедрить Secure Boot, а для защиты BIOS/UEFI — аппаратно-программный модуль доверенной загрузки *(АПМДЗ)*. И наконец, централизованный сбор логов обеспечивает оперативное реагирование и расследование инцидентов благодаря передаче всех событий безопасности в SIEM-систему в реальном времени.

Настоятельно рекомендуется выполнить микросегментацию через программно-определяемые сети *(Software Defined Network)*, чтобы изолировать отдельную виртуальную машину или группу виртуальных машин и тем самым предотвратить распространение атаки за пределы скомпрометированного сегмента. Такой подход реализует концепцию нулевого доверия *(Zero Trust)*. Наряду с этим необходимо настроить управление привилегиями *(PAM)*. Доступ к консоли управления должен осуществляться только через защищенные шлюзы с обязательной двухфакторной аутентификацией *(2FA)*. Также стоит настроить систему резервного копирования, основываясь на практиках построения ее защищенных контуров. Важно учитывать и требования регуляторов.

Дмитрий Горохов

«Приказ ФСТЭК № 117, вступивший в полную силу 1 марта 2026 года, ужесточает требования к защите государственных информационных систем и объектов критической инфраструктуры в виртуальной

среде. Для таких систем необходимо использовать сертифицированные ФСТЭК версии платформ виртуализации или применять наложенные сертифицированные средства защиты. Тем не менее мы настоятельно рекомендуем применять не только сертифицированные версии, но и лучшие практики по построению защиты и харденинга платформы виртуализации».

Сколько стоит спокойствие?

Зачастую компании считают полноценное решение Disaster Recovery баснословно дорогим и поэтому отказываются от него. Но сомнения в необходимости DR-инфраструктуры, как правило, отпадают, если сопоставить общую стоимость владения резервной площадкой с потенциальными убытками от часа простоя систем, включающими прямые потери ***(недополученная прибыль, штрафы от регуляторов и клиентов)*** и косвенные ***(репутационный ущерб, падение акций, затраты на восстановление данных и расследование инцидентов)***.

Дмитрий Горохов

«Защита информационных систем и инфраструктуры от катастрофы требует значительных затрат. Чем меньше данных мы можем потерять и чем быстрее должны провести восстановление, тем дороже будет стоить такое решение. Но игнорировать подобные риски нельзя. Рассмотрите доступные вам сценарии защиты ключевых систем, чтобы бизнес мог восстановить работу при возникновении отказа вплоть до уровня ЦОД».

ИИ и автономная защита

Скорость кибератак быстро растет, а возможности нашей реакции небезграничны, поэтому логично, что следующим шагом в развитии отечественных платформ виртуализации станет глубокая интеграция ИИ-модулей для прогностического анализа сбоев. Это позволит предсказывать сбой оборудования до его фактического отказа и проводить превентивную миграцию виртуальных машин.

Искусственный интеллект можно задействовать и в поведенческом анализе: он станет автоматически выявлять аномальную активность администраторов и виртуальных машин ***(например, внезапное начало массового шифрования файлов)***, а затем — немедленно изолировать подозрительный сегмент. Системы автономного восстановления смогут самостоятельно принимать решения о переключении на резервную копию при обнаружении деструктивной активности вредоносного ПО.

Четыре вопроса к вашей стратегии

Как подчеркнул Дмитрий Горохов, защита бизнес-систем от катастроф — это непрерывный процесс. Чтобы оценить степень готовности к восстановлению и эффективной отработке сценариев после сбоя, необходимо регулярно проводить тесты и учебные восстановления в резервные ЦОД или из резервных копий, руководствуясь четким DR-планом. Крайне важно, чтобы команда эксплуатации была обучена и умела пользоваться таким планом, поддерживая его в актуальном состоянии.

Кроме того, чтобы минимизировать риски информационной безопасности, необходимо постоянно проверять актуальность и достаточность всех настроенных механизмов ИБ, а также их способность защищать инфраструктуру от текущих угроз.

В итоге, чтобы понять степень готовности инфраструктуры компании к новым вызовам, следует ответить на четыре вопроса: протестирован ли DR-план в реальности, настроена ли двухфакторная аутентификация, есть ли неизменяемые копии данных и каковы реальные RPO/RTO.

Дмитрий Горохов

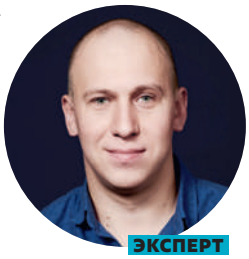
«Российская виртуализация уже готова к промышленной эксплуатации, однако нужно правильно выбрать продукт из доступных на рынке решений и вдумчиво подойти к его использованию. Применяйте базовые аспекты защиты (изоляция сети управления, 2FA, харденинг) и проводите учения по восстановлению системы в случае аварии».

В условиях дефицита кадров выигрывают компании, которые внедряют системы автоматизированного реагирования на инциденты и регулярно проводят восстановительные тесты. Только так, по мнению эксперта, российская платформа виртуализации станет не просто импортозамещающим продуктом, а надежным фундаментом для вашей ИТ-инфраструктуры.


A121205
220 0490380 01
HF

ПОСЛЕДНИЙ ОБОРОНИТЕЛЬНЫЙ РУБЕЖ

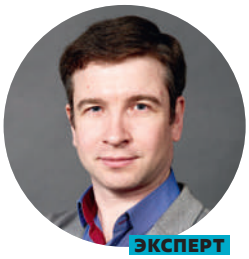
КАК СИСТЕМЫ РЕЗЕРВНОГО КОПИРОВАНИЯ СПАСУТ БИЗНЕС ПОСЛЕ КИБЕРАТАКИ



ЭКСПЕРТ

Игорь Шконда,

руководитель направления систем резервного копирования компании «Инфосистемы Джет»



ЭКСПЕРТ

Олег Кандальцев,

старший инженер-проектировщик систем хранения данных компании «Инфосистемы Джет»

В реалиях цифровой экономики данные компаний — один из наиболее ценных активов, который находится под постоянной угрозой. Число глобальных кибератак с использованием программ-вымогателей (ransomware), особенно шифровальщиков, продолжает расти, как и их сложность. Так, согласно исследованию аналитической фирмы Comparitech, в 2025 году оно увеличилось на 32%, а в опросе компании Veeam Software 89% организаций заявили, что целью хакеров были репозитории резервных копий. Кроме того, безопасности данных угрожают сбои оборудования и непреднамеренные ошибки сотрудников.

В таких условиях классические подходы к резервному копированию уже не работают, а его система *(CPK)* из обычного хранилища файловых копий превращается в важнейший и последний оборонительный рубеж. Теперь это не просто инструмент для копирования данных, а комплексное решение, которое обеспечивает способность восстановить всю ИТ-инфраструктуру — от операционных систем и приложений до бизнес-процессов. Ни один другой ее элемент не воскресит данные после атаки шифровальщиков — CPK защищает их именно от логической порчи.

Концепция «Last Resort Backup» *(резервная копия последней надежды)* выходит в ИТ-тренды, потому что подразумевает создание не просто еще одной копии, а защищенного, проверенного и изолированного бэкапа. Он заточен под то, чтобы выжить, даже когда пробиты все предыдущие уровни защиты. И порой CPK требует большей устойчивости, чем продуктивные системы, причем обеспечивать ее нужно, принимая как технические, так и организационные меры.

О том, почему у компаний возникает ложное чувство защищенности и какие практики построения CPK самые эффективные, рассказали на прошедшей конференции IT Elements эксперты компании «Инфосистемы Джет».

CPK как залог непрерывности бизнеса

Компании до сих пор уповают на то, что наличие резервных копий само по себе является залогом быстрого и успешного восстановления данных, и такая позиция формирует ложное чувство защищенности. Однако в случае атаки обычные копии оказываются бесполезны, потому что они были доступны для записи из скомпрометированной продуктивной сети.

Игорь Шконда

«Хорошая CPK существует не просто потому, что “так надо”. Она базируется на принципах эшелонированной защиты и глубокой интеграции с ИБ-процессами. Тем не менее в корпоративных ИТ-инфраструктурах CPK по-прежнему сводят к утилитарной функции, тогда как она, наоборот, играет ключевую роль в аварийном восстановлении и обеспечении непрерывности критичных бизнес-процессов, зависящих от сложной взаимосвязи данных, учетных записей, сетевых настроек и конфигураций серверов».

Лучшие практики построения СРК

Если разложить систему резервного копирования на фреймворк 3Р *(персонал, процессы и продукты)*, то, обозревая именно технические практики, формирующие многоуровневую защиту, стоит сфокусироваться на продуктах — в частности, на неизменяемых хранилищах.

Первую практику следует взять за правило: резервные копии и компоненты управления СРК должны быть полностью изолированы от продуктивной среды. Если последняя скомпрометирована *(зашифрован или удален продуктив)*, восстанавливать будет не с чего и нечего, а бизнес-процессы придется строить практически с нуля.

Следующая практика заключается в расширении схемы резервного копирования со стандартной «3-2-1» до «3-2-1-1-0». Иными словами, нужно иметь три копии данных *(3)*, две из них хранить на разных носителях *(2)*, одну сделать отчуждаемой и хранить в отдельном знании *(1) (еще лучше — в другом районе города)*, а еще одну — неизменяемой или расположить ее в изолированной среде *(1)* и иметь ноль ошибок при периодических тестовых восстановлениях *(0)*.

Трафик компонентов системы резервного копирования лучше отделить от трафика данных — в идеале на уровне физических интерфейсов, чтобы усложнить злоумышленнику доступ к компонентам СРК.

Олег Кандальцев

«Еще одна полезная практика заключается в принципе минимальных привилегий на основе ролевой модели. То есть не следует давать операторам СРК права администраторов СРК. Также не следует интегрировать интерфейс управления СРК, как и операционные системы мастер- и медиасерверов СРК, с корпоративной службой каталогов (например, Active Directory), потому что она все чаще становится точкой уязвимости и приоритетным объектом атаки. Преступник получает учетные записи администраторов домена и администраторов СРК, доступ к бэкапам, а дальше — дело техники. В СРК нужно использовать только локальные учетные записи с неповторяющимися паролями. В крупных компаниях, с большим количеством пользователей СРК, имеет смысл организовать отдельную изолированную службу каталогов, никак не связанную с корпоративной».

При построении системы резервного копирования важно помнить о концепции Air Gap — так называемого воздушного зазора между бэкапами и основной сетью. Он может быть физическим *(самый простой)* — подразумевающим отчуждение ленточных картриджей, которые предназначены для хранения большого объема данных. Его создание гарантирует восстановление после аварии. Но поскольку ленточные библиотеки пока не представлены в реестре Минпромторга, можно использовать логический Air Gap: его реализуют в объектных хранилищах с помощью технологий WORM *(Write Once, Read Many)* и Object Lock, которые на определенный срок делают данные неизменяемыми, защищают их от перезаписи и удаления.

Несомненно, стоит упомянуть о ключевой роли актуальной документации и о тестовом восстановлении СРК. Наличие схем инфраструктуры и регламентов резервного копирования будет очень кстати в случае аварии — их не придется придумывать заново. Регулярное документирование и тестовое восстановление всей системы или бизнес-процесса —

СЛЕДУЕТ ВЗЯТЬ ЗА ПРАВИЛО: РЕЗЕРВНЫЕ КОПИИ И КОМПОНЕНТЫ УПРАВЛЕНИЯ СРК ДОЛЖНЫ БЫТЬ ПОЛНОСТЬЮ ИЗОЛИРОВАНЫ ОТ ПРОДУКТИВНОЙ СРЕДЫ

РЕГУЛЯРНОЕ ДОКУМЕНТИРОВАНИЕ И ТЕСТОВОЕ ВОССТАНОВЛЕНИЕ ВСЕЙ СИСТЕМЫ ИЛИ БИЗНЕС-ПРОЦЕССА — ЕДИНСТВЕННЫЙ СПОСОБ ПРОВЕРИТЬ РАБОТОСПОСОБНОСТЬ РЕЗЕРВНЫХ КОПИЙ

единственный способ проверить работоспособность резервных копий. Это трудозатратный процесс, однако он точно окупится в случае реальной атаки.

Игорь Шконда

«Разумеется, обязательно нужно настроить многофакторную аутентификацию (MFA) для всех учетных записей, имеющих доступ к системе, а также проводить логирование и постоянный мониторинг аномалий в СРК. К ним относят, например, массовое удаление данных, изменение политик резервного копирования или попытки доступа с неавторизованных хостов. Современные системы могут включать проактивную защиту (Active Protection) от действий шифровальщика».

СРК как Last Resort: кейсы

Концепция Last Resort реализуется, когда все остальные превентивные меры оказались бесполезными. Рассмотрим несколько соответствующих кейсов. Представим атаку Ransomware: домен скомпрометирован, серверы зашифрованы, ключи доступа украдены, а обычные резервные копии, хранившиеся на локальном диске и сетевой шаре, тоже зашифрованы или удалены.

Тестовые данные содержатся в текстовых файлах Word и Excel. Резервные копии данных создаются с помощью СРК «Кибер бэкап». Три резервные копии данных размещены в разных хранилищах: узел хранения ***(локальное хранилище)***, CIFS-шара ***(сетевое хранилище)*** и «Кибер хранилище» ***(объектное хранилище S3 с включенным Object lock)***. Общий объем данных — примерно гигабайт. Вирус-шифровальщик скомпилирован в exe-файл. При запуске на узле хранения резервных копий он получает доступ к сети, компрометирует домен, повышает привилегии доступа к файловой системе, сначала шифрует все файлы резервных копий ***(локальных, сетевых, объектных)***, затем — непосредственно продуктивные данные, а в финале выводит на экран сообщение с требованием выкупа.

Резервные копии в локальной папке уничтожаются безвозвратно. Восстановление может проходить по двум сценариям: через Object Lock на объектном хранилище либо через снапшоты тома сетевой папки.

В первом сценарии используется защищенная от изменения ***(на настраиваемый период времени)*** копия ***(immutable backup)***, хранящаяся в объектном хранилище с включенным версионированием и Object Lock и режимом Compliance.

Олег Кандальцев

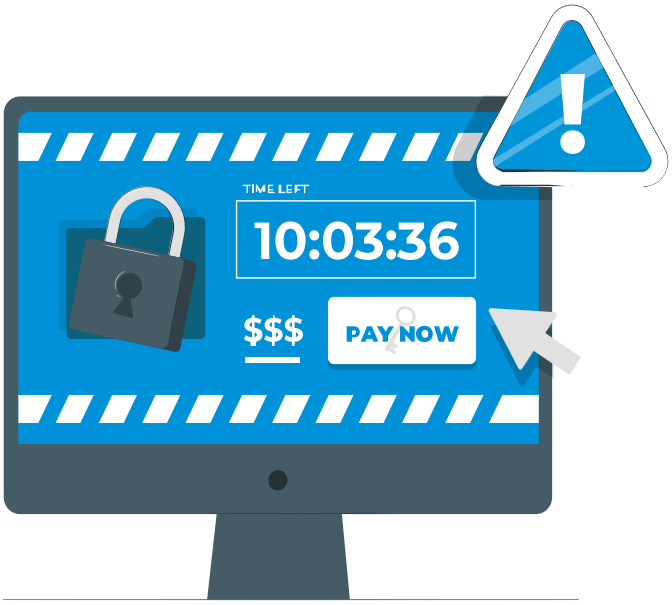
«Даже если злоумышленник попытается перезаписать бэкап с Object Lock, своим действием он создаст новую версию объекта. При этом исходная защищенная и незашифрованная версия может быть просто восстановлена поверх новой зашифрованной. Благодаря этому можно реконструировать практически всё — от отдельных файлов до инфраструктуры в целом».

Непосредственно восстановление можно выполнять вручную, применяя S3-клиент, но лучше написать несложный скрипт-восстановитель с использованием S3 API: в цикле сначала ищется незашифрованная версия каждого объекта в хранилище по времени создания резервной копии, затем эта версия копируется поверх зашифрованной в новую версию, которая делается текущей, и, после восстановления всех объектов, с помощью СРК «Кибер бэкап» восстанавливаются исходные данные. Также можно восстановить файл в объектном хранилище, где

включено версионирование без Object Lock, удалив последнюю версию объекта. Однако если вирус-шифровальщик обнаружит, что Object Lock отсутствует, он может сразу после шифрования безвозвратно удалить первую, незашифрованную версию этого объекта. Неизменяемые копии в объектном хранилище с версионированием и технологией Object Lock остаются нетронутыми.

Во втором сценарии для тома с CIFS-шарой делается снапшот на СХД сразу после бэкапа. После того как эта CIFS-шара будет зашифрована, можно сделать откат тома на этот снапшот и получить таким образом незашифрованные резервные копии. Однако важно понимать, что снапшот лишь дополняет бэкап и формируется вручную, а делать его вручную после каждого бэкапа нереально. Если создавать снапшоты скриптом, высока вероятность ошибок в случаях, когда не удалится предыдущий снапшот перед бэкапом или когда снапшот не успеет вовремя сформироваться: например, если до завершения предыдущего бэкапа начнется следующий бэкап, то при откате на этот снапшот из резервной копии ничего не получится восстановить, так как она останется незавершенной.

Кроме того, следует помнить: если злоумышленник получит административный доступ к интерфейсам управления серверов



(через IPMI), на которых построено объектное хранилище, или к интерфейсу управления СХД с резервными копиями, то он сможет легко уничтожить любые данные безвозвратно — например, удалив пул в СХД или подменив загрузчик на ОС серверов и записав произвольные данные на их тома. Поэтому необходимо либо предусмотрительно отключать кабели от этих интерфейсов, либо подключать их напрямую в один компьютер управления, не связанный с сетью.

RPO + RTO + восстановимость = зрелость ИТ

На способность ИТ-инфраструктуры к восстановлению непосредственно влияют ключевые метрики реальной устойчивости бизнеса — RPO и RTO.

RPO *(Recovery Point Objective)* — это целевая точка восстановления, то есть максимальный период времени, за который могут быть потеряны данные в случае сбоя. Например, если это два часа, то компания должна делать бэкапы как минимум каждые два часа, чтобы ущерб не стал критичным.

RTO *(Recovery Time Objective)* — целевое время восстановления систем после аварии. Максимальный период, в течение которого они могут находиться в нерабочем состоянии.

Игорь Шконда

«Несмотря на установленные метрики, у многих компаний, даже при наличии бэкапов, восстановление может занимать недели. Это происходит потому, что отсутствуют практики тестирования сбоев и восстановления. Соответственно, не хватает документации, и это приводит к неподготовленности сотрудников. Только регулярные тесты позволяют стремиться к заявленным RTO и RPO, определяют устойчивость ИТ-процессов в компании и ее готовность к реальной кибератаке».

В условиях роста киберугроз, которые еще и постоянно совершенствуются, СРК становится стратегическим активом, от которого зависит выживание бизнеса при практически любой нештатной ситуации — от ошибки сотрудника до мощной кибератаки. И как показывает практика, единственный по-настоящему ценный бэкап — это тот, который спроектирован с учетом возможной катастрофы.

ГОСТЬ НОМЕРА

ОБЪЕКТОВАЯ БЕЗОПАСНОСТЬ

ВЕЧНАЯ ЗОЛУШКА ИЛИ МАЧЕХА КОРПОРАТИВНОЙ ЗАЩИТЫ?

АВТОР

Алексей Малинский,

директор департамента управления инвестиционными проектами безопасности и планирования компании «Норникель»

Объектовая безопасность уже давно не ассоциируется только лишь с соблюдением пропускного режима и охраной периметра. В условиях технологической трансформации, новых типов угроз и усиливающегося регулирования она становится элементом стратегического управления, влияющим на устойчивость бизнеса, инвестиционную привлекательность компании и непрерывность производственных процессов. От того, какое место в корпоративной архитектуре отводится объектовой безопасности, напрямую зависит, будет ли она восприниматься как формальность, обременение или системообразующий фактор развития предприятия.

Главные угрозы для промышленных предприятий

Конечно, сегодня мы сталкиваемся с новыми типами угроз безопасности, напрямую связанными с геополитической напряженностью и стремительным развитием технологий. По своему характеру такие угрозы существенно отличаются от рисков, к которым бизнес привык в предыдущие годы. Я бы выделил две ключевые группы угроз.

Первая — это угрозы, связанные с применением беспилотных летательных аппаратов, способных нести боевые заряды или взрывчатые вещества. Речь идет о прямой опасности для производственной инфраструктуры и критически важных объектов. Если раньше система защиты в большей степени строилась вокруг сценариев физического проникновения — условно «штурмовых» атак или диверсионных действий на земле, то сегодня модель преступного воздействия изменилась.

Она предполагает дистанционную атаку на объект, в том числе с использованием беспилотников, что требует принципиально иных решений. Компании рассматривают это направление как одно из приоритетных и внедряют комплекс взаимодополняющих технологий противодействия, опираясь в том числе на обмен практическим опытом с другими промышленными предприятиями.

Вторая группа — нарастающие угрозы в сфере экономической безопасности, в том числе связанные с развитием ИИ. Современные цифровые инструменты используются не только для повышения эффективности бизнеса, но и для усложнения мошеннических схем, манипуляций с данными и иных противоправных действий. Это масштабная и многослойная проблема, требующая комплексных мер — от внедрения систем цифрового мониторинга до совершенствования аналитических инструментов выявления аномалий. В этой сфере крайне важно поддерживать технологическую актуальность, своевременно адаптировать инструменты контроля и действовать на опережение, чтобы эффективно противостоять новым форматам рисков.

Минимизация ущерба от инцидентов на промышленных объектах

Безопасность промышленных объектов и крупных холдингов — это прежде всего вопрос защиты жизни и здоровья людей. Любой серьезный инцидент на производственной площадке несет прямые риски для персонала, подрядчиков и жителей прилегающих территорий. Именно это определяет безусловный приоритет превентивных мер и системного управления безопасностью.

Кроме того, инциденты неизбежно влекут значительные экономические последствия. В первую очередь речь идет о прямом ущербе: потере продукции и, как следствие, выручки, повреждении инфраструктуры, простоях оборудования, затратах на ликвидацию последствий и восстановительные работы. Однако не менее существенны косвенные потери: репутационный ущерб, снижение доверия со стороны партнеров и инвесторов, ухудшение инвестиционной привлекательности как самой компании, так и региона ее присутствия, социальная напряженность. На практике именно косвенные эффекты нередко оказываются наиболее чувствительными для бизнеса, поскольку влияют на долгосрочную устойчивость компании.

Таким образом, последствия инцидентов в сфере промышленной безопасности носят комплексный характер и затрагивают практически все ключевые направления деятельности предприятия. Их предупреждение и минимизация требуют системного подхода. И начать следует с детального анализа рисков и оценки их «веса» — сочетания вероятности наступления и масштаба потенциального воздействия. Актуальная и регулярно пересматриваемая модель рисков становится первым ключевым фактором эффективности всей системы безопасности.

Второй ключ — формирование стратегии компании в области безопасности: разработка текущей и целевой моделей развития функции, определение управленческих акцентов и приоритетов, включая параметры инвестиционного планирования. Именно стратегическая рамка позволяет выстроить сбалансированную систему, в которой ресурсы направляются на противодействие действительно значимым угрозам.

Практика показывает результативность комплексных инвестиционных программ, ориентированных на конкретные категории рисков — прежде всего на предотвращение их реализации и одновременное снижение возможного ущерба. Такой подход применим ко всем направлениям корпоративной безопасности, включая как объектовую, так и экономическую составляющие. Последовательность и стратегическая выверенность шагов позволяют своевременно выявлять уязвимости, концентрировать усилия на наиболее критичных направлениях и в конечном итоге снижать

Безопасность промышленных объектов и крупных холдингов — это прежде всего вопрос защиты жизни и здоровья людей

вероятность инцидентов и защищать бизнес от существенных экономических потерь.

Регуляторные изменения

В условиях усложнения глобальной повестки и появления новых типов угроз регуляторная среда неизбежно развивается во многом в реактивном формате, отвечая на возникающие вызовы и корректируя требования к защищенности объектов. Для компаний стратегического уровня такая динамика означает необходимость постоянной адаптации внутренних процессов безопасности к обновляющимся нормам.

Деятельность «Норникеля» имеет стратегическое значение для экономики страны, поэтому исполнение требований законодательства РФ является базовой и системной задачей как для блока корпоративной защиты, так и для компании в целом. Речь идет не только о формальном соблюдении нормативов, но и о выстраивании устойчивой модели, соответствующей актуальным стандартам регулирования.

В последние годы требования к промышленной и антитеррористической защищенности объектов существенно изменились. Регуляторные изменения нацелены на повышение реального уровня защиты, развитие цифровых инструментов контроля и усиление ответственности за обеспечение безопасности на всех уровнях управления. К примеру, в Федеральный закон № 256-ФЗ «О безопасности объектов топливно-энергетического комплекса» внесены поправки: введено понятие зоны безопасности объекта ТЭК — территории, водного или воздушного пространства вокруг объекта, где реализуются меры по его особой защите; уточнены требования к категорированию объектов с учетом потенциальной опасности и социально-экономических последствий; закреплены обязательные меры защиты от угроз БПЛА.

Актуализированы и требования Минпромторга РФ к промышленным объектам, включая их техническое оснащение и антидроновые решения. Изменения затронули также сферу транспортной безопасности.

Развитие объектовой безопасности с учетом новых требований предполагает:

- детальную оценку каждого объекта с учетом индивидуальной и региональной специфики;
- применение современных интеллектуальных систем видеонаблюдения, контроля доступа и инженерной защиты с обязательной практической проверкой их эффективности и обоснованности затрат;
- централизацию управления на базе ситуационных центров реагирования;
- цифровую трансформацию ключевых направлений работы блока корпоративной защиты.

Роль объектовой безопасности

Золушка или мачеха? Роль объектовой безопасности полностью зависит от подхода организации к культуре безопасности с учетом ее ресурсов и специфики деятельности. В компаниях, где объектовая безопасность рассматривается лишь как техническая необходимость и не интегрирована в общую стратегию защиты бизнеса, ей уделяется меньше внимания по сравнению с кадровой, экономической и другими видами безопасности.

Причины типичны: ограниченность ресурсов, когда бюджет перераспределяется в пользу других направлений; отсутствие стратегического планирования в этой области, поскольку объектовая безопасность не воспринимается как фактор, напрямую влияющий на ключевые бизнес-показатели; сложность измерения эффективности мер физической защиты в категориях прямой прибыли. В такой конфигурации это вечная Золушка — элемент системы, работающий в тени и не получающий инвестиций, необходимых для полноценного развития.

Противоположная крайность не менее рискованна. При избыточной жесткости, бюрократизации

процессов, конфликтах с подразделениями и высоких затратах без видимой отдачи объектовая безопасность начинает восприниматься как ограничение для бизнеса. Нерациональные инвестиции в технические решения или неэффективные схемы охраны формируют ощущение бюджетного бремени и атмосферу недоверия, вызывают недовольство сотрудников и их сопротивление мерам безопасности.

Оптимальный подход, которого придерживаются в «Норникеле», — это соблюдение баланса. Полная интеграция объектовой безопасности в стратегию корпоративной защиты, ее согласованность с другими направлениями, рациональное использование ресурсов и применение современных технологий — аналитики и цифровизации — позволяют выстроить устойчивую модель. Ее дополняют регулярный аудит и адаптация к изменениям бизнес-процессов, технологий и регуляторной среды. Ключевой принцип — предотвращение угроз без ущерба для производственной деятельности.

> Объектовая безопасность, да и безопасность в целом, — не Золушка и не мачеха, а скорее фея-крестная всех корпоративных бизнес-процессов. Без нее невозможна стабильность производственных, транспортных, финансовых, логистических и других цепочек предприятия.

Комплексная безопасность в «Норникеле»

Для крупной промышленной компании развитие корпоративной безопасности — не разовая задача, а непрерывный управленческий процесс. «Норникель», как бизнес с масштабной и территориально распределенной инфраструктурой, объективно сталкивается с широким спектром угроз. А это требует системного внедрения современных технологий и управленческих подходов. Формирование эффективных моделей оценки рисков и разработка комплексных мер противодействия становятся важными элементами стратегического управления безопасностью.

Базовые требования к защите объектов определяются действующим законодательством — в части антитеррористической защищенности, транспортной безопасности и иных нормативных стандартов. Их соблюдение является обязательной основой функционирования системы безопасности. Вместе с тем современные технические решения позволяют выходить за рамки минимально необходимого уровня защиты и решать более широкий круг задач корпоративной безопасности.

Интеграция различных технических инструментов существенно повышает результативность работы профильных подразделений. Инновационные решения, например нейросетевые технологии видеоаналитики, расширяют функциональность системы: помимо физической защиты объектов, такие инструменты поддерживают задачи экономической, промышленной, пожарной и экологической безопасности. Объединение традиционных средств охраны с цифровыми инструментами контроля в сфере экономической безопасности, включая антифрод-решения, обеспечивает комплексный взгляд на риски, позволяет выявлять потенциальные нарушения на ранних этапах и снижать масштаб возможных последствий.

Чтобы подобные решения реализовать, необходима соответствующая инфраструктура, способная обрабатывать значительные объемы данных и одновременно отвечать требованиям информационной безопасности и корпоративной архитектуры. Формирование единой цифровой экосистемы безопасности означает объединение всех систем в одну согласованную структуру, где данные не разрознены, а связаны между собой, процессы работают согласованно, а управленческие решения принимаются на основе полной и целостной картины происходящего.

Следующий этап развития безопасности связан с подготовкой к более широкому применению технологий искусственного интеллекта. Для этого необходимы специализированные и защищенные модели обработки данных, обеспечивающие конфиденциальность и целостность критически важной информации. Такой подход позволяет не только повышать эффективность реагирования на угрозы, но и укреплять устойчивость и конкурентоспособность бизнеса в долгосрочной перспективе.

Конструируя безопасность

Идея внедрения комплексных систем безопасности, активно обсуждаемая в отрасли, когда-то звучала как лозунг, но сегодня уже получила практическое воплощение благодаря значительным достижениям производителей оборудования и софта. Современные решения позволяют объединить традиционные средства обеспечения физической безопасности объектов в рамках единых платформ классов ССОИ *(система сбора и обработки информации)* и PSIM *(программный модуль для управления информацией*

о физической безопасности). Такие системы помогают настроить централизованное управление всеми компонентами безопасности и автоматизацию процессов выявления и устранения угроз.

Крупные промышленные компании, такие как «Норникель», управляют разветвленной инфраструктурой и активами, расположенными в разных регионах. В таких условиях стандартных решений уже недостаточно — требуется более масштабная и системная организация управления безопасностью. Одним из таких решений стала концепция системы ситуационно-аналитических центров безопасности *(ССАЦБ)*.

Она объединяет инструменты мониторинга и аналитики в единую структуру, позволяет централизованно отслеживать ситуацию на объектах и оперативно реагировать на угрозы. Речь идет о контроле рисков в различных направлениях — от корпоративной и экономической до транспортной и антитеррористической безопасности. Такая модель обеспечивает целостное понимание происходящего и повышает управляемость всей системы защиты.

Концептуально архитектура управления ССАЦБ распределена по трем уровням с вертикальной цифровой связанностью:

- **Пункты управления безопасностью объектов:** сбор событий и потоков от объектовых систем безопасности, объединенных в PSIM-системы. Именно здесь происходит управление и оперативное реагирование на инциденты.
- **Региональные САЦБ** *(ключевые регионы присутствия)*: работа с информацией, поступающей с первичного *(объектового)* уровня, аналитика. Они выступают промежуточным звеном, гарантирующим эффективную передачу необходимой информации без перегрузки верхнего уровня лишними деталями.
- **Главный САЦБ** *(главный офис компании)*: агрегирование и обработка поступивших массивов информации, выработка предложений для принятия управленческих решений руководством на основании комплексного анализа ситуации и учета множества факторов риска.

В режиме реального времени на каждый уровень передаются только те события, которые требуют участия или решения вышестоящего звена; остальная информация агрегируется в виде статистики. Вертикальная интеграция системы позволяет при необходимости обратиться к первоисточнику — телеметрии датчиков, видеопотокам охранного телевидения, последовательности действий сотрудников безопасности. Инциденты обрабатываются на объекте и, при необходимости координации или принятия решений, эскалируются в региональные ситуационно-аналитические центры и далее — в главный центр.

Технологическим ядром ССАЦБ является портал безопасности — единая платформа, объединяющая потоки видеонаблюдения *(CCTV)*, контроля и управления доступом, охранно-тревожной сигнализации, навигационных и анти-БПЛА-систем, а также данные по направлениям корпоративной безопасности, включая антифрод-модули и контроль сил и средств. Ключевой акцент сделан на аналитике — автоматизированной обработке показателей, выявлении закономерностей и формировании управленческих акцентов.

В результате предприятие получает цифровую экосистему безопасности в формате «единого окна» с распределением полномочий, прозрачной эскалацией и поддержкой управленческих решений. Такая архитектура обеспечивает эффективную работу с большими массивами данных, оперативное реагирование на инциденты, снижение ущерба и повышение устойчивости бизнеса.

Безопасность как фактор стратегической устойчивости бизнеса

Объектовая безопасность становится органичной частью стратегической архитектуры бизнеса, и ее результативность определяется не количеством регламентов или технических средств, а глубиной интеграции в корпоративные процессы, качеством риск-модели и уровнем управляемости цифровой инфраструктуры.

Для крупного промышленного бизнеса безопасность — это управляемая система, встроенная в контур принятия решений. Она влияет на непрерывность производственных и логистических процессов, инвестиционную привлекательность компании и предсказуемость ее развития. Последовательная работа с рисками, приоритизация инвестиций и цифровая интеграция инструментов контроля формируют устойчивую модель, в которой безопасность становится не издержкой, а элементом стратегического управления.

МАНИФЕСТ

ИНФРАСТРУКТУРЫ БЕЗ СТАБИЛЬНОСТИ, ИЛИ ОТКАЗ ОТ ИНЖЕНЕРНЫХ ИЛЛЮЗИЙ

Современные цифровые системы существуют в мире постоянных изменений. Релизы выходят еженедельно и ежедневно. Нагрузки непредсказуемы. Пользователи распределены географически. Список угроз меняется быстрее, чем архитектурные стандарты.

Система больше не обязана быть законченной. Она обязана быть живой.

В такой реальности инфраструктура, спроектированная как устойчивая, перестает соответствовать темпу изменения мира. Системы, спроектированные как статичные, ломаются именно потому, что **мир перестал быть статичным. Инфраструктура больше не может быть фундаментом,** который просто держит нагрузку. Она становится средой, в которой происходят изменения.

Мы живем внутри инфраструктуры, которая ломается. Каждый день.

КОГДА КОНТРОЛЬ ПЕРЕСТАЛ РАБОТАТЬ

Классическая ИТ-инфраструктура строилась вокруг идеи контроля. Центр принятия решений. Главный дата-центр. Основная и резервная площадки. Заранее определенные сценарии отказов.

Такая модель работала в мире, где изменения были редкими, а границы систем — четкими. Но распределенные приложения, горизонтально масштабируемые нагрузки и онлайн-сервисы умирают в логике центра. Центр в таких системах перестает быть точкой устойчивости. Он становится потенциальной точкой отказа.

Центр больше не точка силы. Центр — это точка уязвимости.

Современная инфраструктура проектируется иначе — как **система без единого центра**. Дата-центры перестают делиться на основные и резервные и становятся равнозначными зонами доступности. Компоненты — автономными. Устойчивость не концентрируется в одной точке и вокруг одного компонента. Отсутствие точек устойчивости трансформирует систему в антихрупкую.

Среда не может быть зафиксирована.

ИНФРАСТРУКТУРА КАК СРЕДА, А НЕ КАК ОБЪЕКТ

Еще один важный сдвиг — изменение самого взгляда на инфраструктуру. Сервер больше не воспринимается как уникальный физический объект, который обязательно нужно защитить и в случае сбоя — восстановить. Он **существует как состояние,** которое можно воспроизвести.

Мы больше не управляем железом. Мы управляем описаниями.

Приложение — не просто запущенный процесс, а набор конфигураций, зависимостей и деклараций. ИТ-ресурсы — не единый дата-центр, а совокупность идентичных зон доступности, работающих независимо.

Инфраструктура все чаще живет в виде кода. Именно **описание системы,** а не ее текущее физическое состояние, **становится источником устойчивости.**

Когда физическое ломается, декларативное остается.

Когда физическое ломается, описание остается. И этого оказывается достаточно, чтобы восстановиться.

ВИРТУАЛЬНОЕ НАДЕЖНЕЕ РЕАЛЬНОГО

Контейнеры, манифесты, шаблоны, образы, декларативные конфигурации долго воспринимались как вспомогательные инструменты. Сегодня они стали **фундаментом.**

Их можно клонировать. Пересоздавать. Масштабировать. Откатывать.

Виртуальное стало надежнее реального.

Виртуальное описание инфраструктуры оказывается надежнее физической реализации. **Не потому, что оно идеальное, а потому, что оно воспроизводимое.** Надежность все меньше связана с сохранением состояния и все больше — со способностью пересоздания.

Мы живем среди симуляций, и именно они позволяют системе выживать.

ΔV: ЗАПАС МАНЕВРА ВМЕСТО ЗАПАСА ПРОЧНОСТИ

Долгое время инфраструктуру оценивали по двум основным критериям: надежность и производительность. Они по-прежнему важны, но перестают быть определяющими.

Сбой — не исключение. Сбой — контекст.

Главный вопрос современной архитектуры звучит иначе: **может ли система меняться, не разрушая саму себя?**

Инцидент — не катастрофа. Инцидент — источник информации.

В этой логике появляется понятие ΔV — запас маневра. Не скорость и не мощность, а способность менять траекторию движения.

Инфраструктура с ΔV пересоздает компоненты вместо их восстановления. Масштабируется за счет добавления однотипных элементов, а не усложнения узлов. Допускает эксперименты, замену компонентов и эволюцию без остановки бизнеса.

ΔV — не метрика. Это свойство архитектуры, в которой изменения не считаются угрозой.

АНТИХРУПКОСТЬ КАК НОВАЯ УСТОЙЧИВОСТЬ

Классический подход к эксплуатации стремился минимизировать сбои. Современный принимает их как неизбежность.

Сбой перестает быть исключением. Он становится частью рабочего контекста.

Антихрупкость — это не отсутствие проблем. Это способность использовать их.

Антихрупкая инфраструктура не просто восстанавливается после инцидентов. Она использует их как **источник информации и развития.**

В этом мире больше не работает идея универсального решения.

Отсюда — внимание к наблюдаемости, SRE-подходам, самовосстановлению и быстрому пересозданию. Эксплуатация перестает быть реактивной. Она встраивается в архитектуру системы.

Контроль больше не гарантирует устойчивости.

ИНФРАСТРУКТУРА, СПРОЕКТИРОВАННАЯ ПОД РАЗРУШЕНИЕ

Отдельный вызов — киберинциденты. Сегодня их рассматривают в парадигме «когда», а не «если».
Инфраструктура, в которой не предусмотрено разрушение, живет **в предположении о стабильном мире.** Ключевыми свойствами становятся **воспроизводимость и быстрая пересоздаваемость.** Когда все ломается, выживает только то, что способно к адаптации.

СВОБОДА АРХИТЕКТУРЫ ВМЕСТО ДОГМ

Современная инфраструктура существует в условиях ограничений: регуляторных, технологических, вендорских. Ответом на это становится отказ от универсальных рецептов.
Нет единственного правильного стека. Есть архитектурные решения для конкретного контекста.
Свобода архитектуры — это не хаос. Есть лишь способность выбирать и менять траекторию, когда меняется среда.

Антихрупкая инфраструктура — это крайняя форма честности. Она гарантирует, что система сможет продолжить.

ИНФРАСТРУКТУРА КАК УСЛОВИЕ БУДУЩЕГО

Инфраструктура больше не служит для консервации прошлого. Ее задача — **сделать возможным будущее.**
В мире постоянных изменений надежность перестает быть синонимом стабильности. Она становится синонимом способности адаптироваться, изменяться и двигаться вперед. Она становится синонимом антихрупкости.

Мы не возвращаемся к центру. Мы не ищем единственный правильный путь. Мы не верим в догмы.

Инфраструктура больше не обещает стабильность. Она предлагает иное — **способность продолжать.**

Инфраструктура больше не служит для сохранения прошлого. Она существует для того, чтобы будущее было возможно

ПОСТМОДЕРН КАК СОСТОЯНИЕ ИНФРАСТРУКТУРЫ

Современную ИТ-инфраструктуру все чаще описывают словами, которые раньше звучали исключительно в философии и архитектуре. Не потому, что инженеры вдруг стали философами, а потому что **другого языка для описания реальности больше нет.**

КОНЕЦ «БОЛЬШИХ АРХИТЕКТУР»

Французский философ Жан-Франсуа Лиотар описывал постмодерн как состояние «конца больших нарративов». Универсальные объяснения — прогресс, рациональность, единая истина — перестают работать. Им на смену приходит множество локальных контекстных логик. В ИТ это проявляется буквально.

Больше нет единственной правильной архитектуры, эталонного стека, универсального стандарта, одинаково подходящего для всех систем.

Каждая инфраструктура существует в собственном контексте со своими ограничениями, рисками и точками устойчивости.

Инженерные «большие нарративы», обещающие универсальный стек, правильную архитектуру и главный ЦОД, больше не выдерживают столкновения с реальностью.

СМЕРТЬ ЦЕНТРА

Модернистская архитектура и в философии, и в строительстве, и в ИТ всегда стремилась к центру.

Центр как источник смысла.
Центр как точка управления.
Центр как гарантия порядка.

Постмодерн разрушает эту конструкцию.

В распределенных системах центр перестает быть опорой и становится уязвимостью. Устойчивость больше не может быть сосредоточена в одной точке. Она должна быть распределена.

Именно поэтому современная инфраструктура все чаще строится как система без центра: равнозначные зоны доступности, автономные компоненты, отсутствие «главного» узла и горизонтальное расширение.

СИМУЛЯКРЫ ИНФРАСТРУКТУРЫ

Здесь язык философии неожиданно становится особенно точным.

Философ Жан Бодрийяр писал о симулякрах — копиях, которые со временем перестают отсылать к оригиналу и начинают существовать как самостоятельная реальность. Симуляция не искажает реальность — она **заменяет ее.** В этой оптике современная ИТ-инфраструктура начинает читаться иначе.

Сервер существует как образ и состояние. Приложение — как описание и конфигурация. Инфраструктура — как набор деклараций, зависимостей и манифестов.

Физическая реализация становится временной. Определяющим становится то, **что можно воспроизвести.**

Контейнеры, образы, манифесты, декларативные описания, Infrastructure-as-Code — это симулякры инфраструктуры. Но именно они оказываются устойчивее физического мира.

Когда физическое ломается, симуляция остается. И позволяет системе двигаться вперед.

ОТ КОНТРОЛЯ К ВОСПРОИЗВОДИМОСТИ

Классическая инженерная логика стремилась сохранить состояние. Постмодернистская — обеспечить возможность пересоздания.

Система считается устойчивой не тогда, когда она никогда не падает, а тогда, когда она может быть быстро пересоздана из описания в любой момент. Надежность больше не равна сохранности, она равна воспроизводимости.

АНТИХРУПКОСТЬ КАК ФИЛОСОФСКАЯ ЧЕСТНОСТЬ

Постмодерн отказывается от иллюзии тотального контроля. Он признает сложность, неопределенность и невозможность полного предсказания.

Антихрупкая инфраструктура исходит из той же реальности. **Она не пытается исключить сбои. Она встраивает их в систему.**

Наблюдаемость, адаптивность и быстрое пересоздание — это не инструменты контроля в классическом смысле. Это способы осмысленного **взаимодействия с неопределенностью.**

ИНФРАСТРУКТУРА КАК ПОЗИЦИЯ

Постмодернистская ИТ-инфраструктура — это не отказ от инженерии. Это **отказ от инженерных иллюзий контроля.**

Она не обещает стабильность навсегда. Она легитимизирует изменчивость мира и проектирует системы, в которых изменчивость – это часть архитектуры.

Именно поэтому язык постмодерна так точно ложится на современную инфраструктуру. Он описывает **мир без центра, без универсальных решений,** но **с системами, которые умеют выживать и продолжать.**

ПОСЛЕ СБОЯ — СИЛЬНЕЕ

В традиционном понимании надежная ИТ-система — это система, которая работает без сбоев. Однако современный ИТ-ландшафт стал значительно сложнее — и полностью исключить сбои практически невозможно. Поэтому сегодня важна не только устойчивость систем, но и их способность адаптироваться к стрессу и изменениям. Это качество все чаще описывают термином «антихрупкость».

АНТИХРУПКОСТЬ ГЛАЗАМИ ЛИДЕРОВ ИТ-ИНДУСТРИИ

Редакция JetInfo обратилась к спикерам IT Elements — одной из крупнейших ИТ-конференций — с вопросом: «Что такое антихрупкость в ИТ?» Ответы представителей индустрии показывают, какие смыслы они сегодня вкладывают в этот термин и как это понятие трактуется на практике.

ИГОРЬ ДОРОФЕЕВ, президент Ассоциации участников отрасли ЦОД:

«Несмотря на некоторое искусственное звучание термина “антихрупкость в ИТ”, он удачно сочетает в себе такие синонимичные понятия, как “гибкость”, “устойчивость” и “основательность”. Все эти характеристики в полной мере применимы не только к ИТ, но и к ЦОД как инфраструктурным объектам. При необходимой прочности и отрасль, и ЦОД не должны быть неповоротливыми и “захрясать” — напротив, им следует оставаться открытыми к изменениям и вызовам».

ВЛАДИМИР МУРАВЬЕВ, ИТ-директор СГ «АльфаСтрахование»:

«Антихрупкость в ИТ — это свойство ИТ-системы или сервиса, которое позволяет им не просто противостоять сбоям (быть отказоустойчивыми или бесперебойными — то есть способными работать в любых условиях), а извлекать выгоду из ошибок проектирования и программирования, а также из волатильности ИТ-инфраструктуры. При отказе или ошибке антихрупкая система или сервис становятся сильнее и развиваются. Пример такого подхода — применение принципов Chaos Engineering для создания сложных и распределенных систем, в которых контролируемые сбои повышают устойчивость системы и гибкость микросервисной архитектуры. Реализация принципа антихрупкости дает возможность проектировать самообучающиеся системы, эволюционирующие под давлением стохастических стрессоров (это могут быть даже регулярные проверки и контролируемые сбои, позволяющие понять, как поведет себя система). Антихрупкость — это не путь выживания, а развитие через стресс и ошибки».

ЕВГЕНИЙ АБАКУМОВ, директор по информационным и цифровым технологиям госкорпорации «Росатом»:

«Антихрупкость в ИТ — это прежде всего люди. Сегодня российская ИТ-команда прошла серьезную закалку: санкции, импортозамещение, сложные и нестандартные проекты, при реализации которых каждый день был вызовом. Именно эти специалисты не только обеспечивают текущую эксплуатацию и поддержку систем, но и создают новое даже в непростых условиях. Разрабатывают идеи, запускают стартапы, предлагают решения мирового уровня. На практике антихрупкость — это команда, закаленная вызовами, но при этом полная энергии и созидательной силы».

ИВАН МЫЗДРИКОВ, директор по продуктам VK Tech:

«Антихрупкость в ИТ означает способность не просто пережить турбулентность, а выйти из нее сильнее. Волна импортозамещения привела на рынок корпоративного ПО много новых игроков, но не все из них выдержали конкуренцию. Укрепили позиции те, кто последовательно развивал продуктовую экспертизу и закрывал реальные потребности бизнеса. VK Tech относится к таким компаниям: за это время мы расширили продуктовую линейку, объединили сервисы в единую платформу и внедрили ИИ в рабочие процессы. Турбулентность стала не угрозой, а условием для роста».

КОНСТАНТИН ТИТКОВ, руководитель центра ИБ дочерних обществ «Газпромбанка»:

«Сфера ИТ — гибкая, и антихрупкость в ней — это планирование и готовность к неожиданностям. Существующий в компании план действий на случай сбоя базы данных или нарушения связи не подойдет при атаке шифровальщика. Восстановление при сбое занимает часы, а при атаке шифровальщика — дни. Подготовившись заранее, можно сократить простой и избежать главных ошибок: считать шифрование обычным ИТ-инцидентом и проблемой только ИТ-/ИБ-служб, рассчитывать быстро справиться своими силами. Поэтому кибербезопасность — важная грань ИТ и тоже напрямую связана с антихрупкостью».

ВЛАДИМИР ЗОЛОТОВ, директор по информационным технологиям АО «Гринатом»:

«Для меня антихрупкость в ИТ — это концепция, выходящая за рамки традиционной отказоустойчивости: системы не просто выживают при стрессе или сбоях, а становятся сильнее и устойчивее благодаря им. В атомной отрасли мы строим антихрупкую ИТ-инфраструктуру, используя распределенные дата-центры, микросервисную архитектуру, гибридные платформы, поддерживающие оборудование и ПО от разных вендоров, а также внедряя в ключевые технологические стеки отечественные решения для снижения внешних рисков и обеспечения технологической независимости».

Директор по архитектуре и стратегии ИТ крупной производственной компании:

«Чтобы объяснить антихрупкость ИТ, сначала важно понять, что такое хрупкость. Хрупкими обычно бывают твердые структуры: они хорошо выдерживают давление, но плохо переносят резкие изменения. Сфера ИТ в компании постоянно испытывает давление — со стороны бизнеса, который требует эффективности и снижения затрат, и со стороны рынка с его конкуренцией и новыми решениями. В ответ компании стремятся создать максимально устойчивую ИТ-инфраструктуру. Однако чрезмерная “жесткость” делает систему уязвимой к изменениям — будь то изменения в бизнес-модели, команде, корпоративной культуре или технологическом ландшафте. Противоположность хрупкости — адаптивность. В ИТ это способность технологий, систем и, прежде всего, модели управления гибко реагировать на изменения. При этом важно не впасть в другую крайность — гипергибкость, которая может подорвать стабильность, особенно в производственных компаниях. Антихрупкость ИТ возникает там, где найден баланс между устойчивостью и способностью адаптироваться к изменениям».

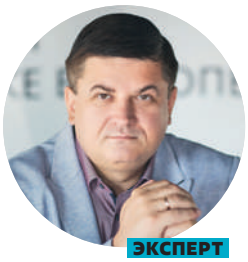
НЕ ТАКОЙ, КАК ВСЕ

В ЧЕМ ОСОБЕННОСТЬ ЦОД ДЛЯ ИСКУССТВЕННОГО ИНТЕЛЛЕКТА

ЭКСПЕРТ

Сергей Андронов,

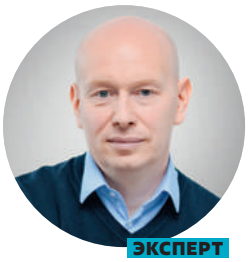
директор центра сетевых решений компании «Инфосистемы Джет»



ЭКСПЕРТ

Сергей Вышемирский,

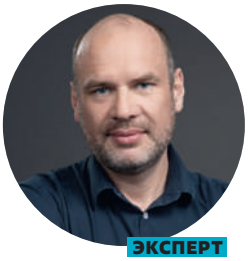
технический директор IXcellerate



ЭКСПЕРТ

Максим Андрианов,

руководитель дирекции по разработке и внедрению ПО компании «Инфосистемы Джет»

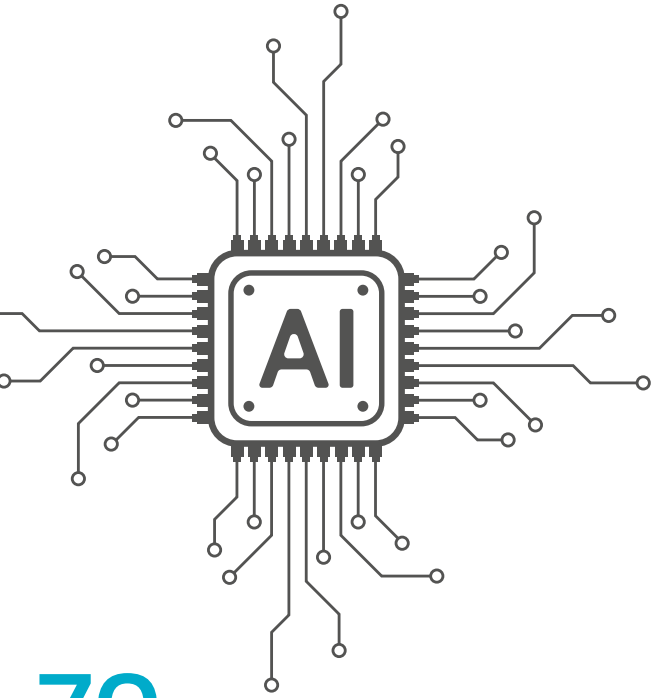


ЭКСПЕРТ

Всеволод Воробьев,

руководитель направления ЦОД центра сетевых решений компании «Инфосистемы Джет»

По данным аналитиков McKinsey, 78% компаний уже используют искусственный интеллект для решения бизнес-задач. Для массового внедрения ИИ-сервисов необходима развитая ИТ-инфраструктура, обеспечивающая их работу. В первую очередь речь идет о центрах обработки данных, спрос на которые в России растет на 10–15% в год. Однако обычный дата-центр «заточить» под нагрузки ИИ не получится. Почему — разбираемся в нашей статье.



ЦОД с особыми условиями

Технологии искусственного интеллекта «перестраивают» дата-центры, так как требуют экстремальной вычислительной плотности. Ее не могут обеспечить процессоры, которыми оснащены обычные ЦОД. Для обработки задач машинного обучения необходимы графические процессоры *(GPU)*. Серверы с графическими ускорителями, объединенные высокоскоростной сетевой инфраструктурой, образуют GPU-кластеры. Они предназначены для ресурсоемких параллельных вычислений, характерных для обработки больших данных, обучения и поддержки работы больших языковых моделей *(LLM)* и других систем искусственного интеллекта. Из набора GPU-кластеров и состоит дата-центр для ИИ.

Для таких ЦОД необходимы специализированные комплектующие, современное жидкостное охлаждение

серверных стоек и продвинутые системы управления, способные обеспечить эффективную работу высоконагруженного оборудования в различных режимах и предотвратить возможные инциденты. Но главное — эти объекты «съедают» значительно больше электроэнергии.

Сергей Вышемирский

«ИИ-нагрузки принципиально меняют логику проектирования дата-центров. Если стандартная стойка сегодня потребляет 5–10 кВт, то для решения задач машинного обучения этот показатель увеличивается до 40–60 кВт — то есть речь идет о кратном росте плотности энергопотребления. Средняя нагрузка на стойку у наших клиентов уже составляет 12 кВт, а в ряде контрактов превышает 20 кВт. Воздушное охлаждение перестает справляться: при размещениях с плотностью от 50 кВт это становится либо технически невозможным, либо экономически невыгодным. Поэтому мы проектируем новые объекты с возможностью гибридного — воздушного и водовоздушного — охлаждения. В Москве в Южном кампусе IXcellerate спроектирован отдельный зал с водяным охлаждением мощностью 1 МВт».

Эксперт отметил, что при строительстве таких объектов важно и то, что ИИ-вычисления допускают кратковременные остановки без потери данных — это позволяет отказаться от избыточного резервирования вычислительных мощностей и оптимизировать капитальные затраты. Главный принцип — закладывать архитектурный и энергетический запас уже на этапе концепции: в дальнейшем адаптировать готовый объект под высокоплотные нагрузки практически невозможно.

Сергей Андронов

«Физику обмануть нельзя, ведь меньшая проектная мощность — это иное оборудование. Даже кабели используются неподходящие для ИИ — обладающие меньшим сечением. Поэтому, чтобы получить большую мощность на стойку при переходе на обслуживание ИИ-приложений, необходимо кардинально менять инженерную инфраструктуру либо распределять нагрузку по большому количеству стоек. Кроме того, не стоит забывать о наличии необходимых для ИИ генерирующих мощностей и готовности энергетических компаний адаптировать выработку электричества для вашего объекта. Все эти решения значительно затрудняют изменение классических ЦОД под задачи обслуживания ИИ-приложений. В большинстве случаев проще построить новый объект с нуля».

В то же время нецелесообразно использовать специализированный ЦОД для ИИ для стандартных задач: получается слишком дорого из-за графических ускорителей. Впрочем, на российском рынке есть гибридные дата-центры: часть площадей отдается под обработку задач искусственного интеллекта, а какой-то зал оборудован под стандартные технологии.

Из Москвы — в регионы: в погоне за энергией

ЦОД для ИИ логичнее всего обеспечивать энергией напрямую от АЭС, гидро- или газовых электростанций. Строительство последних, например, уже запустили такие ИТ-гиганты, как Google, Microsoft и Meta*, и это привело к дефициту газовых турбин на рынке. Интересно, что для питания дата-центров даже планируется проектировать АЭС нового типа: они будут иметь относительно небольшой срок эксплуатации при форсированной генерации электричества. Однако пока ощущается нехватка электроэнергии для ИИ-ориентированных дата-центров.

Всеволод Воробьев

«Электроэнергии в крупных российских городах становится все меньше и меньше. В Москве ее практически не осталось. По нашим прогнозам, в ближайшее время строительство ЦОД для ИИ будет массово смещаться в Московскую и близлежащие области, например Калужскую, Тверскую. Либо в совсем удаленные от столицы регионы, где электричества больше и есть возможность строить такие крупные энергоемкие объекты».

Однако в регионах должен быть выбор провайдеров высококачественных, разносторонних каналов связи для обмена информационным трафиком, который генерируют дата-центры, добавил эксперт.

Полное погружение: как охладить самый горячий ЦОД

Помимо энергетического вопроса, российским операторам ЦОД для ИИ при проектировании объектов приходится учитывать и аспекты, связанные с введением санкций. Ограниченная доступность импортного оборудования стала для них одним из ключевых вызовов. Именно этот фактор побудил IXcellerate развивать собственный R&D-центр.

Сергей Вышемирский

«Мы искали решения, которые позволили бы ускорить запуск новых объектов в условиях, когда привычная компонентная база перестала быть доступной в прежних объемах. В результате были разработаны и запатентованы собственные технологии кондиционирования машинных залов — воздухоохладительная камера статического давления (ВОК), обеспечивающая равномерное распределение воздушных потоков. Решение прошло независимую экспертизу Роспатента и уже эксплуатируется на действующих объектах с суммарной нагрузкой свыше 30 МВт».

Без передовых систем охлаждения эксплуатация ИИ-ориентированных ЦОД становится невозможной из-за экстремальной плотности тепловыделения GPU-кластерами. На первый план сейчас выходят иммерсионные системы, использующие жидкости для отвода тепла. Сервер погружается непосредственно в охлаждающую среду, находящуюся максимально близко к точкам нагрева. Сейчас это один из способов дать большие нагрузки на оборудование. Для упрощения этой задачи производители серверов объединяют усилия с разработчиками ПО и инженерного оборудования. Результат — появление высокотехнологических серверов, которые имеют контуры охлаждения прямо на борту.

Всеволод Воробьев

«Возможностей воздушного охлаждения и свободного охлаждения за счет окружающей среды (технологии free cooling) действительно недостаточно для поддержания работы современных микропроцессоров, использующихся для задач ИИ. Поэтому иммерсионное охлаждение серверов становится все более востребованным. Например, данную технологию тестирует Hewlett Packard Enterprise на своих суперкомпьютерах, а также Meta — на стандартных серверах. Ее основное преимущество в том, что тепло передается жидкости не через воздух, а непосредственно от нагревающихся элементов: процессоров, материнских плат, блоков питания, дисков и т. д. Это намного эффективнее».*

Иммерсионные системы охлаждения бывают двух типов:

- однофазные — в них хладагент всегда остается в жидком состоянии и циркулирует между резервуаром и сервером с помощью насосов;
- двухфазные — предполагают закипание хладагента при контакте с нагретыми компонентами сервера, вследствие чего хладагент поднимается в виде пара и конденсируется в охлаждаемом водой теплообменнике.

Интересно, что горячий хладагент можно применять для решения задач, которые напрямую не связаны с работой ЦОД, — например, для отопления офисов и технических помещений.

При использовании иммерсионной системы охлаждения сервер должен соответствовать определенным требованиям. В первую очередь это отсутствие вентиляторов и наличие антикоррозионной защиты разъемов и блоков питания. Кроме того, может потребоваться замена некоторых компонентов — например, вместо жестких дисков ***(HDD)*** лучше подойдут твердотельные накопители ***(SSD)***. А перед полноценным запуском рекомендуется тщательно протестировать инфраструктуру.

Необходимо подумать и о физической безопасности объектов с таким типом охлаждения. Для ее обеспечения требуется:

- использовать наклонные полы, специальные стоки, аварийные поддоны под резервуарами, а также датчики протечек — на случай утечки жидкости;
- применять химически стойкие материалы в местах контакта с хладагентом;

* Meta признана в РФ экстремистской организацией.

Работу ЦОД для ИИ можно четко разделить на две фазы: первая связана с обучением ИИ-модели и требует максимальной мощности и энергопотребления, а вторая обеспечивает эксплуатацию приложений и не «съедает» такого количества ресурсов

- задействовать систему хранения и утилизации отработанной жидкости.

Если же говорить о внешней инфраструктуре, то для обслуживания серверов с иммерсионным охлаждением необходимы специальные подъемники и высококвалифицированный технический персонал. А эффективная работа систем требует постоянного многоуровневого мониторинга, данные для которого должны собираться многочисленными датчиками давления, температуры и чистоты хладагента.

В будущем альтернативой иммерсионным системам могут стать разработки на основе графеновых технологий охлаждения: их теплопроводность в 2,5 раза больше, чем у меди. Согласно испытаниям IBM, графеновые радиаторы охлаждают на 40% эффективнее, чем классические системы при тех же габаритах. Тепловые трубки из графена уже установлены на суперкомпьютере Fugaku в Японии.

На долю рынка систем охлаждения, вероятно, смогут претендовать и решения, которые используют магнитокалорический эффект изменения температуры под действием магнитного поля. Однако они требуют дорогостоящих материалов ***(например, гадолиния и его сплавов)***, которые способны нагреваться при намагничивании и охлаждаться при размагничивании. Согласно исследованию EU Magnetica, подобные решения по эффективности втрое превосходят чиллеры с водяным охлаждением.

Распределение нагрузки и цифровой самописец

Немаловажным в работе ИИ-ориентированного дата-центра является качественное управление ресурсами. Классический ЦОД — это объект с хорошо прогнозируемыми показателями энергопотребления и мощности охлаждающих систем. При этом режим его работы не сильно зависит от времени дня и различных сезонных событий. С ИИ-ориентированным ЦОД дело обстоит иначе. Его работу можно четко разделить на две фазы: первая связана с обучением ИИ-модели и требует максимальной мощности и энергопотребления, а вторая обеспечивает эксплуатацию приложений и не «съедает» такого количества ресурсов.

Для перехода между режимами необходима интеллектуальная система управления, регулирующая работу инженерной инфраструктуры. Чтобы автоматизировать управление операциями и сетевыми ресурсами, создают программно-определяемые центры обработки данных ***(Software-Defined Data Centers, SDDC)***. Зачастую они используют ИИ для мониторинга событий, происходящих в инженерной инфраструктуре, и регулировки нагрузки на подсистемы ЦОД.

Кроме того, следует предусмотреть и планируемое введение в России законодательных норм, устанавливающих ответственность за ущерб, причиненный ИИ. Они изменят роль инфраструктуры: она будет не просто вычислительной базой, а системой доказательств.

Максим Андрианов

«Организациям потребуется поддерживать архив с различными версиями данных, моделей и параметров, а также документировать одобрения и результаты проверок и фиксировать все действия в защищенных журналах. Помимо этого, придется вести мониторинг производительности и качества, реагировать на инциденты, обеспечивать возможность откатить или остановить работу модели. В обязательный перечень войдут и требования по контролю доступа и управлению сторонними решениями. Фактически ИИ-инфраструктура должна будет функционировать как цифровой самописец, обеспечивающий прозрачность и аудируемость всего жизненного цикла модели».

Важны не только технологии, но и люди

Необходимость запуска все большего числа центров обработки данных для искусственного интеллекта повышает спрос на высококвалифицированных электриков, сантехников и строителей. По мнению генерального директора Nvidia Дженсена Хуанга, такие специалисты будут получать шестизначные зарплаты.

Как отметил Хуанг на Всемирном экономическом форуме в Давосе в 2026 году, бум в этой области уже наблюдается, зарплаты выросли почти вдвое. Он подчеркнул, что каждый сможет хорошо зарабатывать и для этого не нужна докторская степень по информатике.

Однако пока специалистов в этой области не хватает и кадровая ситуация напряженная. К примеру, за 2025 год штат IXcellerate вырос примерно на треть — пришли около 80 новых сотрудников. В компании рассказали, что поиск опытного специалиста с высокой квалификацией может занимать от двух до трех месяцев.

Сергей Вышемирский

«В 2026 году, в связи с запуском двух новых дата-центров, у нас открыто несколько десятков вакансий, которые необходимо закрыть к моменту ввода объектов в эксплуатацию. Для решения кадрового вопроса в долгосрочной перспективе мы развиваем сотрудничество с профильными вузами — в первую очередь с НИУ МЭИ. Наши специалисты участвуют в адаптации учебных программ и выступают в роли гостевых лекторов, а студенты проходят у нас стажировку. По итогам 2025 года первая группа практикантов была трудоустроена на постоянной основе: из 5–7 стажеров технического департамента 4–5 человек остались в компании».

Обмен опытом, поддержка со стороны коллег и вендоров особенно важны в решении кадрового вопроса, уверен и Всеволод Воробьев. Он уточнил, что в отношении ЦОД для ИИ корректнее говорить о поиске даже не сантехников широкого профиля, а более узких специалистов по климатике.

Всеволод Воробьев

«Системы вентиляции и кондиционирования на таких объектах отличаются от тех, что используются в обычных дата-центрах. Эти технологии мало распространены на рынке, поэтому дефицит сервис-менеджеров и инженеров, которые могут их обслуживать, остро чувствуется, причем не только в регионах, но и в крупных городах, в том числе в российской столице».

Впрочем, эксперт считает, что специалиста по бытовым кондиционерам, как и электрика, достаточно быстро можно переобучить для работы в ИИ-ориентированном ЦОД. И в России уже есть несколько организаций, которые предлагают такие курсы. К тому же в вузах открываются кафедры со специализацией по ЦОД.

А вот привлечение мигрантов вряд ли подойдет для восполнения дефицита кадров в этой области, потому что ЦОД являются частью критической инфраструктуры, что накладывает ограничения на допуск иностранных граждан.

ЦОД для искусственного интеллекта сегодня — отдельная инженерная цивилизация. Пока индустрия спорит, чей чип быстрее, настоящая битва за ИИ разворачивается на стройплощадках.

Логикор

Комплексное решение для эффективного сбора, анализа и управления большими массивами данных в режиме реального времени

ЕДИНАЯ ПЛАТФОРМА ДЛЯ ИТ, DEVOPS, SOC И ИБ

- сбор логов и других данных ИТ и ИБ систем
- снижение нагрузки на SIEM до 80%
- масштабируемая архитектура: до 1,000,000 EPS на приём
- глубокая аналитика «больших данных», AI-ready-данные
- оптимизация затрат на хранение и вычислительные ресурсы: до 5 ПБ данных в хранилище

Вы получаете оптимизированную инфраструктуру с высокой пропускной способностью и сниженными операционными затратами.

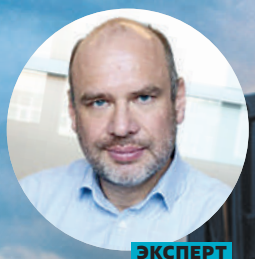
AXEL pro

INFO@AXEL.PRO

ЭКСПЕРТ

Игорь Дорофеев,

президент Ассоциации участников отрасли ЦОД



ЭКСПЕРТ

Всеволод Воробьев,

руководитель направления ЦОД центра сетевых решений компании «Инфосистемы Джет»

ДАННЫЕ НЕ ГОРЯТ

КАК ПОСТРОИТЬ ЦОД, КОТОРЫЙ ВСЕ ВЫДЕРЖИТ

Дефицит вычислительных ресурсов остается актуальной проблемой российского рынка, которая усугубляется постоянным увеличением нагрузки и расширением пула задач, возложенных на ИТ-инфраструктуру. Выход из ситуации — строительство новых ЦОД на современных принципах, главный из которых — высокая отказоустойчивость. По словам экспертов, именно выстраивание надежных центров обработки данных способно уберечь компании от остановки ключевых бизнес-процессов, которая может стоить значительных финансовых и репутационных потерь. О том, как сделать ЦОД по-настоящему надежным, читайте в нашем материале.

Для государственных заказчиков логичнее вложить максимум средств на этапе строительства ЦОД, минимизировав дальнейшие расходы на его эксплуатацию. Для коммерческих компаний дорогое обслуживание более приемлемо в условиях роста клиентского потока

Работа ЦОД должна быть согласована и сбалансирована уже на этапе проектирования. Если же этого нет, то в технологической цепочке образуется слабое звено, усиление которого станет непростой задачей

Более энергоэффективный ЦОД, как правило, по капитальным затратам будет дороже объекта, который потребляет больше электричества для совершения того же количества операций

Надежность ЦОД: от концепции до масштабирования

Надежность и устойчивость ЦОД — это первое, на что смотрят компании при выборе подходящего решения, наравне со стоимостью его покупки и эксплуатации. Заказчик должен быть уверен, что функционирование его оборудования не будет зависеть от влияния человеческого фактора и различных внешних воздействий, будь то природные катаклизмы или техногенные катастрофы. Причем такой подход характерен для всех отраслей экономики, начиная с промышленности и заканчивая ретейлом и финансовым сектором.

И это неудивительно, ведь сбой в работе ЦОД — не просто проблема конкретной компании или организации, а событие, которое потенциально может затронуть жизнь миллионов людей, причинив им значительные неудобства. К примеру, взрыв одного из аккумуляторов ЦОД Национальной службы информационных ресурсов Южной Кореи ***(NIRS)*** в сентябре 2025-го вызвал сильный пожар, в ходе которого была поражена ИТ-инфраструктура нескольких сотен государственных онлайн-служб. В их в числе оказались: госуслуги, налоговые сервисы, реестры недвижимости, торговая платформа и система экстренной помощи. Происходили громкие инциденты и в России: например, отключение обеих независимых линий питания в одном из ЦОД «Яндекса» в прошлом году привело к сбоям в работе сервисов «Яндекс.Музыка» и «Лавка».

Серьезность положения подтверждается и статистическими данными. Так, исследование Института Uptime ***(США)*** показало:

- Для более чем 54% компаний последний серьезный сбой в ЦОД обошелся в сумму, превышающую 100 тыс. долл. А каждый пятый респондент отметил, что суммарный ущерб для его организации составил более миллиона долларов.
- Проблемы с электропитанием — главная причина инцидентов, которые приводили к тяжелым последствиям. Вместе с тем доля значимых сбоев, вызванных ИТ- и сетевыми проблемами, в 2024 году достигла 23%.
- Большинство инцидентов в ЦОД, связанных с человеческим фактором, обусловлено тем, что сотрудники игнорировали инструкции либо эти документы были некачественно составлены.
- 80% операторов ЦОД считают, что более качественное управление позволило бы избежать последнего сбоя, что говорит о необходимости инвестирования в подготовку персонала.

Надежность и устойчивость ЦОД — это первое, на что смотрят компании при выборе подходящего решения, наравне со стоимостью его покупки и эксплуатации

Выработка концепции и проектирование ЦОД — это этапы, которые определяют облик будущего объекта. В связи с этим важен и выбор ИТ-решений, используемых при строительстве. Поэтому на таких этапах стоит сосредоточить максимум внимания, чтобы заложить базу для эффективной отказоустойчивой эксплуатации и удобства обслуживания техники

- За период с 2020 по 2024 год количество публично известных сбоев в компаниях финансовой отрасли снизилось с 11 до 3 случаев. Это связано с ужесточением нормативов, которое произошло после ряда крупных инцидентов.

- Активное развитие сервисов на базе искусственного интеллекта значительно увеличивает нагрузку на энергетические и охлаждающие системы ЦОД.

Для того чтобы не допускать инцидентов, необходимо повышать надежность работы центров обработки данных. Это позволит значительно сократить ущерб либо полностью его избежать.

Игорь Дорофеев

«Надежность любой технической системы, включая ЦОД, — это скорее качественный показатель, который не получится оценить в числовом выражении. Другое дело — такие параметры, как отказоустойчивость и работоспособность. Они зависят не только от топологии ЦОД, но и от оборудования, на котором она реализована. Важен при этом и человеческий фактор, поскольку неверные действия операторов могут привести к краху даже самую совершенную в техническом плане систему — например, вследствие отсутствия необходимого обслуживания либо из-за нарушения эксплуатационных процедур. То же самое касается физической безопасности, без обеспечения которой на объект могут проникнуть злоумышленники и устроить диверсию».

Выработка концепции и проектирование ЦОД — этапы, которые определяют облик будущего объекта. В связи с этим важен и выбор ИТ-решений, используемых при его строительстве. Поэтому на таких этапах стоит сосредоточить максимум внимания, заложив базу для эффективной отказоустойчивой эксплуатации и удобства обслуживания техники. Вместе с тем заказчик зачастую встает перед выбором: сделать ставку на объект с низкими капитальными затратами, но требующий более дорогостоящей эксплуатации, либо вложиться в более капиталоемкий на этапе строительства вариант, который будет обслуживаться с меньшими затратами.

Чаще всего окончательное решение по этому вопросу зависит от сферы, к которой относится организация. В частности, для государственных заказчиков логичнее вложить максимум средств на этапе строительства ЦОД, минимизировав дальнейшие расходы на его эксплуатацию. А для коммерческих компаний дорогое обслуживание будет более приемлемым в условиях увеличения прибыли, получаемой на фоне роста клиентского потока. Кроме того, для организаций важно время, которое требуется для запуска ЦОД в эксплуатацию. Как правило, ускорить этот процесс можно за счет использования более дешевых и менее энергоэффективных технологий.

Важно учитывать и возможность масштабирования нового ЦОД, которая должна соответствовать стратегии развития ИТ-инфраструктуры компании. В противном случае в какой-то момент организация может столкнуться с непреодолимыми технологическими барьерами, когда, например, новые стойки в ЦОД будет физически невозможно разместить из-за отсутствия необходимых ресурсов. Планировать развитие ЦОД рекомендуется с учетом всего его жизненного цикла, который в настоящее время составляет 15–17 лет, а в скором будущем может достигнуть 20 лет и более.

Планировать развитие ЦОД рекомендуется с учетом всего его жизненного цикла, который в настоящее время составляет 15–17 лет, а в скором будущем может достигнуть 20 лет и более

Игорь Дорофеев

«Всегда нужно помнить о том, что ЦОД — достаточно сложный технический объект, в котором взаимодействуют большое количество систем. Поэтому их работа должна быть согласована и сбалансирована уже на этапе проектирования. Если же этого не сделать, то в технологической цепочке образуется слабое звено, и усилить его станет непростой задачей, которую придется выполнять уже в ходе эксплуатации. К тому же достигнутый баланс работы также придется поддерживать весь срок эксплуатации ЦОД, постоянно выявляя и устраняя узкие места».

В уровнях отказоустойчивости дата-центров заказчикам помогают ориентироваться так называемые классификации инженерной инфраструктуры. В мире таких классификаций несколько, самыми известными на базе стандартов являются ISO/IEC 22237 с делением на Class 1–4, ANSI/TIA-942 с делением на Rate 1-4, а также справочный документ частной американской консалтинговой компании Uptime Institute с делением на Tier I-IV. При этом модели и методики хоть и отличаются, но в отношении отказоустойчивости четыре категории по смыслу гармонизированы друг с другом. Так, если центры обработки данных начального класса 1 при поломке отключаются, то ЦОД категории 4 продолжает работать в отказоустойчивой топологии.

Отказоустойчивость VS экономия: как найти баланс

Отказоустойчивость можно формировать на уровне инженерных систем или ИТ-инфраструктуры, а можно использовать комплексный подход — учитывать и то и другое. Выбор необходимого пути здесь будет зависеть от того, на чьей стороне решается эта задача. Например, организации, управляющие ЦОД, в которых установлена ИТ-инфраструктура клиента, могут влиять лишь на инженерные системы. Если же говорить с позиции клиента, то для усиления устойчивости он может, например, размещать собственную ИТ-инфраструктуру в различных ЦОД, выстраивая распределенную систему. При этом метрикой, на которую ориентируется бизнес, будет являться не только надежность систем, но и стоимость владения ими.

Игорь Дорофеев

«Разумеется, экономические показатели всегда будут сдерживать рост уровня отказоустойчивости ЦОД. Центры обработки данных никогда не приблизятся по этому показателю к космическим кораблям и подводным лодкам, в системах которых используется многократное резервирование, требующее дополнительных затрат. И это неудивительно, ведь ЦОД сейчас фактически массовый продукт, к которому предъявляются совсем иные требования. Никто не будет защищать такие объекты от нашествия инопланетян, ведь при наступлении этого события ЦОД уже не понадобится. Если же говорить о типовых рисках, то их учитывают. В частности, это могут быть такие события, как одиночные отказы. А вот в защиту от каскадных отказов компании уже вряд ли будут вкладываться».

Кроме того, по словам эксперта, при выборе ЦОД необходимо принимать во внимание ситуацию в компании и возможные внутренние риски, включая спор относительно прав собственности между владельцами объекта или дефицит средств, который приведет к невозможности обслуживания ИТ-инфраструктуры и последующим проблемам.

Почему резервирование не панацея для надежности

В области отказоустойчивости особое место занимает выбор схем резервирования ЦОД. И в этом

вопросе стоит разделять техническую и маркетинговую составляющие, поскольку зачастую применение определенной схемы подается как конкурентное преимущество дата-центра.

Игорь Дорофеев

«На деле использование той или иной схемы резервирования зависит скорее от условий эксплуатации и технического окружения объекта. Однако заказчик не должен забывать и о других аспектах — в частности, таких значимых, как пожарная безопасность или эксплуатационные процедуры. Ведь никому не нужен сгоревший ЦОД, пусть и с хорошей схемой резервирования».

С другой стороны, слабое резервирование инженерных систем зачастую подразумевает наличие дежурных бригад эксплуатации, содержание которых может себе позволить далеко не каждая организация, особенно если речь идет о небольшом объекте. В этом случае уровень резервирования имеет смысл повысить, увеличив время реакции на выход из строя оборудования. Тогда ЦОД будет способен работать после поломки до момента прибытия аварийной бригады, которая устранит неисправность. Такой же подход следует реализовывать и в ситуациях, когда временный выход ЦОД из строя не будет критичным для организации либо время простоя не обойдется слишком дорого для бизнеса.

Наряду с этим важно учитывать, что далеко не все сложные топологические решения и системы автоматизации повышают отказоустойчивость. Как правило, самая трудная задача в проектировании — сделать систему как можно более простой и элегантной. Простота конструкции сама по себе придает ей надежность за счет снижения количества точек отказа.

Вопросы энергии: почему дешевле не значит экономичнее

Энергоэффективность — один из ключевых показателей при оценке ЦОД потребителями. Любой такой объект необходимо питать электроэнергией, одновременно отводя вырабатываемое им тепло с помощью систем охлаждения. Через этот процесс проходит колоссальное количество энергии.

Более того, ЦОД сам является источником воздействия на окружающую среду: оборудование издает шум, а резервные дизельные генераторы заправляются топливом, которое теоретически может протечь и загрязнить почву, грунтовые воды и ближайшие водоемы. Наконец, ЦОД потребляет большое количество воды ***(особенно, если в нем установлена система испарительного охлаждения)*** и выбрасывает в атмосферу углекислый газ. Все эти факторы оцениваются с помощью соответствующих показателей:

Интересно, что PUE учитывает как объем электричества, который потребовался непосредственно для работы ИТ-систем, так и тот, что пошел на обеспечение этой работы. Однако при вычислении такого коэффициента не принимается во внимание факт того, что оборудование может потреблять электричество и в режиме ожидания, и при активных вычислениях. По этой причине для расчетов эффективности необходимы дополнительные показатели — в частности,

Как правило, самая трудная задача в проектировании ЦОД — сделать систему как можно более простой и элегантной. Простота конструкции сама по себе придает ей надежность за счет снижения количества точек отказа

В европейских странах энергоэффективные ЦОД намного более востребованы, чем в России, где вопросы экономии энергии часто отходят на второй план, уступая место стоимости оборудования

оценивающие, сколько электроэнергии ЦОД затрачивает на выполнение определенного количества операций. Анализ таких показателей позволяет компаниям оптимизировать работу ЦОД и в сфере инженерных систем, и в области ИТ-инфраструктуры.

Игорь Дорофеев

«Более энергоэффективный ЦОД, как правило, будет дороже объекта, который потребляет больше электричества для совершения того же количества операций. И его востребованность напрямую зависит от тарифов на электричество в той или иной стране. Поэтому в Европе такие ЦОД намного более востребованы, чем в России, где вопросы экономии энергии часто отходят на второй план, уступая место стоимости оборудования. Энергоэффективные решения зачастую просто не окупаются на территории РФ. Но с ростом стоимости ресурсов отношения и подходы к вопросу существенно меняются».

Особое значение эксперты придают параметру PUE, показывающему, сколько из выделенной мощности будет использовано для полезной работы серверного оборудования.

Всеволод Воробьев

«Именно PUE играет решающую роль при выборе оптимальной площадки и архитектуры ЦОД. Энергопотребление лишь расширяется с ростом нагрузок, которые принимает на себя современная ИТ-инфраструктура. А необходимость снизить энергозатраты на работу систем охлаждения приводит, например, к развитию технологии жидкостного охлаждения, а также направления free cooling (свободное охлаждение с помощью наружного воздуха). Наряду с этим жидкостное охлаждение имеет особенно низкий PUE и применяется в стойках повышенной вычислительной мощности на 100–150 киловатт, в частности используемых под ИИ».

Когда энергия рядом

Одна из перспективных тенденций в области энергоэффективности — строительство ЦОД рядом с электростанциями различного типа ***(как тепловыми, так и АЭС/ГЭС)***. При этом близость к таким объектам сама по себе обеспечивает высокий уровень физической безопасности, поскольку они являются стратегическими и хорошо защищены. К тому же данная связка ЦОД с электростанцией резко повышает его энергоэффективность, поскольку минимизирует потери, связанные с передачей электроэнергии на большие расстояния.

Такая стратегия в полной мере вписывается в ресурсоориентированную модель размещения ЦОД и, помимо перечисленных преимуществ, имеет свои слабые места — в частности, сложности с выстраиванием каналов связи и набором квалифицированного персонала для удаленных объектов. Подобный вариант может подойти компании в случае, если ЦОД используется для очень ресурсоемких операций — например, обучения моделей искусственного интеллекта, для чего необходимы огромные затраты энергии.

Если же говорить о клиентоориентированной модели, то в ее рамках заказчики стремятся разместить ЦОД поближе к центрам потребления, которые чаще всего находятся в крупных городах.

Бремя управления: ИИ советует, человек решает

Эффективно управлять ЦОД невозможно без понимания происходящих в нем процессов, мониторинг которых необходимо вести постоянно. С другой стороны, тотальный контроль с помощью тысяч датчиков на всех уровнях инфраструктуры будет избыточным и слишком дорогостоящим. Золотая середина на сегодняшний день состоит в мониторинге ключевых параметров ЦОД с помощью ИИ.

Результаты ИИ-анализа будут предоставлены операторам: они увидят целостную картину происходящего, а также с помощью предиктивной аналитики получат прогнозы вероятных событий. Как правило, такая схема работы позволяет грамотно распределить ресурсы на обслуживание ЦОД и, таким образом, обеспечить его надежную и бесперебойную работу. В настоящее время уже началось внедрение ИИ для анализа процессов в крупных ЦОД, и это направление имеет хорошие перспективы развития.

По словам экспертов компании «Инфосистемы Джет», каждый современный ЦОД необходимо в обязательном порядке оснащать системами автоматизации, диспетчеризации и резервного управления. Только с их помощью можно контролировать огромное количество параметров, поступающих от многочисленных устройств и механизмов. Эти системы собирают показатели, анализируют их и выдают соответствующие рекомендации. А если в их работе задействован искусственный интеллект, специалисты могут получить детальные прогнозы технического состояния устройств и подготовиться к их возможному выходу из строя — в частности, запланировав для службы эксплуатации проведение технических работ.

Каждый современный ЦОД необходимо в обязательном порядке оснащать системами автоматизации, диспетчеризации и резервного управления. Только с их помощью можно контролировать огромное количество параметров, поступающих от многочисленных устройств и механизмов.

Всеволод Воробьев

«В настоящее время ИИ пробуют использовать для управления работой ЦОД, однако такие попытки являются скорее смелым экспериментом. Мы же пока придерживаемся консервативных взглядов: окончательные управленческие решения всегда должен принимать человек, который может руководствоваться множеством показателей и подсказок, в том числе от систем искусственного интеллекта».

Надежность малых форм

Основная задача периферийных ЦОД — сбор и предобработка данных, которые компаниям невыгодно отправлять из региона в центральный ЦОД *(например, находящийся в Москве)*. С другой стороны, такие объекты необходимы для тех сфер применения, где для работы техники требуется низкая задержка *(Latency)* при передаче информации, что актуально, например, для беспилотного транспорта. В этом случае периферийные ЦОД должны стоять вдоль дорог — например, по одному объекту на каждые 100 километров пути, что обеспечит приемлемую задержку, не превышающую 5 миллисекунд.

Всеволод Воробьев

«В качестве периферийных часто могут выступать модульные ЦОД: высокая скорость их производства и удобство транспортировки позволяют разместить такие дата-центры максимально близко к объектам генерации данных, в том числе удаленным. При этом ЦОД сразу же находится в состоянии заводской готовности, что само по себе является гарантией его высокой отказоустойчивости. Как правило, модульные ЦОД ставят в филиалах и вблизи различных промышленных объектов — например, месторождений полезных ископаемых, где ведется их добыча. Нередко подобные ЦОД объединяют в распределенную корпоративную сеть, конфигурация которой обеспечивает надежность хранения и обработки данных компании».

От неопределенности к адаптивности

В настоящее время центры обработки данных развиваются в условиях технологической неопределенности. С одной стороны, это значительный рост энергопотребления и производительности вычислительной инфраструктуры, а с другой — кратное увеличение нагрузки и задач, которые должны выполняться в ЦОД *(включая обеспечение работы ИИ-сервисов, чему посвящена отдельная статья в этом номере)*.

Такое положение вещей еще больше повышает значимость работы дата-центров и ужесточает требования к их отказоустойчивости и гибкости. Проектировать и строить такие объекты, закладывая в них большую адаптивность и надежность, — приоритетные задачи инженеров. И от их решения во многом зависит развитие и модернизация российской ИТ-инфраструктуры в будущем.

ЕДИНСТВО ТОЧЕК

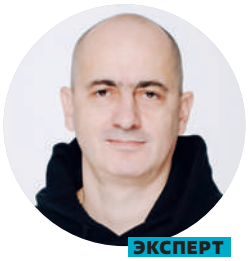
СЕКРЕТ АНТИХРУПКОЙ ИНФРАСТРУКТУРЫ, СОХРАНЯЮЩЕЙ РАВНОВЕСИЕ ПРИ АТАКЕ

Сегодняшние киберпреступники, используя самые продвинутые технологии, могут преодолеть любую защиту ИТ-инфраструктуры — даже самую современную и дорогую. Выход из положения остается один — построение архитектуры в соответствии с концепцией антихрупкости. Особую роль в работе такой структуры играют балансировщики. Они правильно распределяют нагрузку по слоям и элементам системы, чтобы повысить ее живучесть во время атак и облегчить масштабирование сервисов. О том, как правильно использовать эти устройства, JetInfo рассказали эксперты компании «Инфосистемы Джет».

ЭКСПЕРТ

Александр Копылов,

руководитель группы сетевой безопасности компании «Инфосистемы Джет»



ЭКСПЕРТ

Павел Михайлик,

архитектор центра сетевых решений компании «Инфосистемы Джет»

- При реализованной концепции антихрупкости система продолжает работать во время атак за счет разделения на множество независимых узлов
- Балансировщики распределяют нагрузку только между «живыми» (работающими) элементами системы и дают возможность с легкостью ее расширять
- Мишень, по которой стреляют хакеры, прикреплена именно к балансировщику, что говорит о важности модернизации его ПО в случае наличия в нем уязвимостей

На всех уровнях

Киберпреступники все чаще переходят от кражи данных к полному уничтожению ИТ-инфраструктуры компании, что может привести бизнес к краху.

Александр Копылов

«Согласно исследованию, проведенному нашей компанией, в 2025 году доля деструктивных инцидентов, нацеленных на уничтожение инфраструктуры, достигла 76%. Мы видим смену модели угроз: хакеры перешли от тактики шпионажа к вандализму. Единого защитного барьера при таких рисках недостаточно — необходимо обеспечивать автономность и изоляцию каждого узла в отдельности».

По словам эксперта, разделение системы на множество независимых узлов позволяет создать антихрупкую ИТ-архитектуру, дающую возможность продолжать работу во время атак. Те из узлов, что не пострадали от действий хакеров, возьмут на себя функции выбывших элементов, что обеспечит поддержку бизнес-процессов и целостность информации.

И речь здесь идет обо всех уровнях ИТ-инфраструктуры, а не просто о нескольких автономных ЦОД. В случае реализации этого подхода отказ любого из компонентов не сможет повлиять на функционирование конечных сервисов или приложений для пользователей. Антихрупкость подразумевает, что сбой не просто купируется, а становится источником новой информации. В такой архитектуре при инциденте на любом узле система автоматически адаптирует политики безопасности для остальных сегментов. Это позволяет не просто вернуться в бизнес, а выйти из кризиса более защищенными, чем до него.

Одно из основных условий работоспособности такой системы — связанность ее различных уровней друг с другом. Причем она должна сохраняться и в случаях масштабирования и модернизации, когда необходимо учитывать нюансы взаимодействия всех сопряженных между собой уровней. Фактически это означает, что даже при устранении небольшой проблемы ИТ-инфраструктура должна рассматриваться специалистами как единый механизм, все составляющие которого взаимосвязаны.

Архитектура самодостаточности

Сетевая инфраструктура обеспечивает корректное сопряжение и взаимодействие между различными

сервисными слоями, в том числе выполняющими функции безопасности. В этом смысле балансировка нагрузки между защитными решениями дает возможность провести качественное масштабирование при выстраивании и расширении комплексной архитектуры в ИТ.

Павел Михайлик

«Хотя сеть и балансировщики не выполняют функции безопасности, они позволяют оптимальным образом интегрировать инструменты ИБ в общую систему».

Идея антихрупкой ИТ-архитектуры состоит в том, что каждая точка присутствия вычислительных мощностей *(такая как ЦОД, например)* должна быть самодостаточной. И одно из необходимых условий для этого — распределение нагрузки между точками с учетом их мощности и текущего состояния.

Рядом с мишенью

Если российские разработчики балансировщиков не внедряют в них функции безопасности *(за исключением базового файрволинга — например, L4)*, то в ряде иностранных решений эти опции присутствуют. Например, решение от F5 Networks в рамках единого шасси реализует совместную работу балансировщика с web application firewall, который защищает веб-приложения от внешних угроз, фильтруя трафик на сетевом уровне.

Это оправданно, поскольку злоумышленники в ходе атаки могут скомпрометировать и использовать балансировщик, как и любое другое сетевое устройство. Например, если в сетевом либо программном стеке имеется уязвимость, позволяющая провести неправомерную транзакцию. А если движок балансировщика при получении такого запроса позволит установить соединение и получить доступ, то для организации это станет проблемой, которую нужно будет срочно решать службе ИБ.

Павел Михайлик

«Мишень, по которой стреляют хакеры, прикреплена именно к балансировщику, что говорит о значимости модернизации его ПО в случае наличия в нем каких-либо уязвимостей».

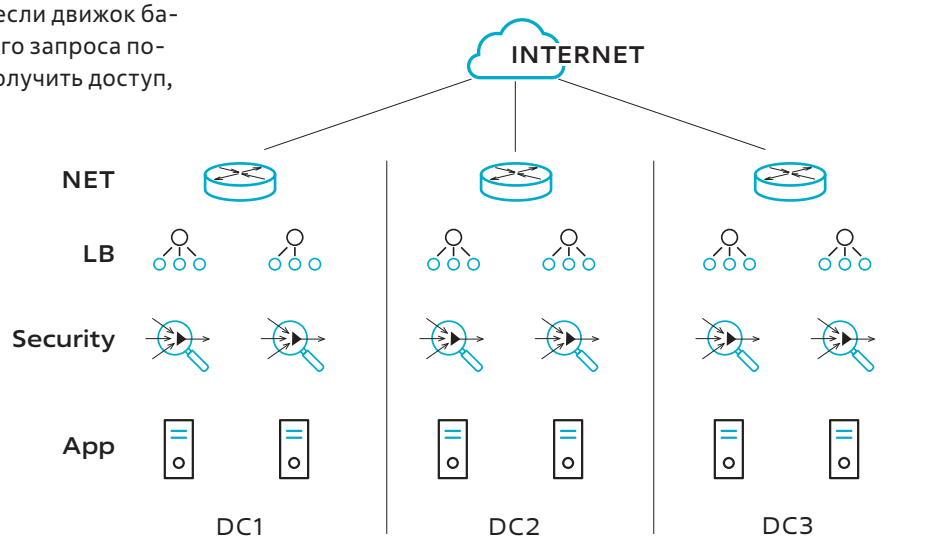
По словам эксперта, имеет смысл также совмещать балансировщики с Anti-DDoS-системами. Несмотря на то, что такие системы — это отдельные продукты, разрабатываемые другими вендорами, у них под капотом чаще всего работает веб-сервер на базе Nginx, что позволяет интегрировать их с балансировщиками, которые работают на основе коммерческой доработки такого же движка *(Nginx)*.

В настоящее время продукты на основе подобной коллаборации не представлены на нашем рынке, однако они могут появиться в будущем, если вендоры реализуют эту идею.

Впрочем, описанный подход может применяться далеко не в каждом случае, и требуется предварительная оценка для принятия решения о его использовании.

Павел Михайлик

«При такой консолидации слоев возможно существенно упростить архитектуру, но, с другой стороны, данная связка элементов может оказаться нерациональной с точки зрения производительности — если на единицу процессорной мощности будет приходиться слишком много функционала. Поэтому



БАЛАНСИРОВКА ВХОДЯЩЕЙ НАГРУЗКИ МЕЖДУ ЦОД

Даже при устранении небольшой проблемы ИТ-инфраструктура должна рассматриваться специалистами как единый механизм, все составляющие которого взаимосвязаны

в каждом конкретном случае заказчику потребуется взвешивать все за и против, выбирая оптимальный вариант именно для своей ИТ-инфраструктуры».

Расширяя слой

Средство балансировки, которое работает со слоем ИБ-решений, в первую очередь должно обеспечивать корректную сигнализацию о доступности того или иного сервиса безопасности, чтобы нагрузка на него распределялась, только когда он «живой» *(работает)*. С другой стороны, чтобы правильно распределить нагрузку между сервисами для обеспечения отказоустойчивости, необходимо учитывать, что каждый узел этого слоя имеет собственную емкость.

Павел Михайлик

«С помощью балансировщика мы можем отслеживать состояние каждого отдельного узла и вовремя переключать между ними нагрузку в случае какого-либо сбоя, что повышает общую надежность системы. А кроме того, у специалистов появляется возможность расширять этот сервисный слой, добавляя в его ресурсный пул дополнительные элементы и произвольно увеличивая емкость по мере роста нагрузки на инфраструктуру, причем не перестраивая ее архитектуру. Таким образом, упрощается процесс масштабирования инфраструктуры и улучшается ее адаптивность к различным условиям работы».

В качестве сервисов безопасности тут могут выступать решения широкого спектра — от межсетевых экранов нового поколения до Anti-DDoS- и Anti-Bot-систем. Последние используются преимущественно в банковской сфере для защиты от атак, которые имитируют массовое поведение реальных пользователей, перегружающее сайты и приложения.

Симметрия трафика

Александр Копылов

«При грамотном применении инструментов балансировки на сетевом уровне и уровне приложений мы реализуем ключевой принцип антихрупкости: пересоздавать проще, чем чинить. Это дает возможность в любой момент заменять скомпрометированные элементы на “стерильные” шаблоны, не меняя общую архитектуру и не останавливая бизнес. Кроме того, такие инструменты обеспечивают симметрию и дешифровку трафика — и это дает нам необходимую наблюдаемость для работы адаптивных политик ИБ. В момент атаки система не превращается в “бетон”, а динамично перестраивается, становясь защищеннее и сильнее с каждым отраженным ударом».

Вклад балансировщиков в киберустойчивость наблюдается и на уровне провайдеров мобильного и проводного интернета. Они используют технические средства противодействия угрозам *(ТСПУ)* как для защиты сети, так и для контроля доступов в собственных каналах передачи данных. Технически это реализуется с помощью отведения трафика на ферму с внутренними балансировщиками. Проходящий через нее трафик фильтруют, чтобы выявить попытки проведения DDoS-атак и отправки различных зловредных приложений. Здесь же реализуется возможность ограничить доступ пользователей к ряду интернет-ресурсов — в частности, мошеннических.

По словам экспертов компании «Инфосистемы Джет», именно правильная балансировка нагрузки сейчас становится связующим звеном при создании антихрупкой ИТ-архитектуры на всех уровнях — от взаимодействия между ЦОД до процессов внутри сервисных слоев. Благодаря такой архитектуре бизнес получает не просто отказоустойчивую систему, а гибкую среду, способную динамически перестраиваться под атакой и адаптироваться к новым угрозам без остановки процессов.

ГЕОРГИЙ РУДЕНКО,

CISO крупного банка, лауреат рейтинга «Топ-25 директоров по кибербезопасности» 2025 года по версии Ассоциации менеджеров и ИД «Коммерсантъ»

«НАИБОЛЕЕ НЕДООЦЕНЕННЫЕ ТИПЫ АТАК — САМЫЕ ПРОСТЫЕ»

Место съемки: «Киберэтаж» — клубное пространство для работы и встреч (Москва)

Лавина киберинцидентов меняет ИТ-ландшафт. Вопрос «Как под нее не попасть?» сменяется другим: «Как под ней не лечь?» О том, почему руководитель информационной безопасности сегодня должен мыслить категориями бизнеса, на чем строится киберустойчивость и где проходят «пороги боли», редакция JetInfo поговорила с Георгием Руденко, CISO крупного банка. Финансовый сектор — цель номер один для злоумышленников, поэтому опыт нашего героя — это проверка теорий ИБ-защиты практикой отражения реальных атак.

Георгий, предлагаю начать с основ. Чем сегодня киберустойчивость отличается от кибербезопасности?

Киберустойчивость — это способность бизнеса не только предотвращать атаки, но и быстро восстанавливаться после них с минимумом потерь. В отличие от классической кибербезопасности, которая фокусируется лишь на предотвращении атак, киберустойчивость подразумевает проактивное планирование непрерывности бизнеса *(business continuity planning, BCP)* и постоянную готовность к инцидентам.

Если киберустойчивость требует проактивного подхода, то как это отражается на роли руководителя ИБ? Судя по всему, приоритеты CISO за последние годы должны были сильно сдвинуться.

Основное изменение для директоров по информационной безопасности — в смещении их роли в сторону интересов бизнеса. Компании все чаще требуют от CISO более широкого взгляда на проблемы и глубокого погружения в специфику организации, поиска сбалансированных решений с учетом интересов всех стейкхолдеров. Получается, что технический эксперт должен трансформироваться в менеджера, который выстраивает процессы под ключ, принимая во внимание все ожидания бизнеса.

А эти ожидания могут быть разными, например:

- обеспечивать соответствие требованиям законодательства;
- улучшать практическую защищенность от кибератак;
- увеличивать прозрачность работы подразделения ИБ;
- менять подходы к работе и культуру в команде;
- повышать эффективность в реализации бизнес-инициатив;
- упрощать процессы, наращивать скорость работы;
- укреплять доверие к компании со стороны клиентов;
- оптимизировать расходы на информационную безопасность.

Руководителю ИБ важно уметь работать со всеми задачами из этого списка, а не сосредоточиваться только на соответствии ИТ-инфраструктуры требованиям в области безопасности и на повышении ее практической защиты, как это часто бывает.

А как все это транслируется на уровень бизнеса? Насколько киберустойчивость встроена в корпоративную стратегию и есть ли у нее измеримые KPI?

В корпоративной стратегии киберустойчивость может упоминаться, но обычно без деталей. Проработанные нюансы, как правило, прописываются в отдельном документе *(технологическая стратегия, стратегия информационной безопасности и т. п.)*. На уровне всей организации самое главное — зафиксировать измеримые результаты в достижении основных целей:

подготовиться к инцидентам и успешно восстановиться после них. Бизнес определяет продолжительность простоя и объем потери данных, которые он выдерживает, а служба ИТ/ИБ обеспечивает выполнение ожиданий. В этом смысле RTO и RPO — базовые KPI устойчивости, потому что они задают границы допустимого простоя и допустимой потери данных.

Если говорить о практике: к чему готовиться ИТ-отрасли в 2026 году? Какие атаки вы считаете наиболее вероятными, а какие — самыми недооцененными?

Все, что связано с социальной инженерией, было и будет актуальным. Если строить прогноз, опираясь на аналитические отчеты за прошлый год, то высокую популярность сохранят атаки на цепочки поставок, а также использование программ-вымогателей *(ransomware)*. А бурное развитие технологий, включая искусственный интеллект, уже позволяет снизить стоимость реализации этих атак для злоумышленников. Особенно сильно может пострадать малый и средний бизнес, который не инвестирует достаточно средств в свою безопасность.

Кроме того, стоит помнить, что наиболее недооцененные типы атак — самые простые. Многие ИБ-специалисты начинают анализировать сложные и редкие сценарии, не обеспечив полностью базовые потребности в защите. Например, выполнив один раз какие-то проверки, успокаиваются и не выстраивают процессов контроля; открывают доступ — и потом забывают его пересмотреть. Частой проблемой команд безопасности является низкий уровень инженерной культуры: не выполняются актуальные обновления, не контролируется полнота покрытия инструментов, отсутствует регулярный пересмотр политик безопасности и процесса управления исключениями. Именно из-за этого многие простые атаки достигают цели.

А как компаниям проверить, что они действительно готовы к кризисным сценариям? Какие методы тестирования вы считаете эффективными?

К основным методам проверки относятся:

- **Оценка практической защищенности путем имитации кибератак.** Можно проводить пентесты для поиска уязвимостей в обозначенном скоупе систем/инфраструктуры. Либо выбрать формат учений «красной команды» *(red teaming)* для симуляции атак с конкретной целью и полным реагированием со стороны SOC. Полезно собрать «фиолетовую команду» *(purple teaming)*, когда нужно проверить эффективность практической работы службы мониторинга и реагирования на конкретных тактиках и техниках атак *(use-case validation)*.

- **Тестирование возможности восстановления.** Для этого необходимо проводить DR/BCP-тесты. Они позволяют убедиться в том, что заявленные RTO/RPO достижимы на практике, включая восстановление из бэкапов, репликацию, аварийное переключение *(failover)*.

- **Разбор каждого крупного инцидента и подготовка плана улучшений.** Важно фиксировать, что сработало / не сработало в защите, и закрывать системные причины, а не симптомы. Не лишним будет изучить уроки, полученные другими компаниями в результате инцидентов, — то есть необходимо поддерживать контакт с CISO разных организаций *(для обмена опытом)*.

- **Организация Tabletop-учений *(настольных)*.** Они менее эффективны на практике, однако помогут проверить, не был ли упущен какой-то важный этап в общем антикризисном плане. Анализ типовых сценариев *(ransomware, утечки данных, отказ в работе услуг провайдера и др.)* позволяет оценить роли всех участников, детально рассмотреть внутреннее взаимодействие, PR-коммуникации и т. п.

Георгий, давайте заглянем в будущее. Какой вы видите идеальную модель киберустойчивости, скажем, на горизонте пяти лет?

Идеальная модель — это когда устойчивость встроена во все бизнес-процессы организации: определены и зафиксированы «пороги боли» *(те же RTO/RPO по сервисам)*, а технологии и процессы позволяют эти пороги выдерживать при динамическом изменении внешней и внутренней среды. Разумеется, все это должно работать с минимальными затратами ресурсов и минимальным участием человека.

Какой принцип в ИБ вы считаете критически важным?

Все рано или поздно ломается. Даже если в моменте работает хорошо. Поэтому периодически стоит проводить аудит эффективности работы всех процессов и инструментов ИБ, даже если кажется, что там нет никаких проблем.

ЗАЩИТНЫЙ КИБЕРКОСТЮМ ДЛЯ РИСК-МЕНЕДЖМЕНТА

КАКИЕ ИБ-РИСКИ ПОКРЫВАЕТ КИБЕРСТРАХОВАНИЕ И ПРИ ЧЕМ ЗДЕСЬ СЛОМАННЫЙ ЗАМОК

На российском рынке киберстрахования сейчас переломный момент. Эффект накопленной критической массы наконец сработал: активное импортозамещение технологий, громкие ИБ-инциденты и штрафы за утечку данных перевели киберстрахование из разряда экзотики для избранных в объективную необходимость для системного риск-менеджмента. О том, как меняется подход бизнеса к ИБ-рискам и какие из них берет на себя киберстрахование, редакции JetInfo рассказали в компании «СОГАЗ».

По данным страхового брокера Mains, в 2025 году объем российского рынка киберстрахования составил 3,5–4 млрд руб. Есть все предпосылки для его уверенного роста в ближайшие годы. К 2027 году рынок вполне способен достичь 5 млрд рублей.

Первый и главный драйвер — сама природа угроз. Атаки сегодня — это сложные многоступенчатые кампании с использованием автоматизации, ботнетов и вредоносного ПО. Для бизнеса это означает переход ущерба в совсем иную весовую категорию. Когда инцидент в производственной сети крупного промышленного предприятия приводит к простою, потери могут достигать десятков миллионов рублей в день.

В прошлом году крупное промышленное предприятие стало жертвой хакеров. Злоумышленники зашифровали данные в производственных системах и потребовали выкуп — в результате бизнес оказался парализованным. Предприятие привлекло экспертов для восстановления работы систем, провело расследование инцидента и предприняло шаги для снижения ущерба. «СОГАЗ» компенсировал затраты на услуги специалистов, восстановление данных, закупку дополнительного оборудования, а также убытки от простоя производства. Общая страховая выплата превысила 150 млн рублей.

Эта сумма вызвала резонанс на рынке. В настоящее время средняя страховая выплата по киберубыткам — от нескольких миллионов до нескольких десятков миллионов рублей.

От чего зависит крой защитного киберкостюма

Долгое время существовал стереотип: киберриски — удел гигантов. Это заблуждение. Малый и средний бизнес находится на линии огня автоматизированных атак. Злоумышленникам неважно, маленький вы интернет-магазин или крупный банк. Им важны данные карт, логины и доступ к инфраструктуре крупных подрядчиков через слабое звено.

От размера бизнеса зависит выбор продукта. Крупному бизнесу желателен индивидуальный «костюм» — программы, которые «шьются» под конкретную ИТ-архитектуру, с уникальными лимитами и учетом специфики производства. Для среднего и малого бизнеса такой подход может быть избыточен и дорог — для него подойдут отраслевые коробочные решения. Это готовый, понятный конструктор, который закрывает основные риски для конкретной сферы: онлайн-образование, медицина, логистика, ретейл.

Не обязательно быть экспертом в кибербезопасности, чтобы купить полис. Нужно просто понимать, что трехдневный простой сайта интернет-магазина — это потерянная выручка, которую, кроме страховой компании, никто не компенсирует.

В целом страхование киберрисков в «СОГАЗе» делится на две основные группы. Первая — это страхование ответственности перед третьими лицами, включая ответственность за разглашение корпоративной информации и персональных данных, а также за несанкционированный доступ к мультимедийному контенту. Вторая группа — это страхование убытков самого страхователя: затрат, связанных с перерывом в деятельности из-за кибератаки, и расходов на восстановление системы, расследование, уведомление о нарушениях или восстановление репутации.

Бизнес может получить комплексную защиту от последствий кибератак, сбоев в программном обеспечении и краж данных, а также застраховать риски, связанные с ошибками при переходе на новое программное обеспечение *(например, в процессе импортозамещения)*. Кроме того, страховой партнер может оказать помощь в локализации киберинцидента, реагировании и дальнейшем расследовании.

Убытки, которые страховщики, как правило, не готовы покрывать:

- связаны с нарушением законодательства;
- возникают в результате действий страхователя, которые суд признает преступлением;
- являются следствием умышленного совершения противоправных действий.

Сумма покрытия и лимиты по типу рисков зависят от различных параметров — например, от специфики деятельности компании и уровня информационной безопасности. Если предприятие не применяет никаких мер информационной безопасности, то это означает, что риск успешной кибератаки реализуется с вероятностью 100%. Стоит ли страховать автомобиль от угона, если у него сломаны замки на дверях, а завести его можно отверткой? Конечно, страховая компания предпочтет предложить выгодные условия бизнесу, уделяющему достаточно внимания защите своих данных. Поэтому любому предприятию важно повышать уровень собственной защищенности и включать киберстрахование в систему риск-менеджмента.

Если в компании внедрена усиленная система информационной защиты или страхуется не вся инфраструктура предприятия, а отдельные ИТ-системы, тариф может быть существенно снижен. И здесь зафиксирован позитивный тренд: компании, проходящие аудит для получения страховки, часто обнаруживают «дыры», о которых не подозревали, и усиливают свою защиту. Страхование становится активным инструментом управления безопасностью, стимулируя повышение киберустойчивости.

Однако мнение о том, что при сильной ИБ-защите хорошая страховка не нужна, ошибочно. Любой специалист из сферы информационной безопасности подтвердит, что взломать можно любую компанию. Если бизнес будет интересен злоумышленникам по экономическим или иным соображениям, то взлом — это лишь вопрос времени и ресурсов. ИБ и киберстрахование — комплементарные продукты, но никак не альтернативные.

Лидеры по защите от киберрисков

По данным «СОГАЗа», за 2025 год расширился спектр отраслей, интересующихся защитой от киберрисков. Наибольшую готовность к киберстрахованию проявляют представители финансовой, добывающей и нефтегазовой отраслей, социальной сферы и здравоохранения, промышленного сектора.

Заметен рост интереса к киберстрахованию со стороны авиакомпаний, предприятий розничной торговли, строительного бизнеса. Страховщики тоже защищают свои активы от последствий кибератак. Цифровые угрозы перестали быть экзотикой, превратившись в фактор, влияющий на устойчивость бизнеса в самых разных секторах экономики.

Перспективы и вызовы рынка киберстрахования

Один из вызовов развивающегося рынка киберстрахования — **дефицит большой статистики** и, как следствие, сложность стандартизации. Решение — в **кооперации**. Профессиональное сообщество нуждается в обмене обезличенными данными об инцидентах, а также в формировании единых стандартов оценки рисков и страхового покрытия. Без этого мы будем двигаться медленнее, чем хакеры.

С каждым днем появляется все больше кейсов, подтверждающих, что страховка от хакерских атак

оправдала себя. И обязательное киберстрахование — это уже не «если», а «когда». В первую очередь это касается **финансового сектора и критической информационной инфраструктуры**. Мотивация государства здесь очевидна: защита от системных рисков. Когда утечка данных клиентов в одном банке или остановка трубопровода из-за вируса создает угрозу для миллионов граждан и экономики в целом, добровольность уходит на второй план. Подобные инициативы сейчас рассматриваются на уровне регуляторов *(например, Министерства цифрового развития)*, поэтому вероятность реализации данного сценария существует.

Потенциал страхования киберрисков повышается благодаря поддержке этого направления государством. Например, теперь компаниям будет проще относить расходы на киберстраховку к затратам, что поможет снизить базу по налогу на прибыль и сделать страхование более выгодным.

В то же время интерес компаний к киберстрахованию усилился из-за ужесточения законодательства о персональных данных. Новая редакция федерального закона № 152-ФЗ предусматривает повышение штрафов, а также вводит отдельные составы ответственности за утечку биометрических и специальных категорий данных. Для крупных же компаний обязательным условием сотрудничества становится наличие киберстраховки у их подрядчиков и партнеров.

Важно понимать, что киберстрахование — это не просто покупка полиса, а выбор партнера по управлению рисками. Правильный страховщик не только выплатит компенсацию, но и поможет предотвратить крупные убытки и быстро восстановиться после инцидента.

ЧЕК-ЛИСТ

на что обращать внимание при страховании киберрисков

1. Потребности компании и актуальные риски

☐ Подумайте, от каких конкретно угроз вам нужна защита: остановка производства, утечка данных, ошибки сотрудников в области кибербезопасности, ошибки при внедрении ПО и др. Какие расходы может вызвать крупный киберинцидент?

Важно, чтобы страховое покрытие включало:

☐ расходы на расследование инцидента и услуги кризисных менеджеров;

☐ убытки от перерыва в деятельности (потерю прибыли);

☐ затраты на восстановление данных и систем;

☐ ответственность перед третьими лицами (клиентами, партнерами) из-за утечки их данных.

Для некоторых компаний может быть актуально покрытие последствий DDoS-атак или рисков, связанных с импортозамещением ПО, фишингом. Обязательно уточните, покрываются ли атаки, реализованные через подрядчиков.

2. Условия договора и исключения

☐ Проверьте общую сумму покрытия и отдельные лимиты по каждому типу рисков (например, лимит на расходы по расследованию).

☐ Обратите внимание на исключения: внимательно изучите раздел «Что не покрывается». Стандартные исключения: признание судом действий страхователя преступными; совершение умышленных противоправных действий; запланированный перерыв в работе информационной системы (например, для обслуживания); повторные события по вине страхователя, не устранившего первопричины инцидента после страхового случая.

На стоимость договора будут влиять различные параметры, в том числе специфика деятельности компании, уровень ИБ и т. д. Наличие сильной защиты может существенно снизить тариф. Кроме того, для экономии можно застраховать не всю инфраструктуру компании, а отдельные ИТ-системы по выбору страхователя.

3. Экспертная поддержка и процесс урегулирования убытков

☐ Уточните, предоставляет ли страховщик доступ к услугам партнеров (юристов, ИБ-экспертов, кризисных PR-менеджеров) на этапе реагирования.

☐ **Процедура уведомления:** выясните, как и в какие сроки нужно сообщить о страховом случае.

☐ **Опыт выплат:** попросите страховую компанию привести примеры реальных выплат. Наличие таких кейсов — признак опыта и надежности страховщика.

4. Выбор партнера

☐ Проверьте финансовые рейтинги надежности страховой компании (например, от «Эксперт РА», АКРА или НКР).

Отдавайте предпочтение страховщикам с подтвержденным опытом в киберстраховании и наличием специализированного подразделения.

Оцените индивидуальный подход:

☐ **для крупного бизнеса:** готов ли страховщик разработать индивидуальную программу страхования или предлагает только коробочный продукт?

☐ **для МСБ:** есть ли понятные и доступные коробочные решения с фиксированной стоимостью?

КРИЗИС ДОВЕРИЯ

КАК РАБОТАТЬ С ПОДРЯДЧИКАМИ БЕЗОПАСНО

АВТОР

Анна Коробецкая,

ведущий консультант по информационной безопасности компании «Инфосистемы Джет»

АВТОР

Станислав Громов,

менеджер по продвижению компании «Инфосистемы Джет»

Большинство российских подрядчиков защищены от кибератак гораздо хуже своих клиентов. При этом из-за неоправданно высокого доверия к поставщикам компании зачастую упускают контроль за ситуацией с ИБ. Уязвимость в инфраструктуре подрядчика становится удобной точкой для развития атак на его заказчиков. Неспроста число инцидентов растет на десятки процентов в год. Как же правильно оценить уровень рисков и выстроить совместную с партнером систему ИБ, чтобы сотрудничество было безопасным? Об этом рассказали эксперты компании «Инфосистемы Джет».

Лишь **36%**
компаний проводят аудит критичных поставщиков услуг

Предоставление подрядчикам избыточных прав доступа систематически приводит к ИБ-инцидентам

В **40%**
случаев подрядчики хранят аутентификационные данные от сервисов клиентов в незашифрованном виде

Уровень безопасности подрядчиков в основном оценивается с помощью опросных листов, что часто носит формальный характер

Партнерство как угроза

Доверие между партнерами — основа бизнеса, без которой сложно выстроить эффективное взаимодействие компаний и добиться успеха на рынке. Однако недостаточная защита инфраструктуры одной из сторон может спровоцировать кибератаки на ее партнеров. По результатам исследования CICADA8, в 2025 году большинство подрядчиков были слабо защищены от хакерских атак из-за наличия множества уязвимостей в ИТ-инфраструктуре — например, у 55% компаний-поставщиков для доступа из интернета был открыт как минимум один из управляющих портов.

Исключением тут не стали и поставщики ИТ-продуктов, для многих из которых работает правило «сапожник без сапог»: они пренебрегают собственными системами ИБ и защищены гораздо хуже своих клиентов. И дело тут не только в стремлении сэкономить на решениях для обеспечения информационной безопасности, но и в неумении выстроить эту крепость.

Именно поэтому киберпреступники все чаще выбирают подрядчиков в качестве наиболее простой и наименее ресурсозатратной отправной точки для развития атак на их клиентов. Это подтверждается и статистикой инцидентов. Так, по данным компании «Информзащита», количество кибератак на российские организации через их поставщиков в январе — марте 2025-го увеличилось на 80% по сравнению с тем же периодом годом ранее.

Желанной целью киберпреступников, как правило, выступает один из самых заметных игроков рынка, поскольку в случае компрометации такого поставщика в зоне риска оказываются все его клиенты. И если на стороне заказчиков меры безопасности не приняты, последствия могут стать фатальными.

Происходит это достаточно часто. Из-за сложившихся доверительных отношений с подрядчиком компания упускает точки контроля за его действиями внутри своего периметра. А вариант возникновения угрозы со стороны поставщика, которая приведет к инциденту ИБ, даже не рассматривается: подрядчик же не станет нам вредить?

Тем не менее бдительность организаций повышается, хотя и не быстро. Согласно исследованию компании «Инфосистемы Джет» ***(«Курс на киберустойчивость: как изменились стратегии CISO»)***, в 2024 году 36% компаний проводили собственный или независимый аудит критичных поставщиков услуг, тогда как в 2023-м это делали лишь 17% респондентов. Кроме того, с 19% до 48% выросла доля компаний, у которых имеется документ, регламентирующий меры безопасности при работе с подрядчиками.

Коллекция заблуждений

Несмотря на большое количество атак, специалисты многих организаций по-прежнему не владеют всей необходимой информацией об угрозах и находятся во власти стереотипов. Перечислим наиболее распространенные из заблуждений вместе с их опровержениями:

«Чем компания известнее и больше — тем она безопаснее»

Размер и популярность компании никак не влияют на уровень зрелости информационной безопасности. На практике неуязвимых компаний не существует, и даже такие крупные игроки, как CISCO, не стали исключением: 10 августа 2022 года ее представители подтвердили факт взлома своих корпоративных систем.

«Анкеты по информационной безопасности достаточно для оценки уровня защищенности подрядчика»

Это не так, поскольку невозможно проверить достоверность всех данных, указанных в анкете. Очень часто подрядчики умышленно завышают свои возможности в области ИБ, выдавая желаемое за действительное.

«Подрядчик в полной мере отвечает за безопасность своих услуг»

Риски информационной безопасности передаются по цепочке, и каждой компании приходится брать на себя свою часть последствий. Зачастую при инциденте на стороне подрядчика репутационный и финансовый ущерб несет заказчик.

«Подрядчик с низким уровнем доступа не представляет угрозы»

Любой доступ является потенциальным вектором атаки. Иногда злоумышленникам достаточно получить в свое распоряжение всего одну учетную запись, для того чтобы провести разведку и начать действовать.

В **40%** случаев логины, пароли, токены и SSH-ключи хранятся в незашифрованном виде и их с легкостью можно найти в файловых хранилищах, системах управления проектами (таких как Jira, Confluence и т. д.) или в конфигурационных файлах

Как по сценарию

Можно выделить несколько наиболее популярных сценариев атаки на цепочки поставок. Самый очевидный из них — это взлом через поставщика услуг, у которого есть доступ к инфраструктуре и бизнес-системам компании.

При таком варианте хакеры действуют по достаточно простой схеме, используя уязвимость на внешнем периметре или фишинг. Когда злоумышленник получает доступ в инфраструктуру подрядной организации, ему остается лишь найти логины и пароли, которые специалисты вводят для подключения к системам заказчика.

По наблюдению экспертов компании «Инфосистемы Джет», приблизительно в 40% случаев подобная информация *(логины, пароли, токены, SSH-ключи)* в организациях хранится в незашифрованном виде и ее с легкостью можно найти в файловых хранилищах, системах управления проектами *(таких как Jira, Confluence и т. д.)* или в конфигурационных файлах.

Бывают и ситуации, когда злоумышленникам удается обнаружить рабочие станции, с которых сотрудники подрядной организации осуществляют удаленное подключение к компаниям по уже установленным соединениям.

Второй популярный сценарий атаки реализуется во время передачи подрядчику чувствительной информации — например, для обучения ML-моделей. В таком случае похитить ее можно всего в один этап — без подключения к ИТ-инфраструктуре заказчика, что значительно упрощает задачу.

Именно поэтому важно понимать, что как только компания выводит чувствительную информацию за свой периметр, она теряет контроль за ее сохранностью и конфиденциальностью, полностью передавая его подрядчику.

Наряду с вышеперечисленным задачу злоумышленников может облегчить наличие у компании незакрытых уязвимостей или устаревших версий ПО при отсутствии актуальной политики безопасности. Все это дает возможность попасть внутрь инфраструктуры без особого труда.

Кроме того, одной из самых распространенных ошибок, которые систематически приводят к инцидентам информационной безопасности, является предоставление подрядчикам избыточных прав — просто «на всякий случай», без анализа их реальных потребностей и учета возможных рисков. К той же категории можно отнести использование бессрочных учетных записей, не привязанных к конкретным проектам, а также аутентификацию с помощью статических паролей без многофакторной защиты для критически важного доступа.

Эти риски усугубляются отсутствием содержательного мониторинга активности подрядчиков в корпоративных системах и подключением их к общей сетевой инфраструктуре без должной сегментации и изоляции, что создает условия для горизонтального перемещения злоумышленников и масштабных утечек данных.

Примеры инцидентов

Один из типичных примеров атаки через подрядчика — инцидент в одной из российских микрофинансовых организаций, расследованием которого занималась команда Центра информационной безопасности *(ЦИБ)* компании «Инфосистемы Джет». Подрядной организацией, от которой исходила угроза, оказалась компания, занимающаяся разработкой, внедрением и сопровождением специализированного программного обеспечения для финансовой отрасли. Скорее всего, подрядчик был атакован через уязвимость во внешнем периметре, после чего хакеры получили доступ к его системе Confluence.

Как только компания выводит чувствительную информацию за свой периметр, она теряет контроль за ее сохранностью и конфиденциальностью, полностью передавая его подрядчику

Как это часто бывает, данные для доступа к своим заказчикам подрядчик хранил в открытом виде, что существенно упростило реализацию атаки, которая проходила в несколько этапов.

В первую очередь злоумышленники думают о собственной безопасности. Поэтому они идут на хостинг и покупают виртуальную машину с IP-адресами из российской подсети, чтобы избежать потенциальной блокировки по геолокации.

Далее в ход идет инструкция по подключению к корпоративному VPN, которую злоумышленники заранее скачивают с конфлюенса подрядчика. Они проверяют наличие второго фактора и убеждаются в том, что его нет. Дело сделано: киберпреступники проникают в инфраструктуру заказчика.

Поскольку подрядчик занимается разработкой и поддержкой программного обеспечения, у него имеются права локального администратора сразу на нескольких серверах, где развернуты его решения. Используя их, хакеры проводят сетевую разведку с помощью сетевого сканера и видят структуру Active Directory *(какие группы и пользователи в ней присутствуют и какие сервисы используются)*.

К тому же права локального администратора позволили хакерам создать для себя сетевой тоннель передачи информации с использованием SocsOverRDP и сделать дамп процесса LSASS, в рамках которого обрабатываются аутентификационные данные пользователей сервера.

В результате этих действий в руках злоумышленников оказалась привилегированная учетная запись в домене заказчика. Далее последовала атака на контроллер домена, нацеленная на получение базы его пользователей *(NTDS.dit)*. А через множественные подключения по RDP к различным серверам был проведен поиск важной информации. В частности, на сервере баз данных хакеры нашли скрипты, в которых в открытом виде хранятся логины и пароли сервисных учетных записей.

А теперь можно разобрать ответные действия заказчика для отражения хакерской атаки.

Обнаружение нелегитимной активности произошло в момент создания дампа NTDS.dit и множественных подключений по RDP. После этого специалисты предприняли ответные действия:

- блокировка IP-адресов;
- сброс VPN-сессий;
- блокировка учетных записей;
- смена паролей в Active Directory;
- исследование скомпрометированных узлов;
- настройка двухфакторной аутентификации.

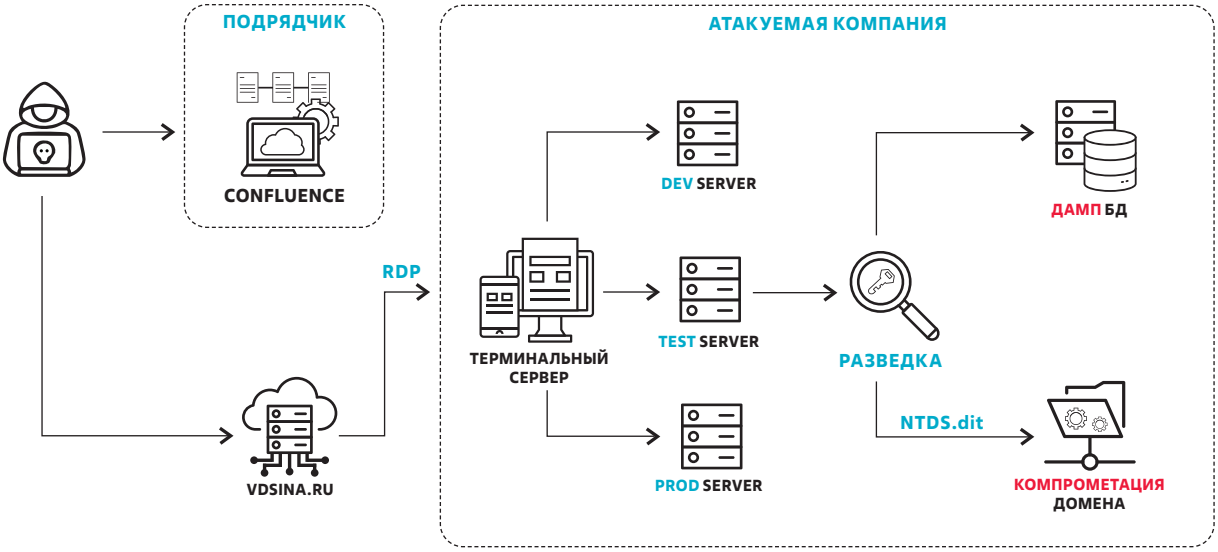
Интересно, что одновременно с описанной атакой, по информации Центра информационной безопасности компании «Инфосистемы Джет», подобные попытки взлома наблюдались как минимум у двух крупных предприятий из энергетической отрасли и одной компании из финансового сектора. При этом хакеры использовали те же самые учетные записи подрядчика. Например, в одной из атак хакерам удалось зашифровать практически всю ИТ-инфраструктуру. Злоумышленники применили шифровальщик сразу на уровне гипервизора. С учетом отсутствия у атакуемой организации сегментирования сети зашифровались не только боевые серверы, но и бэкапы. Это сделало процесс восстановления очень долгим и крайне болезненным.

От слепого доверия к взаимодействию ИБ-служб

В ситуации повышенных угроз со стороны подрядчиков перед компаниями неизбежно встает вопрос построения эффективной защиты.

В идеальной системе защиты ИБ-службы компании и ее подрядчика должны действовать слаженно, применяя современные инструменты ИБ. Однако у подрядчика может не быть собственного процесса

ОПИСАНИЕ ИНЦИДЕНТА



мониторинга и реагирования на инциденты — в этом случае заказчику остается полагаться только на собственный мониторинг ИТ-активов. Если же инструменты ИБ используются подрядчиком, то могут возникнуть другие сложности. Например, организации могут иметь разные критерии анализа событий для выявления инцидентов. В этом случае партнерам необходимо договориться, что именно считать опасным событием для ИБ.

Эффективная защита требует синергии всех основных принципов ИБ в отношении работы с подрядчиками. В первую очередь это Zero Trust — архитектурная философия нулевого доверия для реализации принципа наименьших привилегий. В частности, это означает, что партнеру должны выделяться лишь доступы, необходимые для выполнения его обязательств.

Немаловажно при этом провести грамотную сегментацию сети. Данная мера значительно усложнит развитие атаки в случае, если соблюдения двух первых принципов защиты будет недостаточно. Таким образом, в компании можно реализовать принцип многоуровневой защиты, который доказал свою эффективность на практике.

Важно подумать и об адекватном плане реагирования на инциденты ИБ, связанные с подрядчиком. Он должен включать в себя следующие действия:

- создать сценарии возможного реагирования — например, закрыть доступ всем сотрудникам подрядчика к ИТ-инфраструктуре либо частично блокировать их действия и одновременно начать поиск следов компрометации, которые должны различаться в зависимости от вида инцидента *(компрометация учетной записи, утечка информации и т. д.)*;
- составить перечень сотрудников, которых необходимо уведомить об инциденте;
- назначить ответственного за принятие решений о дальнейшем реагировании на действия хакеров;
- заранее подготовить PR-стратегию для взаимодействия со СМИ в кризисных ситуациях;
- определиться с критериями, согласно которым инцидент ИБ можно считать разрешенным.

Заказчику и подрядчику необходимо договориться, что именно считать опасным событием для ИБ

Однако для принятия необходимых мер защиты компании должны осознать все риски, связанные с взаимодействием с партнерами. На сегодняшний день мероприятия по оценке уровня безопасности подрядчиков проводятся лишь в некоторых компаниях. И реализуются они в основном с помощью такого инструмента, как опросные листы.

Анкетирование, как правило, носит формальный характер, поэтому такую практику стоит усилить другими мерами. Например, это можно сделать с помощью сервисов киберразведки *(OSINT)*, которые позволяют:

- взглянуть на подрядчика глазами потенциального злоумышленника и оценить уровень защищенности внешнего периметра организации *(выявить доступные формы авторизации, уязвимости, устаревшие сервисы и т. д.)*;
- проверить наличие в открытом доступе клиентских данных подрядчика, которые могли быть слиты в сеть, а также выявить информацию о подготовке атак на эту организацию или об оказании инсайдерских услуг ее сотрудниками.

Сервисы киберразведки собирают информацию из открытых источников, поэтому их использование не требует согласования с подрядными организациями. Это одно из неоспоримых преимуществ такого метода. А вот классический пентест на инфраструктуре подрядчика уже требует содействия потенциального партнера и получения от него авторизационного письма, в котором будут зафиксированы границы выполняемых работ на принадлежащих компании активах. Это достаточно трудозатратный, но наиболее показательный метод исследования, который позволяет провести подробный анализ уровня защищенности.

Вместе с тем стоит учитывать, что подрядная организация может легко саботировать подобные работы — например, не предоставляя своего согласия на их проведение либо заведомо скрывая информацию о состоянии своей инфраструктуры.

Кроме того, рекомендуется установить в компании правила безопасной работы с подрядчиками, в которых должны быть представлены:

- перечень защитных мер, которые принимаются компанией на каждом этапе взаимодействия с подрядчиком *(от выбора компании до завершения работ)*;
- критерии выбора подрядчика: какие задачи он должен решать и каким требованиям отвечать *(полный перечень)*;
- порядок учета подрядчиков и предоставленного им доступа к инфраструктуре компании *(к каким ИТ-активам возможно подключение, насколько они критичные, какой тип доступа используется и т. д.)*;
- требования по обеспечению ИБ, которые необходимо соблюдать подрядчику при совместной работе;
- порядок управления доступом третьих лиц к корпоративным ресурсам.

Необходимо обязать подрядчика сообщать о возникновении на его стороне инцидента ИБ, который может повлиять на компанию. Для этого требуется:

- определить критерии оценки инцидента;
- составить список контактных лиц;
- выделить каналы для оперативной связи;
- утвердить сроки информирования об обнаружении инцидента, его локализации и расследования.

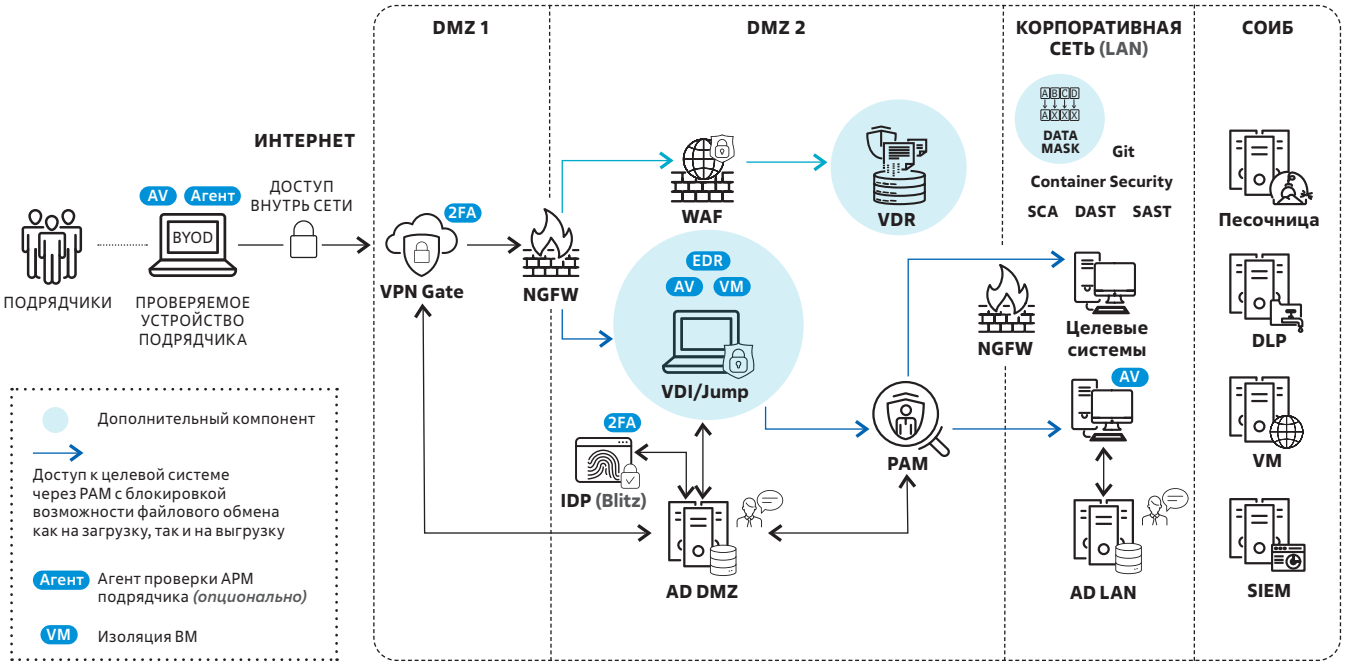
Следует зафиксировать план реагирования на инцидент ИБ подрядчика со своей стороны *(как минимум сценарии компрометации его учетной записи и утечки переданных ему конфиденциальных данных)*.

Решения для контроля

Отдельно остановимся на решениях классов PAM, EDR и SIEM, которые наиболее эффективны при контроле работы подрядчиков. Они позволяют обеспечить безопасную буферную зону и защитить сегмент инфраструктуры, предназначенный для совместного взаимодействия. Типовое архитектурное решение может включать в себя следующие классы и подходы:

- Решение класса NAC или ZTNA — для контроля устройств подрядчиков, с которых они подключаются к сети. В частности, специализированный агент не даст подключиться, если на устройстве не реализованы требования ИБ — например, нет антивируса.
- VPN и 2FA — для обеспечения безопасного удаленного доступа к ИТ-инфраструктуре.
- NGFW — для сегментации сети, контроля трафика и ограничения подрядчиков в рамках выделенных подсетей.
- Решения класса PIM/PAM — ядро архитектуры, которое обеспечивает регулярный

ШЛЮЗ БЕЗОПАСНОГО ДОСТУПА



- мониторинг и контроль привилегированных учетных записей подрядчика.
- VDI — для создания изолированной среды работы каждого подключаемого пользователя с гранулированным доступом к необходимым целевым системам.
- VDR — для повышения уровня защищенности при обмене файлами между подрядчиком и внутренней инфраструктурой заказчика.

Участвуют все

Понять, насколько далеко может зайти хакер при взломе подрядчика, можно с помощью проведения киберучений по сценарию, имитирующему конкретный вид атаки. В случае, если в компании приняты перечисленные выше меры безопасности, такой тест станет отличной проверкой их эффективности. Наряду с этим результаты учений позволят понять, в каких аспектах требуется усилить рубежи защиты, и могут стать значимым аргументом в переговорах с подрядчиками, в безопасности инфраструктуры которых нет полной уверенности.

Если в качестве формата учений был выбран пентест / Red Team / Purple Team, в них будут участвовать команды реагирования *(при их наличии)*, а также представители ИБ/ИТ-подразделений. Если же учения проходят по модели настольного тестирования *(tabletop)*, то в зависимости от их сценария, помимо задействования этих департаментов, рекомендуется участие представителей бизнеса, юридического отдела и отдела маркетинга, то есть фактически всей вертикали сотрудников, обеспечивающей непрерывность бизнеса.

Проведение корректного мониторинга действий внешних специалистов подрядчика требует комплексного подхода, сочетающего различные меры. Техническая реализация должна включать обязательное использование персонифицированных учетных записей с многофакторной аутентификацией, контроль и логирование всех подключений через VPN-шлюзы, доступ к критичным системам через выделенные jump-серверы или специализированные решения для контроля привилегированного доступа *(PAM)* с обязательной записью сессий.

С организационной точки зрения необходимо разработать сценарии мониторинга нелегитимных действий и аномального поведения подрядчиков *(подключение в нерабочее время, попытки обращения к нехарактерным ресурсам, аномальные объемы передаваемых данных и пр.)*.

Все эти меры позволят четко отслеживать аномальную активность подрядчиков и пресекать опасные инциденты до того, как они приведут к ощутимым последствиям для бизнеса.

СОСТОЯНИЕ ГОТОВНОСТИ

ЧТО ДАЮТ КИБЕРУЧЕНИЯ И КАК ЭТО ИСПОЛЬЗОВАТЬ

- Часто бизнес «падает» не из-за накладок в работе техники, а вследствие организационных провалов: задержек в передаче информации, нечетко прописанных ролей и непродуманных решений
- ИБ-специалистам остро не хватает навыков реагирования на инциденты, а также квалификации в этичном хакинге и форензике
- Регулярные киберучения позволяют держать команду в состоянии готовности к возникновению инцидентов

ЭКСПЕРТ

Дмитрий Казмирчук

руководитель группы сервиса киберучений компании «Инфосистемы Джет»

ЭКСПЕРТ

Кира Шиянова,

менеджер продукта Jet CyberCamp

По данным компании «Инфосистемы Джет», спрос российских организаций на проведение киберучений вырос в 2024 году на 25%. Этот тренд остается актуальным, поскольку результативные хакерские атаки наносят колоссальный финансовый и репутационный ущерб, размер которого несопоставим с затратами на проверку устойчивости компаний к инцидентам и укрепление ИБ. О том, в каких случаях необходимо проводить киберучения, как выбрать для них подходящий формат и каких результатов можно ожидать от проверки, — в нашем материале.

Право на ошибку

Оценить уровень ИБ с самых разных точек зрения — как со стороны защиты, так и со стороны нападения — позволяют киберучения, в рамках которых инфраструктура компании рассматривается как потенциальная цель для взлома. В таком формате специалисты могут получить дополнительные знания и освоить новые инструменты защиты компании, а также попрактиковаться в расследовании инцидентов.

Кира Шиянова

«Киберучения можно назвать своеобразной репетицией, проверкой действий сотрудника или всей команды при возникновении инцидента. Они проводятся в условиях, максимально приближенных к реальным. Это дает возможность детально сымитировать работу коллектива во время кибератаки, оставляя сотрудникам право на ошибку, поскольку она не приведет к ущербу».

По итогам киберучений обычно выявляются зоны для усиления защиты, в которых наблюдаются следующие проблемы: несогласованность действий, пробелы в знаниях и опыте, неясные роли и узкие места в ресурсах.

Кира Шиянова

«В понятие киберучений мы включаем не только сами тренировки, нацеленные на проверку знаний. Важный акцент делается на обучении, основанном на многогранном опыте и компетенциях, которые есть у специалистов Jet CSIRT в области консалтинга, аудита и безопасной разработки. Мы упаковываем наши умения в теоретический материал, а затем доносим в различных форматах до заказчиков и комьюнити».

Все это выгодно отличает киберучения от классических тестов безопасности, покрывающих лишь малую часть функционала и в основном нацеленных на проверку дыр в существующей защите и бизнес-процессах.

Киберучения — это своеобразная репетиция, проверка действий сотрудника или всей команды при возникновении инцидента. Они проводятся в условиях, максимально приближенных к реальным

Действия важнее техники?

ИБ не ограничивается поддержанием устойчивости технических средств, которая в любой момент может быть нарушена после грамотно выстроенной атаки. Не менее важны действия сотрудников во время инцидента, которые напрямую зависят от их знаний и подготовки. А навыки устойчивого реагирования на атаки в ходе киберучений формируют опыт быстрого решения проблем в реальности.

Во время киберучений можно оценить уровень подготовки каждого участника и общую эффективность работы команды. Результаты покажут, что у сотрудников получается хорошо, а где требуется усиление или есть несогласованность в действиях. Таким образом, компания получает возможность оценить своих сотрудников не по формальным признакам *(образование или наличие каких-либо сертификатов)*, а исходя из их действий в условиях реального инцидента, что намного показательнее.

Например, в результате проверки боем в ходе киберучений, проводимых в формате Purple Team, эффективность работы команды реагирования будет видна сразу же. При этом будут протестированы процессы SOC, действия Red Team, а также проверены настройки и эффективность работы средств защиты.

Если же киберучения проводятся в формате Tabletop *(когда выполняется гипотетическое моделирование нештатных ситуаций для отработки процесса реагирования на них)*, то можно оценить слаженность работы участников команды, их понимание зон ответственности и корректность мер по реагированию на инциденты.

В особом формате

Форматы киберучений могут значительно отличаться друг от друга в зависимости от решаемых задач и групп сотрудников, которые в них участвуют. Так, во время прохождения классических сценариев

Во время киберучений компания получает возможность оценить своих сотрудников не по формальным признакам (образование, наличие сертификатов), а исходя из их действий в условиях реального инцидента, что намного показательнее

киберучений либо при реализации противостояния Red Team vs Blue Team подсвечиваются технические навыки членов команды и зрелость процессов SOC. В отличие от Tabletop-учений здесь нужно не только распределить роли и составить план действий, но и суметь его реализовать — то есть решить задачи непосредственно в инфраструктуре компании и добиться результата.

Формат мероприятия всегда нужно выбирать с учетом целевой аудитории, степени ее вовлеченности в процесс и частоты возникновения инцидентов. Как правило, вопрос о том, кого необходимо обучить, организаторы киберучений задают одним из первых. Кроме того, для выбора оптимального формата киберучений необходимо осуществить следующие этапы подготовки:

- первичная оценка модели угроз и определение наиболее актуальных рисков ИБ;
- анализ состава инцидентов, выявление повторяющихся и уникальных событий;
- поиск причин возникновения инцидентов и определение их характера *(организационный или прикладной)*.

На основании этой информации можно сделать заключение о предпочтительном типе киберучений и необходимости привлечения сторонних специалистов для их проведения.

Заполнение пробелов в компетенциях, выявленных в ходе киберучений, позволяет точнее строить гипотезы, эффективнее отслеживать атаки и раньше замечать опасные артефакты, оставленные в системах

Форматы киберучений также определяются в зависимости от масштаба задач, которые необходимо выполнить:

- **Стратегические учения** — наиболее глобальный уровень и долгосрочная программа. В качестве целевой аудитории здесь выступают руководители, которым необходимо изучить ИБ-решения, влияющие на безопасность компании и ее репутацию на рынке.
- **Тактические учения** затрагивают координацию отдельных команд и подразделений, для развития которой чаще всего используется командно-штабной формат.
- **Операционный уровень** — это различные варианты классических решений, по результатам которых происходит отработка конкретных действий сотрудников.

Для каждого образовательного формата закладывается собственная методика оценки навыков и компетенций сотрудников. В частности, для анализа результативности киберучений используются такие показатели, как время прохождения, количество ошибок и их повторений, самостоятельное получение результатов или задействование подсказок в ходе прохождения задания.

Кроме того, во время проработки сценариев к процессу подключаются менторы, которые сопровождают участников в ходе киберучений, выполняют разбор их решений, обращая внимание на подход, логику действий, наличие хаоса в коммуникации и т. д. По этим данным можно сделать выводы о традициях и подходах, которые сложились в компании. Зачастую здесь требуются исследовательские и консалтинговые услуги, которые могут включать аудит процессов, документации и т. д.

Кира Шиянова

«Исходя из нашей практики, могу сказать, что наиболее эффективно проходят учения, перед стартом которых были проведены исследовательские работы и выполнена адаптация программы с учетом особенностей текущих процессов заказчика. Как правило, такую схему действий выбирают более зрелые компании, поскольку для ее реализации необходима большая вовлеченность в процесс подготовки и прохождения учений».

В ходе киберучений команды отрабатывают навыки реагирования с распределением ролей: каждый специалист знает, что ему делать в конкретной ситуации и какие инструменты при этом использовать. Границы неизвестного сужаются, и появляется четкое видение происходящих процессов. В результате время реагирования на инцидент сокращается в разы, что минимизирует шансы злоумышленников на проведение атаки и уменьшает возможный урон от их действий.

Если команда уже получила необходимый опыт в решении отдельных кейсов и разборе инцидентов на первичных киберучениях, то можно переходить к следующему формату — purple team. В рамках этого формата команды атакующих и защищающихся действуют сообща, вырабатывая и корректируя защитные меры в реальном времени. Это требует достаточно высокой квалификации обеих сторон и высокого уровня зрелости компании с точки зрения ИБ.

Узкие места

Проведение киберучений позволяет выявить множество проблем в области ИБ, устранение которых способно заметно повысить уровень защищенности организаций.

ОСНОВНЫЕ ФОРМАТЫ КИБЕРУЧЕНИЙ В ЗАВИСИМОСТИ ОТ ЦЕЛЕВОЙ АУДИТОРИИ

КЛАССИЧЕСКИЕ КИБЕРУЧЕНИЯ ПРЕДПОЛАГАЮТ ТЕОРИЮ, ПРАКТИКУ И РАЗНООБРАЗНЫЕ МЕТОДИКИ ОБУЧЕНИЯ

Работа ведется непосредственно с инфраструктурой и средствами защиты информации. Практика для этого формата включает в себя сценарии для следующих направлений:

- **Red Team** (наступление);
- **Blue Team** (расследование инцидентов и реагирование на них);
- **Yellow Team** (защита и инфраструктурные задачи);
- **Purple Team** (совместная работа «синих» и «красных»).

МЕРОПРИЯТИЯ НАЦЕЛЕНЫ НА ПОВЫШЕНИЕ ОБЩЕЙ ГРАМОТНОСТИ В ВОПРОСАХ ИБ И СОБЛЮДЕНИЕ ПРАВИЛ ЦИФРОВОЙ ГИГИЕНЫ ВНУТРИ КОМПАНИИ

Для этого подходит процесс security awareness (повышение осведомленности), включающий периодическое обучение, информирование сотрудников об угрозах и проверку усвоения полученного материала. Последняя реализуется с помощью различных тестовых атак, реакция персонала на которые внимательно отслеживается (например, это может быть открытие фишинговых писем с последующим переходом на мошеннические сайты).

ФОРМАТ УЧЕНИЙ ПРЕДПОЛАГАЕТ РЕШЕНИЕ НЕСТАНДАРТНЫХ ЗАДАЧ В ЗАВИСИМОСТИ ОТ КОНКРЕТНЫХ ПРОБЛЕМ, С КОТОРЫМИ СТАЛКИВАЕТСЯ КОМПАНИЯ

Например, это может быть улучшение качества взаимодействия между службами — для этой цели подойдет проведение командно-штабных учений, подразумевающих пошаговое выполнение заранее подготовленных сценариев.

Наилучших результатов здесь позволяет добиться работа в очном формате по плану, разработанному с учетом внутренних регламентов компании.

ДЛЯ РУКОВОДИТЕЛЕЙ ЛУЧШЕ ВСЕГО ПОДХОДЯТ TABLETOP-УЧЕНИЯ, КОТОРЫЕ ПО МЕХАНИКЕ ПРОВЕДЕНИЯ ПОХОЖИ НА КОМАНДНО–ШТАБНЫЕ, — ЭТО СЦЕНАРНОЕ (ГИПОТЕТИЧЕСКОЕ) МОДЕЛИРОВАНИЕ ИНЦИДЕНТА

Они нацелены на получение опыта реагирования и принятия решений в процессе реального инцидента, но уже на уровне топ-менеджмента, ИТ, ИБ, PR и HR. Важно, что тесного взаимодействия этих подразделений внутри большинства компаний нет. Поэтому их совместные учения могут дать выраженный эффект.

Кроме того, киберучения такого типа позволяют преодолеть так называемый паралич руководства, который часто возникает из-за отсутствия плана, слаженности и опыта взаимодействия. Он сопровождается страхом ответственности и принятия публичных решений или может вести к возникновению противоречивых сообщений вовне или внутри компании.

Наконец, работа с топ-менеджерами важна, поскольку именно они принимают ключевые решения в вопросах финансов и репутации компании. Таким образом, их обучение и осведомленность имеют особый приоритет.

Регулярное проведение киберучений особенно важно для компаний, где возникновение простоев в работе — критичное событие. Например, это характерно для организаций из финансовой сферы, промышленности, энергетики и т. д.

Дмитрий Казмирчук

«В частности, у современных специалистов по безопасности часто выявляется просадка в навыках этичного хакинга. Они прекрасно умеют работать с журналами событий, SIEM и NTA, но испытывают сложности с самостоятельной реализацией атак и слабо ориентируются в возможностях инструментов атакующих. Заполнение этого пробела в компетенциях позволяет точнее строить гипотезы, эффективнее отслеживать атаки и раньше замечать опасные артефакты, оставленные в системах».

По словам эксперта, аналогичная ситуация и с навыками форензики ***(компьютерной криминалистики)***, с задачами которой в своей работе сталкивается далеко не каждый безопасник. Такие навыки крайне важны для проведения низкоуровневых расследований.

Еще одно из узких мест зачастую становится заметным во время Tabletop-учений, когда в определенный момент выясняется, что нет ответственного за конкретное действие по реагированию на инцидент. Например, в компании может отсутствовать владелец того или иного процесса, использоваться неактуальная база контактов, возникать конфликты интересов ***(например, между ИБ и ИТ)***, а юристы и PR могут подключаться к реагированию слишком поздно и т. д.

Своими силами?

Как правило, если компания проводит киберучения самостоятельно и регулярно, использует актуальные данные и методики, положительный результат не заставит себя долго ждать, а привлечение внешних исполнителей либо не потребуется, либо ограничится минимальными объемами.

Если же проблемы остаются, а тем более возникают новые ***(что-то ломается на прикладном уровне, либо увеличивается количество инцидентов и время на их реагирование продолжает расти)***, то это показатель того, что имеет смысл позвать стороннюю команду и воспользоваться ее экспертизой.

Однако такой шаг сопряжен с определенными рисками. Например, при привлечении внешних специалистов может произойти несовпадение ожиданий от их работы с реальностью. Так, заказчик рискует столкнуться с невнимательной проработкой требований, однообразием используемых сценариев или навязчивым продвижением определенных защитных решений.

Дмитрий Казмирчук

«Сервис Jet CyberCamp для киберучений позволяет экспертам донести свой богатый опыт до заказчиков. Кроме того, в его основе лежит мультивендорный подход, что дает возможность выбирать решения, которые будут использоваться в обучении, — чтобы компании могли либо работать с привычными инструментами, либо присмотреться к новым для себя решениям и протестировать аналоги».

Регулярные киберучения: когда начинать их проводить

Регулярное проведение киберучений особенно важно для компаний, где возникновение простоев в работе — критичное событие. Например, это характерно для организаций из финансовой сферы, промышленности, энергетики и т. д. В качестве дополнительной меры стоит провести анализ инцидентов ИБ, произошедших в других компаниях, определив частоту направленных против них атак и объяснив, почему это происходит. Разумеется, основанием для принятия мер являются

и инциденты, с которыми компания уже столкнулась *(чтобы не повторялись ошибки, ставшие причиной события)*.

Дмитрий Казмирчук

«Учиться необходимо не только на своих ошибках, но и на чужом опыте, который часто оказывается куда более показательным и зачастую более объемным, что представляет большой интерес для изучения. Это одна из причин того, почему специалисты компании “Инфосистемы Джет” часто подключаются к расследованию громких инцидентов. Это позволяет пополнять корпоративную библиотеку новыми сценариями атак и вариантами реагирования на инциденты».

Регулярные киберучения позволяют держать команду в состоянии готовности к возникновению инцидентов, что в конечном счете отражается на показателях рабочих процессов. Для их контроля используется методология оценки сотрудников по освоенным навыкам и параметрам прохождения различных сценариев. Среди них: время обнаружения и реагирования на инциденты, количество эскалаций, качество принятых решений, наличие повторных ошибок и т. д.

Причем тут важны как результаты, показанные в ходе обучения, так и показатели, полученные в рамках реального процесса. Интересно, что такие критерии, как количество отраженных атак и их отношение к общему числу инцидентов, эксперты считают бесполезными, поскольку они не находятся в прямой зависимости от работы участников процесса.

Тот самый триггер

Киберучения значительно влияют на взаимодействие ИТ-, ИБ- и бизнес-команд в стрессовой ситуации. В ходе совместного решения задач их представители находят общий язык и формируют единое понимание приоритетов, которое пригодится при наступлении реального инцидента.

Дмитрий Казмирчук

«Часто бывает так, что киберучения оказываются тем самым триггером, который позволяет специалистам из различных команд познакомиться друг с другом и разобраться в зонах ответственности. А в случае реального инцидента процесс реагирования на него уже проходит по накатанной и все специалисты справляются с ситуацией намного легче».

Кроме того, успешное прохождение киберучений является одним из способов подсветить зрелость компании в области обеспечения собственной и клиентской безопасности.

Это особенно актуально в ситуации роста числа кибератак, которые проводятся через ИТ-инфраструктуру поставщиков *(виду инцидентов мы посвятили отдельный материал в этом номере)*. Здесь правило «вся цепь крепка настолько, насколько крепким является ее самое слабое звено» полностью соответствует ситуации с ИБ. И именно инфраструктура подрядчика часто оказывается этим слабым звеном: как правило, она находится вне зоны контроля, что дает киберпреступнику возможность получить легкий доступ к основной инфраструктуре. К тому же при реализации таких инцидентов не всегда будет виден изначальный вектор атаки, что осложнит восстановление всей цепочки событий во время расследования.

Проведение учений, вне зависимости от их формата, учит бизнес реагировать на внешнее вмешательство, угрожающее его работе, согласно следующим принципам: не паниковать, действовать по плану и уметь этот план вовремя и без потерь адаптировать к реальным условиям.

Успешное прохождение киберучений является одним из способов подсветить зрелость компании в области обеспечения собственной и клиентской безопасности, что является дополнительным аргументом для начала сотрудничества

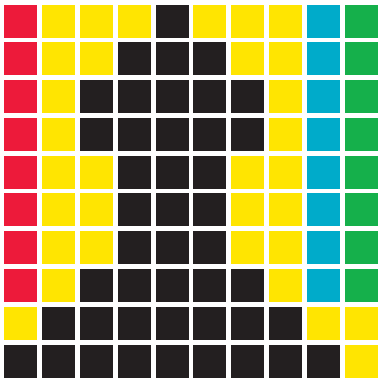
TABLETOP-УЧЕНИЯ

КАК ТРЕНИРУЮТ УПРАВЛЕНИЕ КИБЕРКРИЗИСАМИ, КОГДА АТАКА — ВОПРОС ВРЕМЕНИ

ЭКСПЕРТ
Аскар Мусаев,
эксперт по непрерывности бизнеса компании «Инфосистемы Джет»

Можем ли мы исключить технические сбои автомобиля в дальней дороге? Нет. Но мы точно знаем, что без профилактического осмотра вероятность поломки гораздо выше. Системы диагностируют реальные и потенциальные неполадки, прогнозируют поломки, предотвращают сбои в работе автомобиля и заменяют расходники, тем самым обеспечивая бесперебойное движение. Такая же логика применима и к предотвращению киберинцидентов.

ТОП КИБЕРУГРОЗ 2025 ГОДА ПО РЕЗУЛЬТАТАМ РАССЛЕДОВАНИЙ КОМАНДЫ JET CSIRT



44%
Шифрование инфраструктуры: LockBit, Babyk, Zeppelin, Phobos, Enmity

32%
Разрушение инфраструктуры *(wiper)*

8%
Утечка конфиденциальных данных

8%
DDoS-атаки (с остановкой бизнес-процессов)

8%
Хактивизм: продажа доступов, дефейс, нелегитимные финансовые операции, майнеры

В 2025 году команда Jet CSIRT расследовала серию резонансных киберинцидентов в ретейле, ИТ, на транспорте и в грузоперевозках, в здравоохранении и страховании. Атак становится больше, и при их успешной реализации в 70% случаев речь идет о наиболее разрушительных сценариях — применении вирусов-шифровальщиков *(44%)* и вайперов *(32%)*, способных полностью уничтожить инфраструктуру и остановить бизнес-процессы. Под ударом оказываются компании, критически зависящие от доступности цифровых систем и непрерывности операций, — а значит, к таким кризисным сценариям необходимо готовиться заранее.

Жизнь в условиях постоянных кибератак уже не эксцесс, а новая норма. Преимущество получают компании, которые умеют быстро адаптироваться к инцидентам и восстанавливаться после них. Одним из инструментов такой адаптации становятся Tabletop-учения *(TTX)*. Но как часто команды ИБ, ИТ и топ-менеджеры действительно собираются вместе, чтобы в одной комнате принимать решения в условиях кризиса? Tabletop-учения моделируют именно такую ситуацию в безопасной среде, где цена ошибки равна нулю, а ценность полученного опыта бесконечна.

Tabletop-учения — известный формат управленческого моделирования. Его основная цель — не техническая проверка систем, а именно проработка процессов, ролей, взаимодействий и принятия решений в условиях кризиса без воздействия на реальные ИТ-сервисы или инфраструктуру. В отличие от тестирований планов аварийного восстановления *(DRP)*, когда инженеры отрабатывают технические навыки восстановления систем, Tabletop сфокусированы на возможных кризисных сценариях и обсуждении действий, а не на активном использовании инструментов. Это дискуссионная модель реакции и принятия решения.

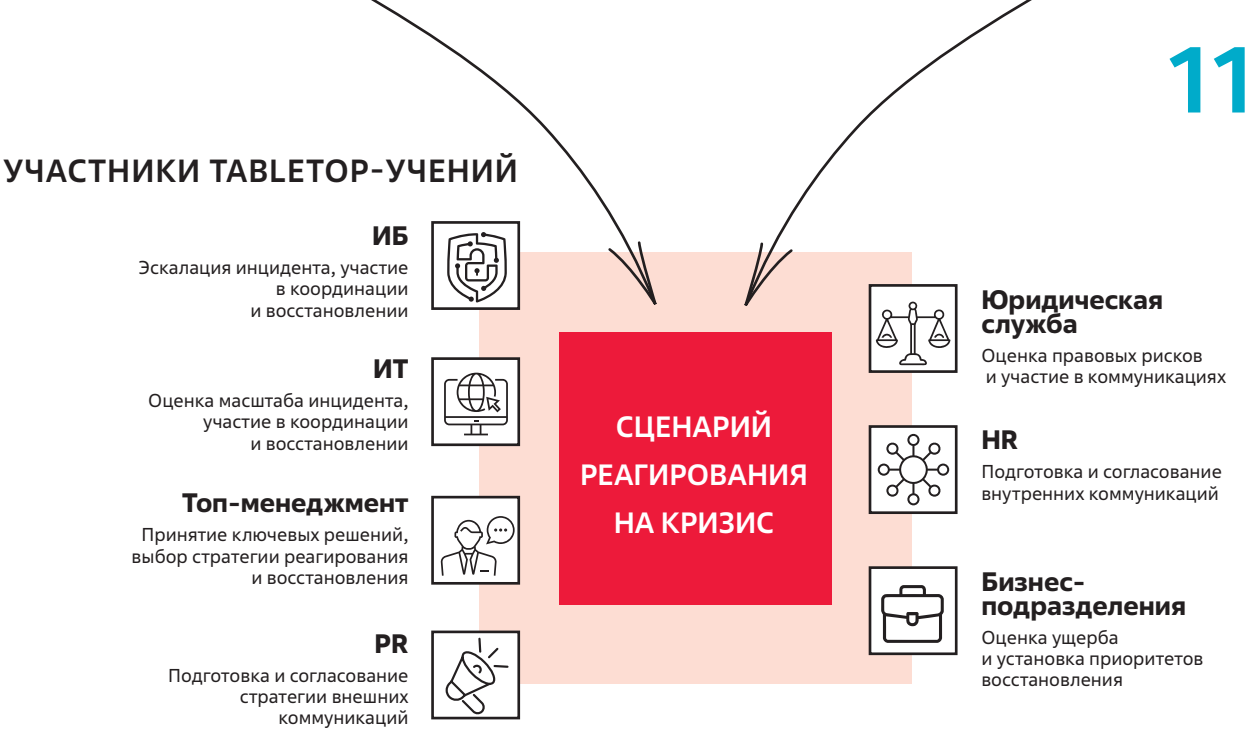
От военных карт к цифровым кризисам

Идея настольных учений возникла не в ИТ, а в военной сфере. Военные давно применяли варгейминг для оценки стратегий, тактик и вероятных действий противника: такие сессии позволяли отрабатывать сложные сценарии без реальных боевых действий и тем самым снижать риски.

Сначала подход был адаптирован для проверки устойчивости компаний в условиях моделирования природных и техногенных катастроф, а с ростом цифровых угроз и зависимости бизнеса от информационных систем эту практику приспособили и для усиления киберустойчивости. Сегодня настольные тестирования уже закреплены на уровне международных стандартов и методических рекомендаций — это не «экспериментальный формат», а устоявшаяся практика. Так, European Union Agency for Cybersecurity *(ENISA)* разработало подробную методологию подготовки и проведения киберучений, включая Tabletop-формат, — от постановки целей и выбора сценариев до оценки результатов и последующего улучшения процессов.

В США Cybersecurity and Infrastructure Security Agency *(CISA)* публикует готовые сценарные наборы для отработки различных типов киберинцидентов — от атак с использованием программ-вымогателей до компрометации цепочки поставок. Эти материалы используются как основа для практических тренировок в организациях разного масштаба.

Одна из ключевых ценностей Tabletop-учений — возможность заранее проработать управленческие решения и подготовить к ним топ-менеджмент. В кризисной ситуации руководству так или иначе придется погружаться в детали — особенно если речь идет, например, об инциденте с вирусом-



шифровальщиком. Когда кризис станет реальным, решения придется принимать быстро и под сильным давлением, а времени разобраться и взвесить риски может не оказаться.

Аскар Мусаев

«Такой формат учений позволяет в спокойной обстановке пройти всю цепочку реагирования — от первичного информирования до решений о восстановлении и внешних коммуникациях. Участники могут остановиться на спорных моментах, обсудить варианты, выработать взвешенные решения прямо во время учений или оформить их как домашнее задание по итогам сценария. Все нюансы и "мелочи", которые неизбежно всплывают в ходе реального инцидента, здесь прорабатываются заранее — без стресса и с максимальной пользой для компании».

Зачем бизнесу Tabletop-учения

1. УСИЛЕНИЕ КОМАНДНОГО ВЗАИМОДЕЙСТВИЯ

Основные участники Tabletop-учений — команды ИБ и ИТ. На практике нередко складывается ощущение, что в рамках таких сценариев они видят друг друга впервые. Сразу появляется множество идей, гипотез и версий реагирования на инцидент. В повседневной работе эти команды чаще пересекаются во время регламентных процессов и редко — в условиях масштабных кризисов.

Аскар Мусаев

«Проживание инцидента в формате тренировки позволяет участникам синхронизироваться, лучше понять логику и приоритеты друг друга и, как результат, значительно усилить командное взаимодействие. Это нередко приводит

ЧТО-ТО ТОЧНО ПРОИЗОЙДЕТ, И ВЫ ДОЛЖНЫ БЫТЬ К ЭТОМУ ГОТОВЫ

к появлению новых, более взвешенных решений, которые сложно было бы выработать в одиночку».

Один из показательных кейсов реального Tabletop-учения был связан с паролями администраторов. Если при шифровании инфраструктуры вместе с основными системами будет выведен из строя и менеджер паролей, как сотрудники, отвечающие за восстановление, получат доступ к критически важным ресурсам? В ходе учения команды ИТ и ИБ оценили масштаб риска и проработали возможные сценарии. В результате было предложено, а затем внедрено безопасное решение на случай кризиса — так называемый ноутбук судного дня, предназначенный для восстановления доступа в условиях полной компрометации инфраструктуры.

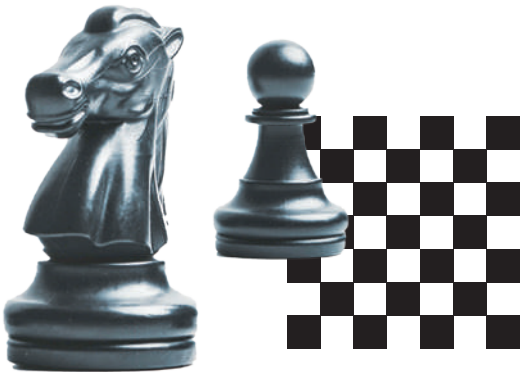
2. ВЫЯВЛЕНИЕ «СЕРЫХ ЗОН»

«Серые зоны» во время Tabletop-учений обнаруживаются неизбежно. Таким аспектам раньше не уделяли должного внимания, но их можно и нужно «подсвечивать». Например, ИТ-команда может считать себя полностью готовой к инциденту, ссылаясь на наличие резервных копий и возможность быстрого восстановления.

Аскар Мусаев

«Сразу возникает логичный вопрос: кто и когда проверял защищенность контура, в котором хранятся эти резервные копии? Если такой проверки не было, она становится очевидным следующим шагом — например, в формате дополнительного тестирования или пентеста с прикладным фокусом. Еще один типичный конфликт приоритетов возникает на этапе восстановления. Для ИТ-специалистов зачастую важно как можно быстрее перезапустить сервер и вернуть сервисы в рабочее состояние. А с точки зрения ИБ, напротив, следует отключить систему, изолировать ее, зафиксировать следы компрометации, понять характер атаки и лишь после этого принимать решения о дальнейших действиях. Tabletop-учения позволяют заранее выявить такие расхождения и выработать общий, согласованный подход».

В одном из кейсов во время тестирования топ-менеджмент сразу обозначил позицию: расследование инцидента должно быть доведено до конца, даже если это приведет к более длительному простою.



Такое решение, принятое в рамках учения, позволило заранее определить баланс между скоростью восстановления и глубиной анализа. В случае реального инцидента команды уже будут понимать приоритеты и действовать без дополнительных согласований.

3. УРОВНИ РЕАГИРОВАНИЯ

В формате Tabletop-учений теоретически можно проверить любой сценарий и план — вплоть до пожарной эвакуации. Сам по себе формат всегда остается одинаковым: участники собираются за столом и в дискуссии последовательно «проживают» развитие кризисного сценария.

Аскар Мусаев

«Ключевое различие заключается не в формате, а в уровне реагирования, который вы хотите протестировать. Именно этот уровень может и должен быть разным. В контексте Tabletop наиболее рационально фокусироваться на реакции топ-менеджмента. Маловероятно, что в реальной жизни у компании будут возможности или ресурсы “прожить” крупномасштабный инцидент, который полностью парализует бизнес, просто ради тренировки по принятию управленческих решений. Поэтому целесообразно заранее разделять сценарии по уровням реагирования, которые планируется тестировать. При этом проверка низкоуровневых процедур, таких как планы аварийного восстановления (disaster recovery plan), не всегда подходит для формата Tabletop. Эти документы, как правило, представляют собой четкие инструкции: что и в какой последовательности нужно делать. Гораздо эффективнее проверять их с помощью практических имитаций и технических текстов. При этом сам сценарий инцидента может быть практически любым — важно лишь, чтобы он соответствовал тому уровню реагирования, который вы хотите отработать».

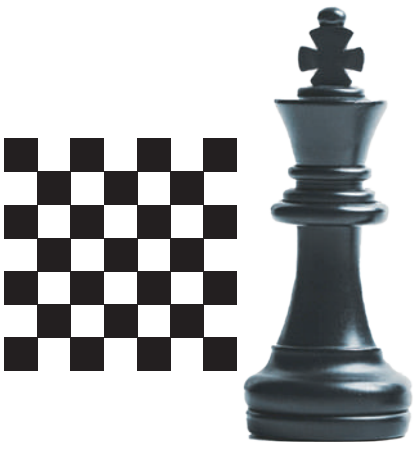
Как проходят Tabletop-учения

АНАЛИЗ КОНТЕКСТА КОМПАНИИ
Зачем: понять, в какой реальности работает компания. Изучаются базовая ИТ-среда, ключевые бизнес-процессы, роль подрядчиков, отраслевые риски и регуляторные требования.

РАЗРАБОТКА ДЕТАЛЬНОГО СЦЕНАРИЯ
Зачем: смоделировать развитие кризиса шаг за шагом. Сценарий описывает эскалацию инцидента — от первых сигналов до критической фазы. Акцент делается на управленческих, коммуникационных и стратегических решениях.

ПРОВЕДЕНИЕ TABLETOP-УЧЕНИЙ
Зачем: прожить кризис в безопасной среде. Участники за одним столом поэтапно проходят сценарий и принимают решения в условиях неопределенности. Учения длятся более трех часов и строятся в формате дискуссии.

ИТОГИ И РЕКОМЕНДАЦИИ
Необходимо превратить учения в практический результат. По итогам готовится отчет с выявленными пробелами и рекомендациями. При необходимости формируется или дорабатывается план кризисного реагирования.



ФОРМИРОВАНИЕ ЛЕГЕНДЫ ИНЦИДЕНТА
Зачем: заложить правдоподобный кризисный сценарий. На основе контекста разрабатывается легенда атаки — например, через подрядчика или фишинг. Сценарий проверяется на реализуемость и согласуется с компанией.

ПОДГОТОВКА УЧАСТНИКОВ
Формируется межфункциональная команда: топ-менеджмент, ИБ, ИТ, PR, HR и бизнес. Определяются роли и зоны ответственности в кризисе.

ПРОРАБОТКА КОММУНИКАЦИЙ
Зачем: заранее договориться, с кем, как и когда говорить. Обсуждаются внутренние и внешние коммуникации, работа с паникой, слухами и запросами СМИ. Компания сама выбирает баланс между прозрачностью и осторожностью.

ТИПИЧНЫЕ ОШИБКИ И ЗАБЛУЖДЕНИЯ
Одна из самых распространенных ошибок при проведении Tabletop-учений — поверхностная проработка кризисного сценария. Он должен быть не абстрактным описанием, а детальным, пошаговым разбором развития событий — от первых сигналов и косвенных признаков до эскалации и управленческих решений. Без такой глубины учения теряют практическую ценность и превращаются в теоретическое обсуждение.

Кейс

В ходе одного из проектов у оператора связи модератор задал, казалось бы, простой вопрос: как вы планируете собрать команду реагирования при масштабной недоступности инфраструктуры, если все ключевые сотрудники пользуются связью собственной компании? В зале повисла тишина: готового ответа не оказалось. По итогам обсуждения топ-менеджмент оперативно принял решение выдать ключевым сотрудникам резервные SIM-карты альтернативного оператора.

И это показательный момент: если бы подобный сценарий развернулся не в формате Tabletop-учения, а в реальности, времени на поиск решения могло бы просто не быть.

Аскар Мусаев

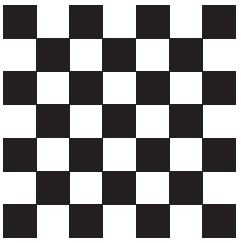
«Вторая типичная ошибка — опора исключительно на внутреннюю экспертизу компании. Если в организации нет специалистов уровня SOC или DFIR (киберкриминалистов), которые регулярно работают с реальными инцидентами, сценарий часто получается оторванным от реальности. Всё может выглядеть логично на бумаге, но не отражать того, как атаки развиваются на самом деле».

Именно поэтому в качественные Tabletop-учения обязательно вовлекаются внешние эксперты с практическим опытом реагирования. Их задача — сделать сценарий максимально приближенным к реальности, а не «придуманным из воздуха», а также учесть специфические трудности, с которыми уже пришлось столкнуться в ходе настоящих атак. Помимо перечисленных ошибок, распространенным заблуждением является ожидание быстрой отдачи в виде идеального плана реагирования. Нужно понимать, что практическая ценность учений — не в готовых ответах, а в выявлении слабых мест и проблемных зон, а также расхождений в понимании ролей.

ПРАКТИЧЕСКАЯ ЦЕННОСТЬ УЧЕНИЙ — НЕ В ГОТОВЫХ ОТВЕТАХ, А В ВЫЯВЛЕНИИ СЛАБЫХ МЕСТ И ПРОБЛЕМНЫХ ЗОН, А ТАКЖЕ РАСХОЖДЕНИЙ В ПОНИМАНИИ РОЛЕЙ

Tabletop-учения как элемент зрелой киберкультуры

Tabletop-учения перестают быть разовой инициативой или формальным требованием безопасности и становятся полноценным элементом корпоративной культуры. Эта практика формирует здоровые киберпривычки — заранее думать о рисках, продумывать сценарии развития инцидентов и оценивать последствия решений. Главная задача — не предотвращать все возможные кризисы, а минимизировать потери компании: финансовые, репутационные и операционные. Чем лучше команда понимает, как действовать в условиях неопределенности, тем меньше возникнет хаоса и тем выше будут шансы пройти кризис максимально безболезненно.



Зарубежные сценарии для вдохновения

ПЕРВЫЕ 24 ЧАСА ПОСЛЕ КИБЕРАТАКИ

ЧЕК-ЛИСТ ДЛЯ РУКОВОДИТЕЛЕЙ

☐ **Зафиксировать точку невозврата**

Сохранить резервные копии. Изолировать их физически. Проверить целостность.

Бэкапы — это не архив, а ваш единственный шанс вернуть бизнес в строй.

☐ **Остановить распространение**

Разорвать зараженные связи. Изолировать сегменты сети.

Инфицированные системы не выключать — они источник доказательств и понимания масштаба.

☐ **Перекрыть вход**

Оценить возможность полной изоляции от интернета. Удаленный доступ — только через VPN + 2FA. ***Никаких исключений и «срочно нужно подключиться».***

☐ **Взять в руки управление**

Создать кризисный штаб: руководство, ИТ, ИБ, юристы, PR. Отдельный защищенный канал связи с личных устройств. Один центр ответственности и никаких параллельных обсуждений.

☐ **Подключить внешнюю команду реагирования**

Независимая оценка масштаба. План локализации и восстановления. Каждый час задержки — это рост убытков и удар по репутации.

☐ **Решить, что спасаем в первую очередь**

Что генерирует выручку?

Что критично для клиентов?

Что поддерживает операционную деятельность?

В кризисе спасают не всё — спасают главное.

☐ **Перезагрузить доверие**

Сменить все критические пароли. В первую очередь — администраторские учетные записи.

Ключевые доступы — двойной сброс и усиленная аутентификация.

После атаки нельзя считать ни один доступ безопасным.

Команда спасения «Инфосистемы Джет»

ВОССТАНОВЛЕНИЕ И УСИЛЕНИЕ ИНФРАСТРУКТУРЫ ПОСЛЕ АТАКИ

ЧЕК-ЛИСТ ДЛЯ ТЕХНИЧЕСКОЙ КОМАНДЫ

☐ **Поднять базовый контур**

- Определить порядок запуска ИТ-систем/сервисов для базовой работы инфраструктуры.

В приоритете — виртуализация, домен, DNS, базы данных, критичные сервисы для бизнес-систем. Далее восстанавливаем исходя из бизнес-ценности, а не по списку серверов.

☐ **Вернуть данные без повторного заражения**

- Проверить копии на целостность.
- Разворачивать копии только в изолированном сегменте.
- Проверить копии на отсутствие признаков компрометации.
- В продуктив переносить исключительно проверенные данные.

«Выжившая» копия = небезопасная копия.

☐ **Хосты: ничего «как было» не возвращаем**

Незараженные системы

- Не перезагружать до завершения сбора цифровых улик (логов).
- Проверить на отсутствие компрометации хостовыми средствами защиты (антивирусное ПО/EDR).
- При подозрениях — полная переустановка.
- Только актуальные версии ПО.

Зараженные системы

- Снять цифровые улики (логи).
- Полное форматирование.
- Чистая установка ОС.
- Развернуть защиту с актуальными правилами.
- Вернуть только проверенные сервисы.

Восстановление из старого образа — риск повторной атаки.

☐ **Доступы: доверие обнуляется**

- Принудительный сброс всех доменных и локальных паролей.
- Для krbtgt — двойной сброс с ожиданием репликации.
- Пересмотреть права администраторов.

После инцидента «чистых» учетных записей не существует.

☐ **Сеть: минимальный периметр**

- Удаленный доступ — только VPN + 2FA.
- Разрешить только то, что крайне необходимо.
- Внедрить сегментацию и жесткие правила между сегментами.
- Загрузить актуальные индикаторы компрометации на периметровый межсетевой экран.

☐ **Обновить и усилить**

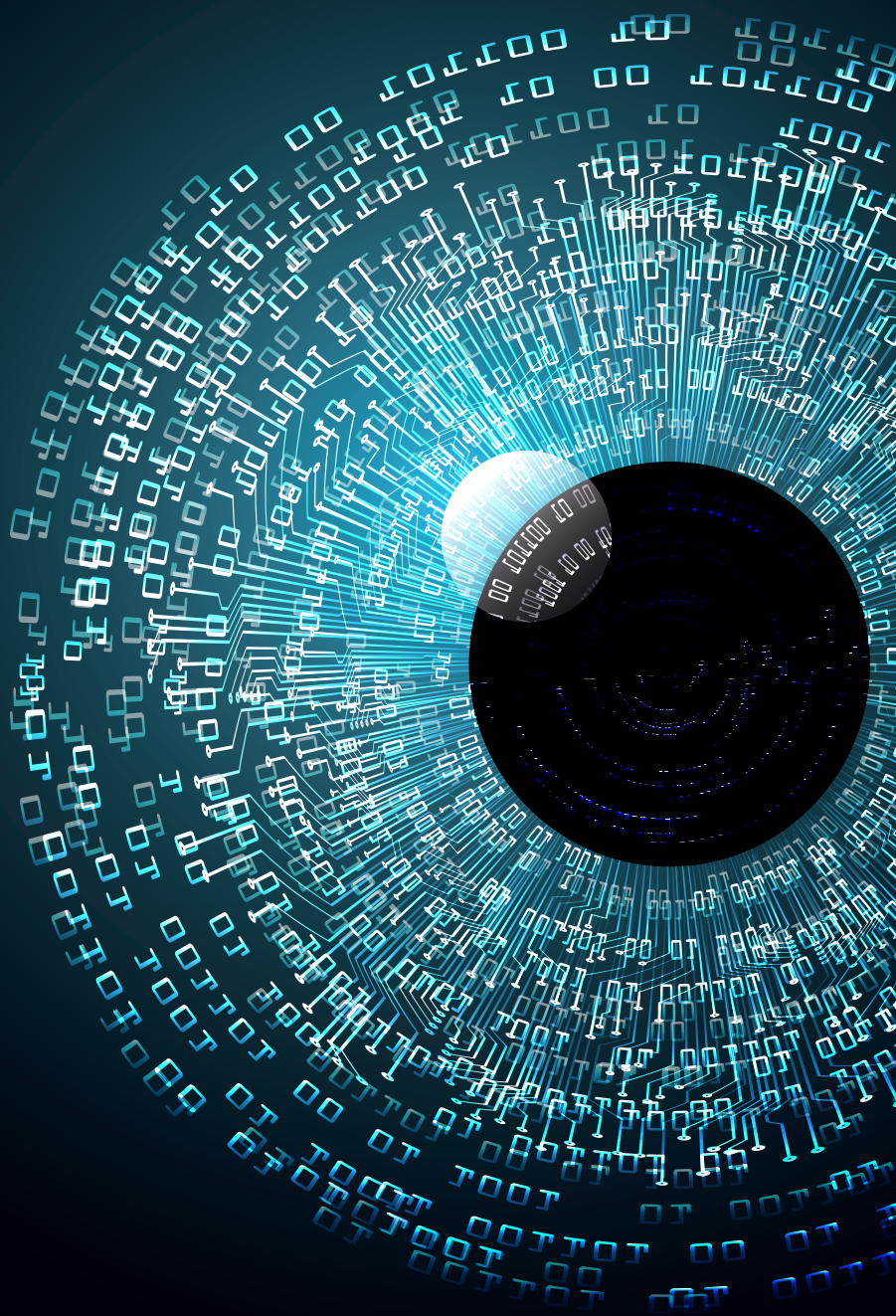
- Обновить устаревшее ПО.
- Перевести системы на поддерживаемые версии.
- Провести настройку безопасности Active Directory.
- Отключить устаревшие протоколы (SMBv1, NTLMv1, LLMNR).
- Проверить делегирование и избыточные привилегии.

Восстановление — это не возврат к прежнему состоянию. Это точка пересборки инфраструктуры.

Команда спасения «Инфосистемы Джет»

JET SCALE

[анализ кода как сервис]



Платформа, объединяющая:

- Анализ кода на уязвимости с помощью SAST / SCA / DAST / Secret Detection
- Анализ достижимости уязвимостей
- Корреляцию и дедупликацию результатов
- Экспертную валидацию
- Бесшовную интеграцию в ваш CI/CD

JET SCALE

jetscale@jet.su

ГОСТЬ НОМЕРА

МОЖНО ЛИ ПРЕДСКАЗЫВАТЬ КИБЕРКАТАСТРОФЫ?

АВТОР

Алексей Лукацкий,

главный евангелист
Positive Technologies

Когда жители Древней Греции собирались у подножия Парнаса, ими двигало не только почтение к богам и желание участвовать в симпосиях, на которых пили разбавленное вино и вели умные беседы. Они шли к оракулу с очень простым и понятным человеческим желанием — узнать, будет ли война, придет ли засуха и выживет ли их город. Будущее пугало своей туманностью, а цена ошибки была слишком высокой. Люди всегда искали тех, кто умеет заглядывать за горизонт.

В других цивилизациях происходило то же самое. Шаманы, жрецы, звездочеты, толкователи снов — методы были разными *(кто-то смотрел на звезды, кто-то — на полет птиц, а кто-то — на внутренности жертвенных животных или на витиевато разлитую кофейную гущу)*, но мотив оставался общим: снизить неопределенность. Сделать неизвестное хоть немного управляемым. Человеку вообще трудно жить в состоянии «мы не знаем», особенно когда на кону выживание. Это стремление предсказать критические события не исчезло вместе с оракулами. Оно просто сменило форму.

Сегодня вместо храмов — дата-центры. Вместо жрецов — аналитики, актуарии и специалисты по безопасности. Вместо прорицаний — модели, симуляции и сценарные стресс-тесты. Засухи сменились глобальными сбоями облаков, нашествия варваров — атаками вымогателей, а вражеские армии — скомпрометированным ПО в цепочках поставок. Современные города — это распределенные ИТ-инфраструктуры, где одна уязвимость может «уронить» десятки компаний разом. И вопрос все тот же: что будет, если случится катастрофа? И, как и тысячи лет назад, нас беспокоит не сама неопределенность, а ее последствия.

Моделирование киберрисков — это, по сути, современная попытка понять: можно ли заранее вычислить, куда придется следующий удар судьбы? Конечно, сегодня мы не гадаем по дыму костра. Мы строим вероятностные распределения, прогоняем симуляции по методу Монте-Карло, считаем хвостовые риски и анализируем точки отказа. Мы оперируем терминами «системные риски», «каскадные сбои» и «недопустимые события». Но в основе лежит все то же человеческое стремление — сделать будущее чуть менее пугающим благодаря знанию.

Вопрос только в том, не превращаемся ли мы иногда в новых оракулов — с красивыми графиками вместо туманных пророчеств. И здесь начинается самое интересное, потому что довольно быстро становится ясно: современные модели — это не оракулы древности.

Проблема «погоды» и поведения

Засуху можно изучать по архивам осадков, землетрясения — по тектонике, ураганы — по температуре океана. Там есть физика, исторические ряды и повторяемость. Именно поэтому страхование жизни или ОСАГО — понятные услуги: они базируются на актуарных таблицах с данными многолетних наблюдений.

Но киберкатастрофа — это не природное явление. Это поведение.

Поведение злоумышленника, который сегодня действует ради денег, завтра — по идеологии, а послезавтра — по указке спецслужб. Поведение инженера, который вовремя не поставил патч, сославшись на стандартное окно в 90 дней. Поведение компании, решившей сэкономить на сегментации сети, потому что «раньше ничего плохого не случалось». Поведение рынка, который массово пересел на один и тот же облачный сервис, единственный оставшийся после ухода всех иностранцев из России.

Мы пытаемся моделировать не погоду, а систему с разумными участниками, причем некоторые из них кровно заинтересованы в том, чтобы разрушить нашу модель. Поэтому моделирование здесь — это не про «что случится», а про то, «насколько плохо может быть».

Как мы пытаемся предсказывать сегодня?

Современные подходы можно разделить на несколько типов:

1. Сценарные модели. Мы придумываем стресс-сценарий: падает крупное облако, появляется zero-day в глобально используемом софте, компрометируется популярная библиотека. Задаем параметры: сколько компаний затронуто, сколько длится сбой, какой ущерб. Это полезная, но все же гипотеза.

2. Вероятностные модели. Здесь появляются распределения, «хвосты» и симуляции Монте-Карло. Они не предсказывают конкретную атаку, но рисуют диапазон потерь и показывают ту самую зону «1 раз в 200 лет», в которой компания может просто перестать существовать.

3. Поиск «черных лебедей». Попытка встроить в модели гипотетические сверхсценарии: глобальный сбой DNS, массовая компрометация маршрутизаторов, подмена популярной библиотеки в репозитории. Это уже не статистика, а управляемая фантазия.

4. Поведенческие подходы. Red Team'инг, киберучения, симуляции киберпреступников в рамках кибериспытаний. Они не считают вероятности, они проверяют реакцию: как быстро отключится сегмент, кто примет решение, где возникнет паника.

5. Принципы антихрупкости. Подход, при котором мы не предсказываем удар, а строим систему так, чтобы он не стал фатальным. Микросегментация, избыточность, физическое разделение. Это уже не столько про прогнозирование, сколько про изменение самой философии оценки рисков.

Отдельно стоит регуляторный подход *(обычно от ФСТЭК и Банка России)*. Часто требования здесь строятся не на расчетах, а на экспертной оценке. Иногда глубокой, но чаще — интуитивной. Где-то устанавливается «допустимый уровень риска» без прозрачной методологии, где-то определяются «негативные последствия» без оценки вероятности. Экспертное мнение — важный инструмент, особенно при нехватке данных, но у него есть пределы. Эксперт — человек, а значит, он подвержен когнитивным искажениям, опирается на недавний опыт и часто мыслит шаблонами уже случившихся инцидентов. Тема этих искажений глубока как океан, и именно они часто делают экспертную оценку слишком уязвимой.

Ловушка точности

Выше я назвал только несколько самых популярных подходов. А ведь существуют еще кооперативное моделирование угроз, коллективные векторные сценарии, теория допустимого ущерба, индикаторы на уровне экосистемы, агрегированные модели и др. В итоге мы получаем странную картину. С одной стороны — сложнейшие математические модели, с другой — управленческие решения, принятые «на глаз», просто потому что так кажется разумным. Это главный конфликт современной кибербезопасности.

Мы хотим точности, но живем в неопределенности. Считаем «хвосты», но решения принимает человек. Графики дают ощущение контроля: кажется, что хаос приручен, а катастрофа — это просто число в таблице. Но именно здесь и начинается самообман, продиктованный уже не раз упомянутыми когнитивными искажениями. Модель может оценить масштаб потерь, но она не гарантирует, что этот масштаб будет пределом. Любая модель — лишь приближение.

Если в системе есть единая точка отказа, модель может ее подсветить, но она ее не устранит. Если инфраструктура монолитна, если процессы централизованы, если управление завязано на один канал связи, если технологическая цепочка не имеет физической альтернативы — предел разрушения уже встроен в систему. И тогда цифра «1 в 200 лет» становится просто аккуратно оформленной иллюзией.

Анатомия недопустимых событий

Разговор о катастрофах должен в какой-то момент перестать быть разговором о вероятностях *(может, поэтому в последней методике оценки угроз ФСТЭК от вероятности отказались совсем)*. Он должен стать разговором о границах:

- Где заканчивается локальный инцидент и начинается системная деградация?

- Где штраф становится триггером каскадных финансовых последствий?
- Где потеря прибыли оборачивается потерей бизнеса?

И вот мы плавно подходим к идее недопустимых событий, которые могут быть чем угодно: простоем, штрафом, потерей прибыли, отзывом лицензии, остановкой отгрузок, срывом контрактов, падением доверия регулятора, массовым оттоком клиентов.

Даже «обычная» утечка данных, если она случилась в неподходящий момент и по неправильной причине, может стать недопустимой *(оборотный штраф в начале года при поступлении основных доходов в 4-м квартале)*.

Ключевой критерий здесь — недопустимое событие. Это ситуация, которая переводит систему в состояние, из которого нет приемлемого возврата — по времени, по деньгам или по управляемости.

Недопустимое событие — это не обязательно «взрыв». Иногда оно выглядит внешне скучно:

1. Производство стояло не сутки, а месяц, и цепочка поставок развалилась *(как это было в инциденте с шифровальщиком у Jaguar Land Rover летом 2025 года)*.
2. Штраф оказался не просто большим, а экзистенциальным, потому что совпал с кассовым разрывом и кредитными ковенантами.
3. Потеря небольшого контракта привела к небольшому проседанию прибыли, но контракт оказался с ключевым клиентом — и после этого была потеряна существенная доля рынка.
4. Формально после инцидента всё восстановили, но регулятор приостановил деятельность, а рынок изменил отношение к компании.

Недопустимость — это про порог разрушения. Нас должен интересовать не «средний ущерб», а вопрос: где у нашей компании проходит линия, после которой восстановление становится бессмысленным или очень-очень-очень дорогим? Моделирование полезно именно здесь: оно помогает понять, какие цепочки событий и сценарии способны довести нас до этой линии.

Инженерия выживания

Вероятностная модель соблазняет думать категориями «0,5% в год». Но для конкретной компании сценарий «1 раз в 200 лет» не означает «через 200 лет» *(и это снова про когнитивные искажения)*. Это означает: может случиться завтра. Вероятность — это характеристика множества наблюдений. Но катастрофа — это всегда единичное событие. В этом месте статистика сталкивается с реальностью. Именно поэтому Талеб говорил об антихрупкости. Мы должны признать, что мир нестабилен. Если вы не можете точно предсказать удар, его место и время, а также последствия, измените структуру так, чтобы удар не был фатальным.

Поэтому единственный верный путь — антихрупкость. В результативном кибербезе это означает:

- уменьшать связанность и изолировать сегменты;
- исключать единые точки отказа;
- допускать управляемую избыточность и проектировать отказоустойчивые механизмы;
- ограничивать «радиус взрыва» любого сбоя.

Это не снижает неопределенность, но снижает последствия. Модель говорит: «Вот хвост», а инженерия отвечает: «Мы сократим его длину». Ну и конечно, нельзя забывать про проверку достижения реального снижения последствий, что реализуется выставлением компании на кибериспытания.

У нас есть преимущество перед древними греками, которые не могли изменить судьбу: мы можем менять свою «природу». Мы можем не концентрировать контроль в одном облаке, не строить монолитные сети и не завязывать все на одного вендора. В этом месте моделирование перестает быть гаданием и становится инструментом дисциплины мышления. Антихрупкость создается не в Excel или «Моем офисе», она создается за счет архитектуры. Главный сдвиг, который нам нужно сделать, — спрашивать не «что случится?», а «что не должно нас разрушить?».

Когда компания начинает мыслить именно так, кибербезопасность перестает быть цифровой Кассандрой, которой никто не верит. И она уже не мальчик, кричащий: «Волки, волки!» Она становится нормальным инженерным инструментом выживания.

ГЛАЗАМИ ХАКЕРА

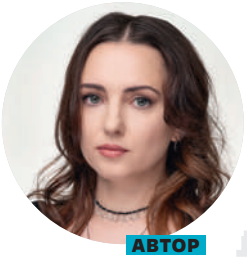
КАК ОСТАВАТЬСЯ НА ШАГ ВПЕРЕДИ КИБЕРПРЕСТУПНИКОВ И КАКИЕ СИГНАЛЫ МОЖНО НАЙТИ В ИНТЕРНЕТЕ

За последние три года угроза уничтожения ИТ-инфраструктуры предприятий в результате хакерских атак перестала быть гипотетической. Она перешла в категорию реальных наравне с техногенными авариями, финансовыми кризисами и санкционными ограничениями. Минимизировать риски и не допустить реализации негативного сценария — ключевая цель информационной безопасности. И ценность мониторинга внешних цифровых угроз — не столько в попытках предсказывать катастрофы («черных лебедей»), сколько в возможности находить уязвимые места, которые делают систему чувствительной к ударам, и заранее укреплять ее там, где уже видна трещина.

АВТОР

Ринат Сагиров,

директор центра мониторинга и реагирования компании «Инфосистемы Джет»



АВТОР

Анастасия Кисько,

руководитель группы мониторинга внешних киберугроз компании «Инфосистемы Джет»

Геополитическая напряженность остается одним из основных драйверов роста числа кибератак. И в 2026 году в России их станет на треть больше по сравнению с 2025-м, следует из прогноза Positive Technologies. Причем злоумышленникам не важен размер компании — любой бизнес может оказаться под угрозой. Киберпреступники проникают в систему и могут долго находиться в инфраструктуре незамеченными, чтобы собрать информацию для последующей продажи или публикации. Мы наблюдали кейсы, когда в открытый доступ попадали дампы с большим количеством чувствительных данных компании, включая информацию о клиентах и подрядчиках.

Кроме геополитики, фактором расширения поверхности атак становится цифровизация: применение облачных технологий, удаленная работа и прочие аспекты увеличивают количество потенциальных точек входа в ИТ-инфраструктуру.

Кейс

Недавно при мониторинге GitHub *(веб-сервиса для хостинга ИТ-проектов)* наша команда выявила публичный репозиторий, используемый злоумышленниками для подготовки масштабной фишинг-атаки на нашего клиента — государственную организацию.

В ходе анализа в репозитории были обнаружены:

- HTML-код поддельного сайта, полностью имитирующего официальный портал госорганизации;
- PDF-документы для создания легенды наполненности сайта;
- два APK-файла *(формат файлов приложений для Android)*: «Официальное приложение организации» и «Антивирус организации».

Анализ APK показал наличие вредоносной нагрузки, функции перехвата данных, доступа к системе и скрытого управления устройством. Специалисты компании «Инфосистемы Джет» своевременно оповестили клиента и отреагировали на выявленную угрозу. Наши рекомендации клиенту включали выпуск предупреждения через официальные каналы, проверку пользовательских устройств и блокировку доменов.

Кошки-мышки и базовая гигиена

Хакерские группировки, как правило, используют в своих атаках давно известные уязвимости и мисконфигурации ИТ-инфраструктуры. По статистике наших команд коммерческого SOC *(Security Operations Center — центр мониторинга ИБ)* Jet CSIRT и лаборатории практического анализа защищенности, на получение повышенных привилегий в инфраструктуре уходит не более одного дня с момента получения первоначального доступа.

При реализации мягкого сценария реагирования «выбивание» хакеров зачастую превращается в игру в кошки-мышки, так как специалисты ищут иголку в стоге сена. Поэтому крайне важно усложнить путь хакерам по времени, реализовав меры базовой гигиены. К ним относятся:

- устранение уязвимостей и мисконфигураций на сетевом периметре;
- сетевая сегментация;

- харденинг *(усиление защиты)* и устранение высококритичных misконфигураций в базовых ИТ-сервисах: корпоративном домене, центре сертификации, корпоративной почте, среде виртуализации;
- устранение высококритичных уязвимостей в инфраструктуре;
- обеспечение безопасности среды виртуализации.

Взгляд на инфраструктуру со стороны

Для построения антихрупкости важны сигналы: они заставляют систему адаптироваться и эволюционировать. Но даже идеальный SOC видит только то, что уже внутри периметра. Чтобы обнаружить угрозу до входа, нужен взгляд со стороны. Мониторинг внешних цифровых угроз, который входит в более широкое понятие кибербразведки, позволяет заметить такие сигналы до того, как угрозы перерастут в инцидент, поскольку показывает инфраструктуру глазами злоумышленников. Это способ превратить хаос атак в конструктивный стресс. Не защититься от неизвестного, а снизить уязвимости там, где их видно снаружи.

Мониторинг внешних цифровых угроз помогает:

- заметить утечки данных и обсуждение вашей компании на хакерских форумах до атаки;
- найти уязвимые точки на внешнем периметре *(старые домены, открытые порты, незащищенные сервисы)*, которые видны злоумышленникам;
- понять, кто может атаковать *(конкуренты, киберпреступники)*, какие методы *(фишинг, эксплуатация уязвимостей)* и инструменты использует злоумышленник, а также на что он нацелен;
- отследить риски атаки через подрядчиков — часто нападают не напрямую, а через слабое звено в цепочке поставок;
- быстро блокировать фишинговые домены и поддельные ресурсы, защищая бренд и сотрудников.

Мониторинг внешних киберугроз позволяет перейти от реакции к действиям — заранее закрыть слабые места, представляющие опасность для компании. Это экономит время, деньги и бережет репутацию.

Интернет дает больше, чем кажется

Источники для мониторинга внешних цифровых угроз можно перечислять бесконечно, но на практике все строится на одном фундаменте — открытых данных. Весь интернет, от публичных репозиториев до соцсетей и утечек, дает больше полезной информации, чем кажется.

От аналитика уже зависит дальнейшее:

- как быстро находить сигнал в шуме — например, украденные креды *(учетные данные)* сотрудников в утечках или обсуждение инфраструктуры компании на форумах;
- как работать с даркнетом: понимать логику площадок, видеть разницу между шумом и реальной угрозой, не светить себя при сборе данных;
- когда и как вести легендированную переписку — не для «охоты на хакеров», а чтобы получить контекст: какие данные продаются, кто в них заинтересован.

Главный принцип простой: не гнаться за количеством источников. Лучше глубоко освоить 3–4 рабочих канала и встроить их в процессы — мониторинг, реагирование, оценку рисков. Инструменты приходят и уходят, а ценность создает аналитик, который умеет задавать правильные вопросы и видеть картину целиком.

Практические рекомендации

Добавив мониторинг внешних цифровых угроз в процессы мониторинга, команда SOC получает возможность увидеть инфраструктуру глазами хакера и проактивно отреагировать на атаку еще на этапе ее подготовки. Это не формальная процедура ИБ, а эффективный инструмент защиты критически важных активов компании. На основе получаемой аналитики формируются конкретные рекомендации для команды внутренней ИБ: что поставить на контроль и усилить в реализуемых мерах.

Связка «внешняя разведка — внутренняя защита» на практике

Учетные данные компании в продаже на форумах	**Рост атак через подрядчиков**	**Критическая уязвимость во внешних сервисах компании**	**Фишинговые домены под бренд компании**	**Рост массовых DDoS-атак на ресурсы компаний смежного профиля**
Проверить наличие МФА (многофакторной аутентификации) либо рассмотреть ее внедрение, проверить компрометацию сотрудников, усилить парольную политику, сменить пароли	Ввести обязательный аудит третьих сторон. При компрометации подрядчика проверить наличие нелегитимных действий в ИТ-инфраструктуре из-под его учетных данных, поставить на дополнительный контроль	Присвоить уязвимости высокий приоритет, организовать экстренное обновление ПО, временно ограничить доступ. Провести threat hunting (охоту за угрозами) для проверки гипотезы эксплуатации, проработать способы детектирования	Провести проверку на предмет взаимодействия с фишинговым доменом из инфраструктуры	Пересмотреть настройки периметра, увеличить резерв каналов, актуализировать план реагирования, добавить в политику ИБ разделы по противодействию сетевым атакам

Таким образом, внешний мониторинг собирает информацию о потенциальных и реальных стрессорах. И это знание помогает превратить ее в возможности для усиления системы. По Талебу, для построения антихрупкости важно выявлять трещины до того, как по ним ударят, — и не просто заклеивать их, а перестраивать архитектуру.

Ценность мониторинга внешних угроз

Мониторинг внешних угроз формирует устойчивое преимущество компании по четырем направлениям:

Преимущество во времени. Компания еще до начала атаки обнаруживает ее признаки: утечку учетных данных сотрудников, подготовку DDoS-атак или обсуждение ее инфраструктуры в закрытых сообществах. Это дает дни или недели на устранение уязвимостей — вместо часов после взлома.

Снижение ущерба. Даже при успешном проникновении злоумышленника компания, обладающая данными внешней разведки, быстрее идентифицирует вектор атаки и сокращает время реагирования. Часто удается остановить атаку на этапе разведки — до компрометации критических активов.

Информационная асимметрия в пользу компании. Раньше злоумышленник действовал с преимуществом: он знал слабые места инфраструктуры, а компания — нет. Мониторинг внешних угроз меняет баланс: компания видит свой периметр глазами хакера.

Формирование культуры осведомленности. Регулярное получение сведений о реальных угрозах трансформирует отношение к информационной безопасности внутри коллектива. Разработчики закрывают уязвимости осознанно, сотрудники становятся осторожнее с письмами, руководство быстрее принимает решения по ИБ. Это меняет мышление — с «надо бы» на «мы видим угрозу — действуем».

На три хода вперед

Использование данных внешнего мониторинга позволяет сфокусироваться на актуальных угрозах, специфичных для организации, оптимизировать распределение ресурсов ИБ с учетом текущих рисков и обосновать необходимость инвестиций в информационную безопасность. Но главное — перейти от реактивной защиты к опережающей. Вместо ожидания инцидента организация заранее укрепляет наиболее уязвимые точки, основываясь на данных о реальных угрозах. Это дает возможность подготовиться к атаке.

Можно провести аналогию с шахматами: побеждает не тот, кто быстрее двигает фигуры, а тот, кто видит на три хода вперед. Эксплуатировать базовые и известные критические уязвимости начинают достаточно быстро, поэтому наличие одного лишь внутреннего мониторинга не является гарантией безопасности. Однако мониторинг внешних цифровых угроз помогает проактивно реагировать и обеспечивать компании преимущество в этой игре. Он не гарантирует, что атаки не будет, но позволяет усилить защиту перед нападением.

СЕРИЯ 1


Пятница, вечер.
Все почти разошлись
ENCRYPTION INITIALIZED.
ALERT: MASSIVE FILE CHANGE DETECTED
PING

ПРОДОЛЖЕНИЕ СЛЕДУЕТ...

ЕСЛИ ВСЕ ЗАШИФРОВАНО

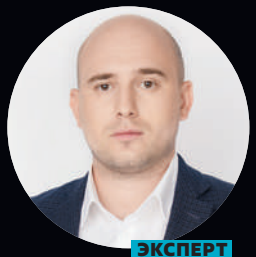
АЛГОРИТМ ДЕЙСТВИЙ, КОГДА ВИРУС УЖЕ В СЕТИ

- Шифровальщики используют одни и те же точки входа в большинстве атак
- Злоумышленник может месяцами находиться в инфраструктуре незаметно
- Ошибки реагирования часто наносят больший ущерб, чем сама атака

ЭКСПЕРТ

Константин Сапронов,

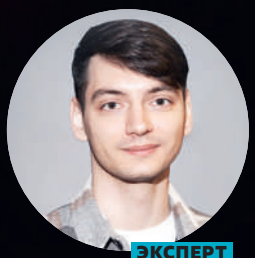
руководитель глобальной команды по реагированию на компьютерные инциденты «Лаборатории Касперского»



ЭКСПЕРТ

Ринат Сагиров,

директор центра мониторинга и реагирования компании «Инфосистемы Джет»



ЭКСПЕРТ

Владимир Гришанов,

руководитель BI.ZONE Compromise Assessment

Атаки программами-шифровальщиками уже давно перестали быть проблемой «плохо защищенных» компаний. Сегодня под удар могут попасть все — даже организации с развернутыми системами мониторинга, сегментацией сети, многофакторной аутентификацией и формально выстроенными процессами информационной безопасности.

Константин Сапронов

«Атаки шифровальщиками в последние годы стали самой распространенной причиной обращений. Причем их доля постепенно увеличивается из года в год. Если смотреть на инциденты в пределах одного года, то обычно речь идет о действиях одних и тех же групп атакующих. Они используют хорошо отработанные техники, тактики и процедуры, которые повторяются от атаки к атаке. Поэтому даже компании с развитой системой защиты могут оказаться уязвимыми, если в их инфраструктуре остаются слабые архитектурные места или не закрыты типовые точки входа».

Причина проста: злоумышленники действуют системно. Они изучают инфраструктуру, закрепляются в ней, повышают привилегии, уничтожают резервные копии и только затем запускают шифрование. В результате даже зрелая с точки зрения средств защиты компания может столкнуться с полной недоступностью ключевых сервисов. В этой реальности фокус смещается. Главный вопрос звучит не «Как мы защищаемся?», а «Как мы восстанавливаемся?».

Ринат Сагиров:

«Традиционные подходы к обеспечению непрерывности бизнеса формировались в эпоху, когда основной угрозой для бизнеса считались природные катастрофы, аварии оборудования и человеческие ошибки. Но за последние годы компании столкнулись с кибератаками, которые выводят их из строя на дни, а иногда — на недели. Сейчас важно задавать себе два вопроса: “Как мы восстановимся после шифрования?” и “Как мы будем действовать, когда нас взломают?”. Эти вопросы переориентируют вектор развития и направляют объединенные усилия ИТ и ИБ в сторону антихрупкой ИТ-инфраструктуры, основными принципами которой являются: снижение поверхности атаки для замедления действия злоумышленника в инфраструктуре; выстраивание эффективных процессов выявления и реагирования; знание точной последовательности действий по восстановлению».

Ниже — структурированный алгоритм действий в ситуации, когда вирус-шифровальщик уже в сети, а стандартный план реагирования оказался недостаточно продуманным.

Как ломают: актуальные сценарии проникновения

Перед тем как говорить о восстановлении, важно понять, через какие векторы злоумышленники чаще всего получают доступ.

Владимир Гришанов

«В 90% компаний, подвергшихся атакам программами-шифровальщиками, мы видим одни и те же критические проблемы: слабая защиты почты, отсутствие многофакторной аутентификации, уязвимый периметр и недостаточный контроль внешних подключений».

СРЕДНЕЕ ВРЕМЯ НАХОЖДЕНИЯ ЗЛОУМЫШЛЕННИКА В ИНФРАСТРУКТУРЕ ДО ЗАПУСКА ШИФРОВАНИЯ СОСТАВЛЯЕТ

МИНИМАЛЬНЫЙ ПЕРИОД ОТ ПРОНИКНОВЕНИЯ ДО НАЧАЛА ШИФРОВАНИЯ МОЖЕТ СОСТАВЛЯТЬ ВСЕГО

МАКСИМАЛЬНЫЙ ПЕРИОД ОТ ПРОНИКНОВЕНИЯ ДО НАЧАЛА ШИФРОВАНИЯ МОЖЕТ СОСТАВЛЯТЬ ДО

ВЗЛОМ УДАЛЕННОГО ДОСТУПА: RDP, СЛАБЫЕ ПАРОЛИ, БРУТФОРС

Протокол удаленного рабочего стола *(Remote Desktop Protocol, RDP)* остается одной из самых частых точек входа для злоумышленников. При отсутствии ограничения по IP, двухфакторной аутентификации и политики сложных паролей, RDP становится удобной мишенью для атак методом перебора *(brute force)*.

Типовой сценарий:

- перебор учетных данных;
- вход под легитимной учетной записью;
- закрепление в системе;
- эскалация привилегий до доменного администратора.

ФИШИНГ И СОЦИАЛЬНАЯ ИНЖЕНЕРИЯ

Зараженные вложения в электронных письмах, ссылки на поддельные порталы, эксплуатация доверия сотрудников — классика, которая продолжает работать. Во многих расследованных инцидентах именно электронная почта становится первоначальной точкой входа.

По данным расследований BI.ZONE, недостаточно защищенная почтовая инфраструктура остается одной из самых распространенных точек входа. Если почтовые шлюзы не используют современные механизмы фильтрации вложений и ссылок, фишинговые письма легко обходят защиту и становятся стартовой точкой атаки.

После запуска вредоносного кода злоумышленники:

- получают первичный доступ;
- разворачивают инструменты удаленного администрирования;
- начинают разведку сети.

УЯЗВИМОСТИ В ПУБЛИЧНЫХ СЕРВИСАХ

Особенно часто используются:

- VPN-шлюзы;
- почтовые серверы;
- веб-приложения.

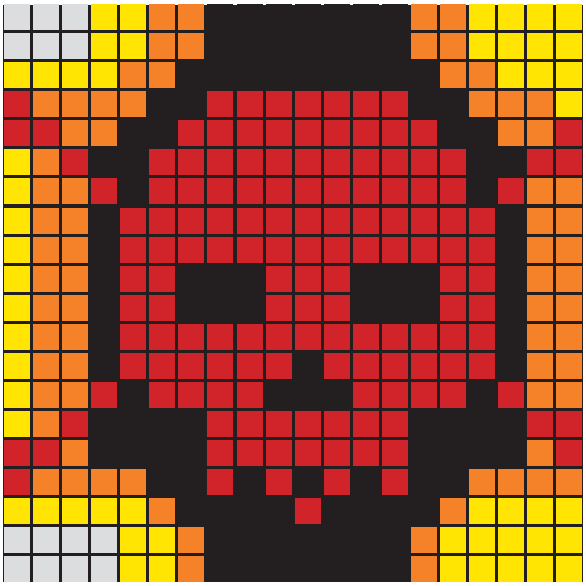
Отдельную роль играет скорость эксплуатации уязвимостей. Например, среднее время от публичного раскрытия уязвимости до начала ее массовой эксплуатации сегодня составляет всего несколько дней. В резонансных случаях сканирование инфраструктуры начинается уже в первые часы после появления в открытом доступе proof-of-concept *(PoC)* — кода, демонстрирующего возможность эксплуатации.

Невыполненные обновления, известные уязвимости, ошибки конфигурации позволяют обойти аутентификацию и получить прямой доступ во внутренний контур.

Владимир Гришанов

«По данным экспертов по цифровой криминалистике и реагированию на инциденты (DFIR) BI.ZONE за 2025 год, среднее время нахождения злоумышленника в инфраструктуре до запуска шифрования составляет 42 дня. При этом минимальный период от проникновения до начала шифрования может составлять всего 12,5 минуты, а максимальный — до 181 дня».

Это означает, что атака редко происходит сразу после проникновения. Чаще злоумышленники используют это время для разведки инфраструктуры, повышения



КАК ЗЛОУМЫШЛЕННИКИ ПРОНИКАЮТ В ИНФРАСТРУКТУРУ

- **37%** Эксплуатация уязвимостей публично доступного приложения
- **28%** Внешние удаленные сервисы
- **18%** Фишинг
- **13%** Доверенные отношения
- **4%** Прочее

привилегий, компрометации резервных копий и подготовки инфраструктуры к массовому шифрованию.

По оценке специалистов по реагированию «Лаборатории Касперского», продолжительность атаки может существенно варьироваться в зависимости от целей злоумышленников. В финансово мотивированных операциях атакующие часто действуют стремительнее — от нескольких дней до нескольких недель. Обычно они стараются быстро получить доступ, подготовить инфраструктуру и запустить шифрование. Однако в отдельных случаях присутствие в инфраструктуре может длиться месяцами: киберпреступники выжидают удобного момента для запуска шифрования или публикации украденных данных.

В то же время хактивистские группы могут намеренно откладывать финальную фазу атаки, чтобы приурочить ее к значимой дате или использовать инцидент как негативный информационный повод.

КОМПРОМЕТАЦИЯ ПОДРЯДЧИКОВ И ЦЕПОЧЕК ПОСТАВОК

Атаки через доверенных поставщиков получают все большую распространенность. Если у подрядчика есть удаленный доступ, он автоматически становится частью периметра. При этом сам подрядчик может быть скомпрометирован задолго до инцидента у заказчика.

В расследованиях BI.ZONE подобные сценарии встречаются все чаще. Если подрядчик обладает постоянным удаленным доступом к инфраструктуре, например через VPN или системы удаленного администрирования, его компрометация фактически превращается в готовый канал проникновения в инфраструктуру заказчика. При этом атака может оставаться незамеченной до момента активной фазы шифрования.

Когда все зашифровано: первые часы и стабилизация ситуации

ОПРЕДЕЛЕНИЕ МАСШТАБА

Первые часы после обнаружения шифрования определяют масштаб дальнейших потерь. В этот момент компания фактически оказывается в режиме операционного кризиса, где любое неверное действие способно усугубить ситуацию. Главная задача на этом этапе — не восстановление, а стабилизация. Попытки «быстро починить» инфраструктуру, перезагрузить серверы или срочно запустить антивирусное сканирование чаще всего приводят к утрате цифровых следов и затрудняют последующее расследование.

Константин Сапронов

«Одной из наиболее распространенных ошибок на этом этапе становится попытка немедленно восстановить работоспособность инфраструктуры, не разобравшись в деталях атаки. Если начать переустановку систем или восстановление данных до того, как определены начальный вектор проникновения и перечень скомпрометированных ресурсов, существует высокая вероятность повторной атаки — иногда с еще более серьезными последствиями».

⚓ ИЗОЛЯЦИЯ

Критически важно сохранить текущее состояние систем. Если зараженные серверы немедленно выключить или перезагрузить, можно потерять данные оперативной памяти, в которых находятся ключевые артефакты атаки: процессы шифрования, инструменты удаленного администрирования, активные сетевые соединения. Именно поэтому в первые часы основное внимание необходимо уделять изоляции, а не выключению. Требуется отрезать от сети зараженные хосты, ограничить межсегментное взаимодействие, временно закрыть доступ к общим сетевым ресурсам и, при необходимости, отсоединить удаленные подключения.

Константин Сапронов

«В первую очередь необходимо изолировать сетевую инфраструктуру от внешних соединений и убедиться, что резервные копии критичных данных доступны и надежно защищены. Параллельно нужно начать расследование инцидента — определить тип используемого шифровальщика, возможную точку входа и масштаб компрометации. Только после устранения начального вектора атаки можно переходить к восстановлению систем».

⚓ ПРОВЕРКА ИНФРАСТРУКТУРЫ

Отдельного внимания требует проверка инфраструктуры каталогов. Если используется Microsoft Active Directory, необходимо оценить, не были ли изменены привилегированные группы, не появились ли новые администраторские учетные записи, не модифицированы ли политики безопасности. Как правило, злоумышленник уже получил повышенные привилегии до запуска шифрования и редко действует импульсивно.

⚓ ФИКСАЦИЯ ЦИФРОВЫХ СЛЕДОВ

Параллельно с изоляцией необходимо фиксировать состояние среды. Логи серверов, сетевого оборудования, систем виртуализации, журналы аутентификации и конфигурационные файлы должны быть выгружены и сохранены вне зараженного контура. Эти данные потребуются для анализа вектора атаки, оценки глубины компрометации и подготовки юридической позиции компании.

Управление кризисом: скорость решений важнее иерархии

Когда атака переходит в фазу массового шифрования, классическая модель согласований перестает работать. Если решение об отключении сервисов, остановке VPN или изоляции сегмента принимается через длинную управленческую цепочку, компания теряет драгоценное время. Поэтому в зрелой организации к этому моменту уже должен быть активирован механизм кризисного управления, в рамках которого распределены роли и полномочия.

Если подобная структура заранее не формализована, ее приходится создавать в режиме реального времени, что увеличивает длительность простоя и повышает вероятность ошибок. Практика показывает, что отсутствие четко определенного центра

ТРИ УРОВНЯ РЕАГИРОВАНИЯ

принятия решений приводит к хаотичным действиям: одни команды пытаются восстановить сервисы, другие — продолжают расследование, третьи —дают комментарии внешним контрагентам. В условиях атаки вируса-шифровальщика подобная несогласованность усугубляет ситуацию и наносит дополнительный ущерб.

Оценка масштаба: глубина компрометации и целостность резервных копий

После стабилизации и локализации распространения начинается наиболее сложный этап — оценка реального масштаба ущерба. Важно понять, что зашифрованные файлы — это лишь видимая часть проблемы. Ключевой вопрос заключается в том, насколько глубоко злоумышленник проник в инфраструктуру и какие компоненты были скомпрометированы до запуска шифрования.

Необходимо определить, затронуты ли контроллеры домена, скомпрометированы ли учетные данные администраторов, изменены ли политики безопасности и конфигурации сетевого оборудования. Если злоумышленник находился в сети продолжительное время, велика вероятность того, что он получил доступ к системе резервного копирования и попытался удалить или модифицировать копии.

Проверка целостности бэкапов становится отдельной задачей. В идеале процесс восстановления должен опираться на четкое понимание того, где хранится доверенная резервная копия — заранее проверенная и подтвержденная как безопасная еще до того, как она может понадобиться. Такой подход позволяет исключить риск скрытых «закладок» и предотвратить повторное возникновение инцидента. Важно убедиться, что резервные копии действительно изолированы от производственной среды и не содержат вредоносного кода. Если заражение произошло задолго до обнаружения, восстановление «чистой» версии может потребовать отката на более позднюю точку, чем предполагалось изначально. Это напрямую влияет на фактический объем потерянных данных.

Стратегия: перестроить или восстановить

Когда масштаб компрометации становится понятен, компания встает перед ключевым выбором: восстанавливать инфраструктуру из резервных копий или перестраивать ее с нуля. В теории восстановление из бэкапа выглядит более быстрым вариантом, однако на практике все зависит от уровня доверия к среде.

Если скомпрометированы учетные записи доменных администраторов и неясно, какие изменения были внесены в системные компоненты, частичное восстановление может оставить в инфраструктуре скрытые точки присутствия злоумышленника. В этом случае более рациональной стратегией становится полная переустановка ключевых компонентов с последующим восстановлением данных в очищенную среду.

При наличии офлайн-копий или неизменяемых хранилищ восстановление обычно проходит быстрее за счет изоляции контура резервного копирования от зараженной инфраструктуры. Однако такая изоляция не гарантирует чистоты бэкапов: при длительном присутствии злоумышленника в сети в них могли попасть уже скомпрометированные системы. Если же резервное копирование интегрировано в общий домен без изоляции, риск его компрометации существенно возрастает.

Приоритизация восстановления должна опираться на заранее проведенный анализ воздействия на бизнес. В первую очередь поднимаются те сервисы, без которых невозможна базовая операционная деятельность: учет заказов, логистика, финансовые операции или клиентский сервис, а также поддерживающие их ИТ-сервисы. Все остальные системы восстанавливаются по мере стабилизации среды.

Внешние эксперты и правовые аспекты

В большинстве серьезных инцидентов компания не может ограничиться внутренними ресурсами. Подключение специалистов по цифровой криминалистике и реагированию на инциденты Digital Forensics & Incident Response позволяет определить точку входа, зафиксировать

НЕ СУЩЕСТВУЕТ ОДНОГО ИНСТРУМЕНТА ИЛИ ТЕХНОЛОГИИ, СПОСОБНЫХ ПОЛНОСТЬЮ ЗАЩИТИТЬ ИНФРАСТРУКТУРУ ОТ АТАК ШИФРОВАЛЬЩИКАМИ

цифровые доказательства и оценить возможность дешифрования без выплаты выкупа. Это особенно важно в случаях, когда существует риск утечки персональных или коммерческих данных.

Юридическая оценка необходима для определения обязательств перед регуляторами и контрагентами. В зависимости от отрасли и характера утечки, компании может потребоваться уведомить надзорные органы, клиентов и партнеров. Крайне важно параллельно выстраивать внешнюю коммуникацию: неконтролируемые комментарии сотрудников способны нанести репутационный ущерб, сопоставимый с техническими потерями.

Если киберриски компании застрахованы, условия полиса обычно предусматривают обязательное уведомление страховщика в установленный срок. Несоблюдение процедур может привести к отказу в компенсации.

После восстановления: пересборка архитектуры безопасности

Завершение технического восстановления не означает завершения кризиса. На этом этапе начинается архитектурная переоценка всей модели защиты. Практика показывает, что компании, пережившие атаку вируса-шифровальщика, пересматривают принципы сегментации, усиливают контроль привилегий и внедряют модель Zero Trust.

Владимир Гришанов

«Организации начинают системно внедрять сетевую сегментацию, пересматривать модель доступа к критическим системам и усиливать контроль привилегированных учетных записей. Без этих изменений риск повторной атаки остается высоким».

Изоляция системы резервного копирования становится обязательным требованием. Контур бэкапов должен быть логически и физически отделен от производственной среды, а также предусматривать использование неизменяемых хранилищ и офлайн-копий. Одновременно необходимо усиливать мониторинг: внедрять EDR-решения, выполнять централизованный сбор логов, контролировать аномальную активность учетных записей.

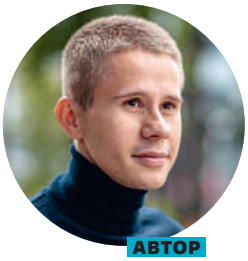
Кроме того, следует уделить внимание регулярным учениям. Тестовые восстановления, сценарные Tabletop-сессии и моделирование атак позволяют не только проверить техническую готовность, но и оценить скорость принятия управленческих решений. Именно в этом проявляется реальная зрелость процессов.

Важно помнить, что не существует одного инструмента или одной технологии, которые способны в полной мере защитить инфраструктуру от атак шифровальщиками. Эффективная защита строится как комплекс мер: установка антивирусной защиты на всех узлах сети, внедрение системы мониторинга и реагирования, разработка надежной стратегии резервного копирования, использование многофакторной аутентификации, регулярное обновление программного обеспечения и управление уязвимостями. Только сочетание этих практик позволит значительно снизить риск реализации катастрофического сценария.

КОГДА «ВСЕ ЛЕЖИТ»

- Атака в любой момент времени — теперь не исключение, а фоновый риск цифровой инфраструктуры
- Защита не может оставаться статичной: любое изменение в инфраструктуре неизбежно требует пересмотра модели угроз и корректировки защитных механизмов
- Сегодня защита от DDoS — это не вопрос удачи, а элемент системного управления рисками

ПРАКТИЧЕСКИЙ РАЗБОР ЗАЩИТЫ ОТ DDoS



АВТОР

Никита Осипов,

ведущий инженер по информационной безопасности компании «Инфосистемы Джет»

DDoS традиционно ассоциируется с атаками на федеральные порталы или крупные телеком-компании. Однако статистика последних лет демонстрирует иную картину: атаки направлены на организации любого масштаба — от госсектора до образовательных и игровых сервисов. Согласно отчету Cloudflare, 2025 год показал кратный рост числа DDoS-инцидентов — до 47,1 млн за год, что на 121% больше, чем в 2024-м. Это означает, что нападение в любой момент перестало быть исключением и стало фоновым риском цифровой инфраструктуры.

Чтобы рассмотреть проблему системно, разберем гипотетический сценарий на примере быстрорастущей компании из сегмента IoT, разрабатывающей и обслуживающей интеллектуальные дверные замки с удаленным управлением.

Бизнес быстро растет, продукт востребован, инфраструктура постепенно усложняется. Какие ресурсы для такой компании критичны? Прежде всего — люди и среда их работы. Это офисная сеть с устойчивым

доступом в интернет, корпоративная почта, система видео-конференц-связи. Для удаленных сотрудников — RA VPN, обеспечивающий безопасный доступ к внутренним ресурсам, а также, при необходимости, корпоративная телефония.

Коммерческая модель предполагает активное онлайн-присутствие. Минимальный набор — публичный веб-портал, через который ведутся продажи и осуществляется коммуникация с клиентами. Однако для самого продукта требуется значительно более сложная ИТ-поддержка: система контроля и управления, серверы обновлений, а также мобильные приложения для iPhone и Android. Функция информационной безопасности формально выстроена: в штате есть руководитель и два специалиста. Однако приоритеты бюджета очевидны: основные инвестиции направлены на развитие продукта и масштабирование бизнеса, — тогда как ИБ финансируется по остаточному принципу.

Компания демонстрирует стремительный рост и уже занимает вторую позицию на рынке. Стратегическая цель — лидерство. Этому способствуют качественный продукт, стабильная работа сервисов и отсутствие публичных инцидентов. Репутация становится ключевым активом. Однако любая рыночная история предполагает наличие противодействующей стороны. Это может быть конкурент, группа хакеров или даже одиночный скрипт-кидди — иными словами, любая из категорий, которые в профессиональной среде принято обозначать термином «черная шляпа».

«Черная шляпа»

Перейдем к анализу ситуации с позиции атакующей стороны. Мотивация может быть различной — от прямого вымогательства до идеологического давления. Мы же в рамках рассматриваемого сценария сосредоточимся на варианте недобросовестной конкуренции.

Компания обслуживает тысячи интеллектуальных замков, внедрила технологию распознавания лица через видеоглазок и фактически сформировала у пользователей новую модель поведения — отказ от физических ключей в пользу мобильного приложения и биометрии. Удобство становится частью повседневной жизни, но именно эта цифровая зависимость и формирует точку уязвимости. В подобном бизнесе репутация — ключевой актив. Пользователь доверяет поставщику не просто устройство, а доступ в собственный дом. Следовательно, воздействие злоумышленников должно быть направлено на подрыв этого доверия. И наиболее чувствительный сценарий — нарушение доступности сервиса. Даже кратковременный отказ системы способен вызвать резонанс и поставить под сомнение надежность решения. Для атакующей стороны это очевидная цель. Рассмотрим возможные инструменты для ее достижения.

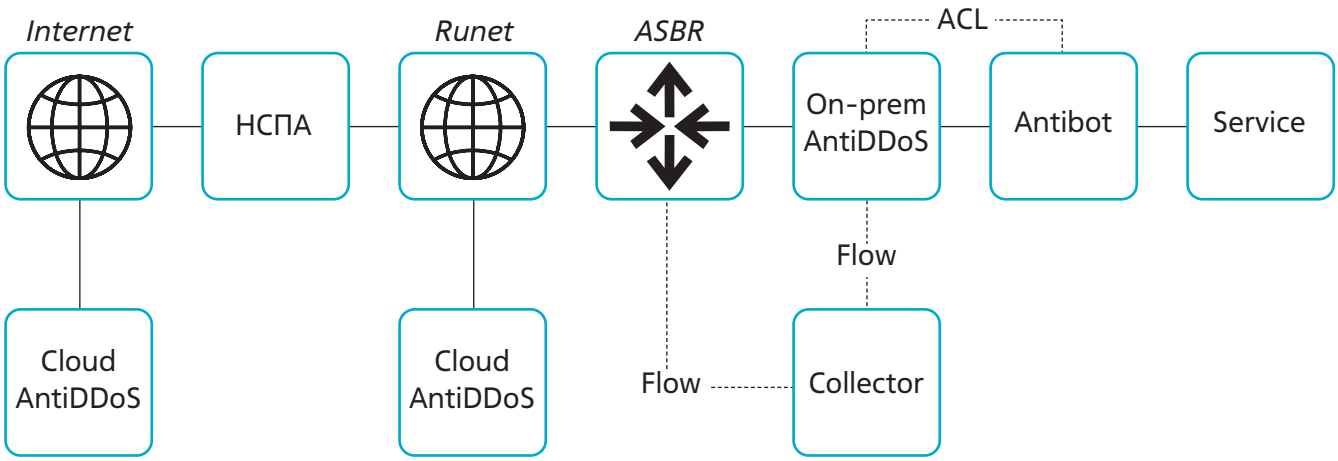
Первый вариант — DDoS-атака сетевого уровня модели OSI ***(L3)***. Механизм хорошо известен: перегрузка канала связи и сетевого оборудования за счет резкого увеличения объема трафика. Такие атаки относительно просты в реализации, при этом рынок DDoS-as-a-Service давно сформирован: аренда ботнета доступна за сравнительно небольшие средства. Если у цели опубликованы веб-приложения, логичным развитием становится комбинированная L3+L7-атака ***(она затрагивает не только сетевой, но и прикладной уровень)***.

Однако современный веб — это уже не набор статичных HTML-страниц. Типовой сервис включает авторизацию ***(в том числе с отправкой SMS-подтверждений)***, поиск, динамический контент, видеотрансляции и т. д. За каждым пользовательским действием стоят обращения к базам данных, системам хранения и сторонним сервисам — с соответствующей нагрузкой на вычислительные и финансовые ресурсы компании.

Второй вариант — атаки прикладного уровня ***(L7)***, ориентированные на логику приложения. Они не требуют большого объема трафика и поэтому менее заметны в общем потоке. Медленные соединения, сложные поисковые запросы, скачивание «тяжелого» контента — все это приводит к постепенному исчерпанию ресурсов сервера. Если дополнительно инициировать массовую отправку SMS-кодов через ограниченное число ботов, можно увеличить операционные затраты и ускорить деградацию сервиса.

В результате пользователь сталкивается не с мгновенным отказом, а с ухудшением качества его работы: задержками, ошибками авторизации, недоступностью функций. Для бизнеса, зависящего от доверия, этого уже достаточно.

Цель сформулирована: нарушение доступности и подрыв репутации. Инструменты определены. Сценарий выглядит реализуемым.



«Белая шляпа»

Вернемся из роли атакующего в позицию защитника. Все сценарии, которые мы только что рассмотрели, применимы к нашей инфраструктуре в полной мере. Вопрос «Готовы ли мы?» неизбежно трансформируется в более практичный: «С чего начать?»

Как и любая атака, защита начинается с разведки — но уже собственной. Необходимо провести инвентаризацию активов — в этом помогают открытые инструменты, такие как Shodan и BGP Looking Glass. Shodan позволяет выявить открытые порты и доменные имена, ассоциированные с конкретным IP-адресом. BGP Looking Glass *(например, bgp.tools)* предоставляет информацию об IP/AS, в том числе с отрисовкой графа связности автономных систем до Tier-1. Анализ маршрутов позволяет убедиться, что весь входящий трафик действительно проходит через заявленных провайдеров защиты и не имеет обходных путей.

Результатом инвентаризации должна стать карточка сервиса, содержащая как минимум:

- назначение сервиса;
- IP-адреса, порты и протоколы взаимодействия;
- доменные имена, закрепленные за сервисом;
- IP-адреса, порты и протоколы зависимых систем *(внешние интеграции)*.

Дополнительно целесообразно подготовить сетевую или логическую схему с полной картой оборудования, через которое проходит трафик, а также зафиксировать результаты нагрузочного тестирования, если оно проводилось. Нагрузочные тесты могут выполняться с использованием Apache Jmeter, Gatling или облачных сервисов. В рамках нашего сценария карточек должно быть не менее шести: интернет, почта, ВКС, VPN, веб-портал, управление замками. Эта информация формирует базовые профили легитимного трафика и позволяет оценить потенциальные векторы атак. Важно учитывать, что атаки разных уровней требуют различного подхода и зачастую средств защиты разных классов.

Отдельного внимания заслуживает архитектура самих средств защиты. Любой компонент может стать точкой отказа. Размещение NGFW перед сервисом или использование его в качестве замены специализированного AntiDDoS-решения только на основании заявленного функционала способно привести к отказу самого NGFW раньше, чем будет достигнут предел устойчивости защищаемого сервиса.

Поэтому принцип эшелонированной защиты остается актуальным. Практика показывает, что эффективная AntiDDoS-архитектура включает:

- фильтрацию на стороне провайдера связи;
- сервис очистки трафика *(scrubbing center)*, в том числе с антибот-функционалом для противодействия продвинутым L7-атакам;
- дополнительный уровень фильтрации внутри ИТ-контура компании.

Компоненты должны быть интегрированы для автоматической передачи политик и запросов на очистку. Для повышения отказоустойчивости архитектуру желательно дублировать на уровне провайдеров. Однако при таком подходе стоимость защиты может оказаться несоразмерной стоимости защищаемых активов. Возникает необходимость оптимизации, и среди возможных мер:

- защита только критически важных опубликованных сервисов;
- формирование запаса прочности за счет масштабирования *(например, средствами Kubernetes или путем добавления серверов приложений)*;
- использование CDN и кэширующих серверов для статического контента;
- ограничение обращений к базе данных по времени выполнения и объему выборки.

Отдельный вариант — перевод трафика на очистку только в период атаки. Такой режим требует наличия анализатора *(FlowCollector)* в собственной инфраструктуре, настройки передачи flow с пограничных маршрутизаторов и механизма оперативного обновления BGP-анонсов по сигналу анализатора.

Вернемся к нашему сценарию. Учитывая ограниченность бюджета и высокую значимость репутации, руководство принимает решение сосредоточиться на защите критических сервисов — веб-портала и системы управления замками. Подготовлены карточки сервисов, подключен сервис защиты от DDoS, настроены профили трафика. Формально — все готово, но реальность, как это обычно бывает, вносит свои коррективы. В праздничный день сервис оказывается недоступным: реагирование происходит без заранее отработанного плана и больше напоминает хаотичные попытки восстановить работоспособность. После стабилизации ситуации проводится разбор причин и выясняется, что защита функционировала корректно, но атака была направлена на устаревшие IP-адреса приложений, для которых отсутствовал ACL на прием трафика исключительно от сервиса защиты.

Еще один важный вопрос — обнаружение инцидента. Информация о проблеме поступила не от системы мониторинга, а была выявлена по факту недоступности сервиса. Это указывает на отсутствие полноценного контроля аномалий трафика и регламентированной процедуры уведомления.

Поэтому план реагирования в случае DDoS, помимо фильтрации, должен включать:

- мониторинг роста трафика и аномалий;
- уведомление дежурной смены;
- заранее определенный план реагирования;
- распределение ролей и взаимодействие с руководством и технической поддержкой.

Логичным этапом развития становится автоматизация. В качестве примера — автоматическая передача FlowSpec-правил провайдеру для применения на границе сети или внесение адресов в списки блокировки на сервисе DDoS по сигналу внутреннего анализатора.

Нормативная база и реальные подходы к AntiDDoS

До этого момента мы рассматривали ситуацию как гипотетический кейс. Возникает закономерный вопрос: насколько такие рассуждения соотносятся с реальной регуляторной практикой? Что предписывает государственный регулятор в части защиты от атак, направленных на отказ в обслуживании?

6 февраля 2026 года на сайте ФСТЭК России был опубликован проект методического документа «Мероприятия и меры по защите информации, содержащейся в информационных системах». В документе прописаны требования к реализации защиты от DDoS-атак, и значительная часть положений коррелируют с теми выводами, к которым мы пришли в рамках сценарного анализа. Однако присутствуют и акценты, заслуживающие отдельного внимания. Например, в документе указывается, что обеспечение защиты должно предусматривать «анализ логической схемы сети с целью поиска узких мест на пути прохождения трафика и реализацию мер по увеличению ресурсов для обработки трафика и сетевых соединений минимум с двухкратным запасом от ожидаемого легитимного трафика».

Иными словами, речь идет не только о фильтрации, но и о проектировании инфраструктуры с учетом потенциальных пиковых нагрузок и резервирования ресурсов. Кроме того, подчеркивается необходимость использования правил фильтрации, исключающих пропуск «всего трафика», то есть от любого

сетевого адреса источника и *(или)* сервиса к любому адресу назначения. Реализуется принцип «все, что явно не разрешено, — запрещено». Это означает, что правила должны быть максимально специфичными и точными, не допускающими прохождения трафика по протоколам и сервисам, которые не используются информационной системой.

Формально требования документа распространяются на государственные информационные системы *(ГИС)*, объекты критической информационной инфраструктуры *(КИИ)* и информационные системы персональных данных *(ИСПДн)*. Однако с инженерной точки зрения изложенные подходы универсальны и применимы к любой организации, заинтересованной в устойчивости своих сервисов.

Документ пока имеет статус проекта, однако его появление уже сейчас доказывает, что рассмотренные нами сценарии не являются теоретическими допущениями. Их логика совпадает с подходами, которые регулятор закладывает в требования к защите от атак, направленных на отказ в обслуживании.

Защита как постоянная практика

Информационные системы динамичны по своей природе: они масштабируются, усложняются, обрастают новыми интеграциями и сервисами. Поэтому их защита не может оставаться статичной: любое изменение в инфраструктуре неизбежно требует пересмотра модели угроз и корректировки защитных механизмов.

AntiDDoS в этом контексте — не разовая настройка, а непрерывный процесс совершенствования. Он включает:

- проведение тестовых DDoS-атак с последующей корректировкой после результата;
- организацию киберучений для группы реагирования и оптимизацию процессов на основе полученного опыта;
- мониторинг и автоматическое пополнение черных списков на базе внешних источников *(feeds)*;
- регулярную инвентаризацию защищаемых ресурсов и актуализацию применяемых политик;
- нагрузочное тестирование сервисов для определения предельной устойчивости;
- внедрение ловушек *(ханипотов)* и анализ поведения атакующих;
- группировку сервисов по профилям трафика и организацию гранулярных политик для каждой группы;
- проработку сценариев полного отказа *(оперативное восстановление)*;
- системное взаимодействие с провайдерами связи и регулятором.

В качестве примера можно привести Национальную систему противодействия атакам *(НСПА)*, в рамках которой круглосуточно осуществляется блокировка атак различной мощности. Организации могут подключать собственное on-site-оборудование защиты от DDoS для автоматической активации контрмер в общей инфраструктуре противодействия. Подобная модель позволяет перераспределить нагрузку, сократить время реакции и, как следствие, минимизировать потенциальный ущерб.

Практические шаги к снижению DDoS-рисков

Практический минимум, который можно выполнить уже сейчас:

- провести инвентаризацию опубликованных сервисов — собственными силами или с привлечением внешнего аудитора;
- оценить их значимость и выделить критичные для непрерывности бизнеса;
- зафиксировать метрики работы в «мирное» время;
- проработать вопрос блокировок на уровне провайдера связи;
- протестировать решения для on-prem- или cloud-защиты от DDoS.

Сегодня защита от DDoS — это не вопрос удачи, а элемент системного управления рисками. Мотивация атакующих может различаться: конкурентная разведка, вымогательство, попытка дестабилизации или банальное хулиганство. Однако последствия для бизнеса предсказуемы: финансовые потери, снижение доступности сервисов и репутационные издержки.

Следовательно, ключевой принцип — проактивность. Ожидание инцидента как повода для действий в современной цифровой среде недопустимо. Необходимо заранее проверить устойчивость инфраструктуры, сформировать и отработать план реагирования, а также убедиться, что провайдер связи и выбранные средства защиты способны противостоять как сетевым *(L3)*, так и прикладным *(L7)* атакам.

КИБЕРУСТОЙЧИВОСТЬ БЕЗ ИЛЛЮЗИЙ

АВТОР

Аскар Мусаев,

эксперт по непрерывности бизнеса компании «Инфосистемы Джет»

АВТОР

Александр Морковчин,

руководитель отдела развития консалтинга по ИБ компании «Инфосистемы Джет»

- Киберинциденты становятся одной из ключевых причин прерывания бизнес-процессов
- Отсутствие синергии ИТ, ИБ и бизнеса приводит к стихийности в восстановлении инфраструктуры
- Стратегическая киберустойчивость требует системного подхода и участия руководства

ПОЧЕМУ ТОЛЬКО ЗАЩИЩАТЬСЯ УЖЕ НЕДОСТАТОЧНО

В российских компаниях редко можно встретить настоящую синергию между функциями ИБ, ИТ и управления непрерывностью бизнеса. Исторически сложилось так, что кибербезопасность отвечала за предотвращение и обнаружение атак, а ИТ и бизнес в авральном режиме совместно устраняли последствия, если защита не срабатывала.

Именно такой разрыв — отсутствие сквозного процесса реагирования и восстановления — сегодня становится ключевым вызовом для компаний. Масштаб и частота атак, особенно после 2022 года, окончательно изменили подход бизнеса: вместо вопроса «Может ли это произойти с нами?» все чаще звучит другой — «Что мы будем делать, когда это произойдет?». Ответ на последний вопрос зависит не только от успешной работы ИБ- и ИТ-подразделений, но и от наличия зрелых практик управления непрерывностью бизнеса — одного из ключевых элементов киберустойчивости.

Чтобы понять, насколько российские компании готовы к новой реальности, аналитики дирекции информационной безопасности компании «Инфосистемы Джет» провели исследование **«Восстановление как стратегический аспект киберустойчивости бизнеса»**. Его результаты показали, что именно киберинциденты сегодня становятся одной из ключевых причин прерывания деятельности компаний, опережая по воздействию многие традиционные риски. При этом эффективное противодействие таким угрозам невозможно осуществить лишь силами одной функции — требуется координация ИБ, ИТ, управления непрерывностью бизнеса и кризис-менеджмента.

Все новое — хорошо забытое старое

Практики управления непрерывностью бизнеса традиционно становились особенно актуальными во времена глобальных потрясений — природных катастроф, эпидемий и пандемий. Как и любой элемент менеджмента, они эволюционировали под давлением внешних вызовов: технологических, регуляторных, геополитических. В результате многие крупные организации выработали базовую устойчивость к классическим угрозам непрерывности — отказам оборудования и инфраструктуры, сбоям электропитания и связи, недоступности объектов, ошибкам персонала, а также нарушениям в работе подрядчиков и цепочек поставок. Для таких сценариев, как правило, определены зоны ответственности, разработаны планы реагирования и восстановления, а также отработаны на практике ключевые процедуры.

Однако киберинциденты долгое время оставались вне фокуса управления непрерывностью бизнеса. Современные атаки, особенно с использованием программ-шифровальщиков, способны уничтожить не только продуктивные системы, но и резервные копии, что может полностью парализовать бизнес.

Концепция киберустойчивости возникла как ответ на новую реальность. Она предполагает способность организации продолжать функционировать даже в условиях киберинцидента — благодаря подготовке, планированию, эффективному реагированию и последующему восстановлению. В этой модели управление непрерывностью бизнеса становится фундаментом устойчивости, а ИТ-архитектура приобретает свойства антихрупкости — способности не только выдерживать атаки, но и становиться устойчивее после них.

Практика российских компаний: результаты исследования

Исследование компании «Инфосистемы Джет» позволило понять, какую роль сегодня играет управление непрерывностью бизнеса в обеспечении киберустойчивости и насколько существующие практики помогают компаниям сохранять работоспособность в условиях атак.

В большинстве российских компаний управление непрерывностью бизнеса по-прежнему воспринимается как техническая задача, а не проблема, требующая комплексной подготовки к реагированию и восстановлению. Часто ответственность за устойчивость процессов возложена на ИТ-подразделения, участие же службы ИБ и тем более бизнес-руководителей носит эпизодический характер. Такой перекос напрямую сказывается на зрелости практик: планы восстановления существуют, но зачастую не привязаны к реальным бизнес-приоритетам. По данным опроса, лишь около 20% организаций имеют план восстановления, согласованный с бизнесом.

Отсутствие интеграции между ИТ, ИБ и бизнесом приводит к стихийному управлению инцидентами. Формально планы восстановления существуют, и около 70% компаний заявляют, что тестируют их. Однако полноценные сценарные учения с моделированием реальных кризисных ситуаций

проводятся значительно реже. В результате при возникновении серьезного инцидента организация теряет время на координацию действий, определение ролей и принятие решений.

Такой стихийный подход чреват не только технологическими сбоями, но и управленческим кризисом. Когда между функциями управления непрерывностью, ИТ и ИБ нет синергии, а роли и зоны ответственности не определены заранее, бизнес становится уязвимым перед любыми сценариями — от отказа серверов до атак вымогателей. В этих условиях восстановление после инцидента превращается в «героизм на пустом месте», требующий принятия решений на ходу. Наличие заранее выстроенных процессов и согласованных планов во многом позволяет этого избежать.

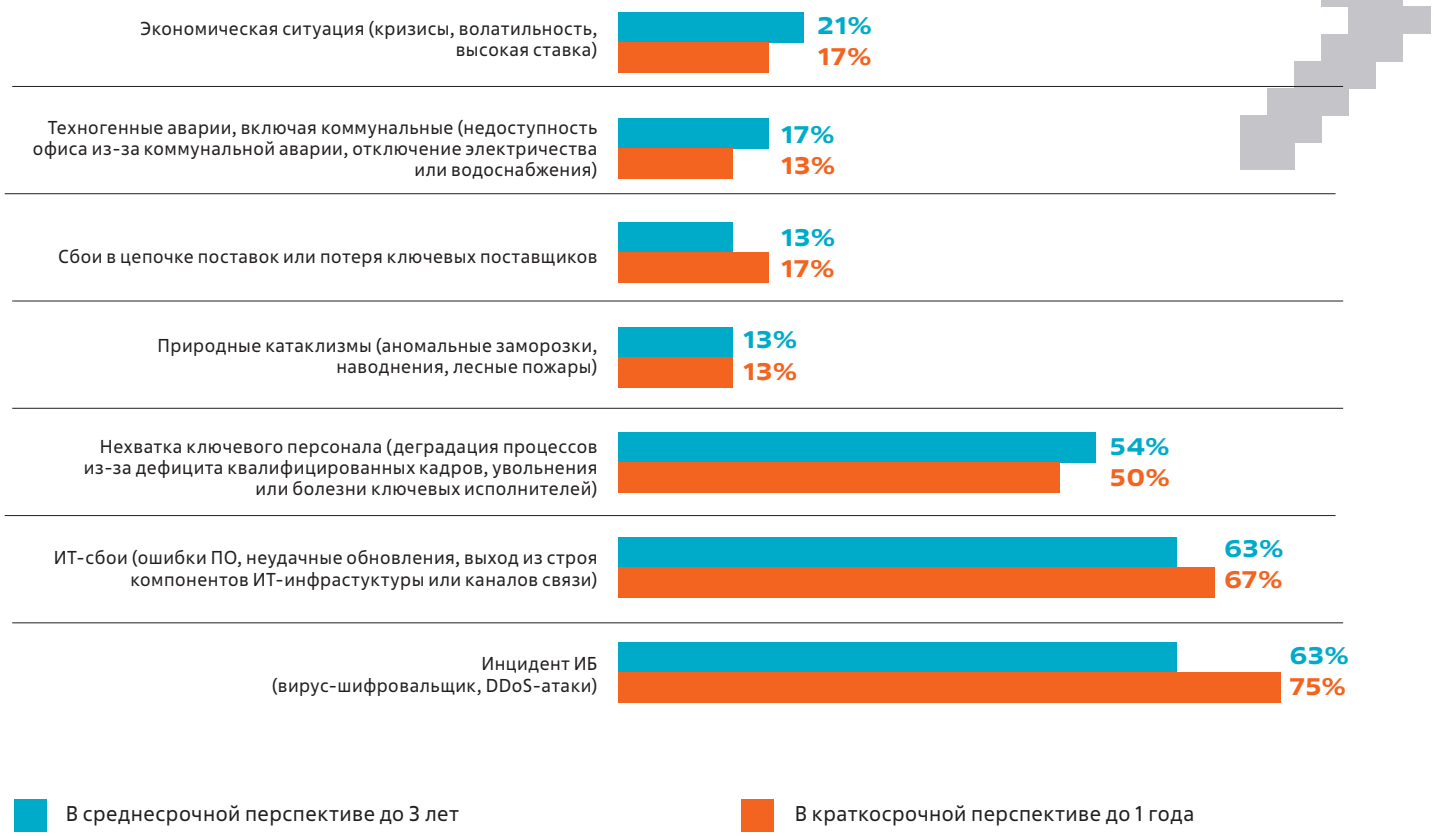
Проблема затрагивает и коммуникации. Только около 40% компаний готовы публично сообщать о киберинцидентах. Для большинства закрытость по-прежнему воспринимается как способ защиты репутации, но на практике такая позиция тормозит развитие отраслевых практик: без обмена реальным опытом рынок лишается возможности коллективного обучения, а сами компании не могут объективно оценить собственную готовность на фоне других.

Поэтому переход к зрелой модели обеспечения непрерывности невозможен без вовлечения бизнеса на стратегическом уровне, регулярных сценарных учений и большей прозрачности. Сегодня российский рынок находится на этапе формирования такого подхода: понимание значимости устойчивости уже сформировано, однако системная управленческая модель пока только вырабатывается.

Вместе с тем отечественные компании уже осознают появление новых существенных рисков для непрерывности бизнеса. Среди них:

- инциденты информационной безопасности;
- масштабные сбои ИТ-инфраструктуры;
- зависимость от отдельных специалистов.

РИСКИ ДЛЯ НЕПРЕРЫВНОСТИ БИЗНЕСА



Как выстраивать непрерывность: четыре ключевых этапа

В исследовании выделены четыре ключевых этапа управления непрерывностью бизнеса в контексте киберустойчивости, выполнение которых помогло бы снизить последствия от реализации ключевых рисков. Рассмотрим каждый из них:

1 **Планирование и подготовка.** Интеграция практик управления непрерывностью бизнеса во все процессы компании, а также вовлеченность руководства — ключевые факторы достижения киберустойчивости. Одним из инструментов для реализации таких требований может служить Business Impact Analysis *(BIA)* — анализ, позволяющий понять, как быстро компания получит непоправимый ущерб, если процессы или ключевые системы остановятся. Это основной инструмент, помогающий сфокусироваться на требованиях бизнеса к киберустойчивости.

2 **Реагирование на инцидент.** Основной задачей для организации является выстраивание эффективного процесса реагирования. Должны быть четко сформулированы критерии, позволяющие определить, при каких обстоятельствах нежелательное событие или потенциальный инцидент кибербезопасности могут перейти в масштабный кризис и потребуется подключение практик кризис-менеджмента. Простой и понятный план кризисного реагирования, включающий стратегию коммуникаций компании, назначение ответственных и определение ролей в управлении кризисом, снизит затраты времени при реагировании и поможет сфокусироваться на инциденте, не отвлекаясь на сопутствующие организационные процессы. Пока лишь пятая часть опрошенных понимают ценность такого подхода:

Есть ли в организации определенная команда реагирования на кризисную ситуацию (выделенные роли/должности, которые участвуют в реагировании)?

59%
Нет, участники реагирования собираются ситуационно в зависимости от инцидента

20%
Да, на уровне всей организации (топ-менеджмент, маркетинг, ИТ, ИБ, HR, бизнес)

21%
Да, внутри подразделения (координаторы в ИТ и/или в ИБ)

Кейс

В одной из компаний частота резервного копирования кадровой системы была определена ИТ-подразделением экспертным путем на основе средней частоты вносимых в систему изменений. При возникновении инцидента с повреждением базы ее восстановили из резервной копии, сделанной несколько дней назад, однако потеря данных оказалась критичной для бизнеса: подходил срок сдачи отчетности, и за эти несколько дней в базу было внесено больше изменений, чем обычно. Бизнес не был вовлечен в определение критичности используемых ресурсов, а ИТ-подразделение не подозревало о пиковых нагрузках в определенное время.

3 **Поддержание ключевых функций.** Основной критерий оценки эффективности практики — зрелость бизнес-процессов компании с точки зрения непрерывности. Необходим периодический анализ воздействия на бизнес *(BIA)*, в рамках которого могут быть изучены и альтернативные варианты функционирования процессов для последующей подготовки планов обеспечения непрерывности. Наличие планов и понимание очередности восстановления в кризисной ситуации повышают шансы компании оставаться киберустойчивой во время инцидента.

Кейс

Определение потенциальных потерь компании от простоя критически важных процессов помогло департаменту ИТ обосновать бюджет на модернизацию системы резервного копирования. Сравнив величину инвестиций для достижения требуемого бизнесом времени восстановления и размер возможного ущерба при существующей системе резервного копирования, руководство приняло решение о модернизации.

4 **Полное восстановление и возврат к норме.** Однако при отсутствии резервных копий, соответствующей инфраструктуры и необходимых специалистов выстроить процессы и сформировать планы будет недостаточно. Комплексные проверки и тестирование как «бумажной» составляющей, так и готовности ИТ-инфраструктуры покажут, насколько компания киберустойчива. При этом важнейшей составляющей гарантированного восстановления после шифрования или уничтожения инфраструктуры является система резервного копирования. Это понимают как злоумышленники, рассматривая резервные копии в качестве одной из приоритетных целей в атаке, так и опрошенные эксперты, считая такие инциденты ИБ ключевым риском для непрерывности именно из-за потенциального масштаба ущерба. Только комбинированные методы защиты помогут сохранить «последнюю милю», но внимания этому уделяется пока недостаточно.

Переход к стратегической киберустойчивости

Несмотря на растущее внимание к вопросам устойчивости, практики обеспечения непрерывности бизнеса в российских компаниях пока не достигли достаточного уровня зрелости. Компании уже осознают неизбежность киберинцидентов и необходимость подготовки к восстановлению, однако реактивный подход остается доминирующим, а интеграция ИТ, ИБ и бизнеса реализована не полностью.

Во многом непрерывность по-прежнему видят как набор технических мер, а не как полноценную дисциплину управления. Это и приводит к разрыву между планами и реальностью: формальные планы есть, но в кризис они не работают. Дополнительный сдерживающий фактор — нежелание компаний делиться информацией о происшествиях, а без открытости рынок лишается коллективной памяти и рост зрелости практик замедляется.

В этих условиях фактором успеха становится переход к стратегической киберустойчивости. Он подразумевает участие руководства, интеграцию ИТ, ИБ и бизнес-процессов, регулярную проверку сценариев и готовность пересматривать планы на основе реального опыта. Такой подход позволит компаниям не просто восстанавливаться после сбоев в авральном режиме, а выстроить устойчивую модель работы, способную выдерживать усиливающееся давление в условиях цифровых рисков и неопределенности.

Защищенность контура резервного копирования*

* Можно было дать несколько вариантов ответа.

АВТОР

Александр Морковчин,

руководитель отдела развития консалтинга по ИБ компании «Инфосистемы Джет»

7 СТРАТЕГИЙ АНТИХРУПКОСТИ

ПРАКТИЧЕСКИЙ ФРЕЙМВОРК: КАК ПЕРЕЖИТЬ КИБЕРАТАКУ И СТАТЬ СИЛЬНЕЕ

В эпоху сложных и целевых кибератак выигрывает не тот, кто надеется, что его не сломают, а тот, кто умеет оперативно обнаружить вторжение, продолжить работать под атакой и быстро восстановиться. В этой статье рассмотрим основные подходы к достижению этих целей.

Без права на восстановление: новая этика хакеров

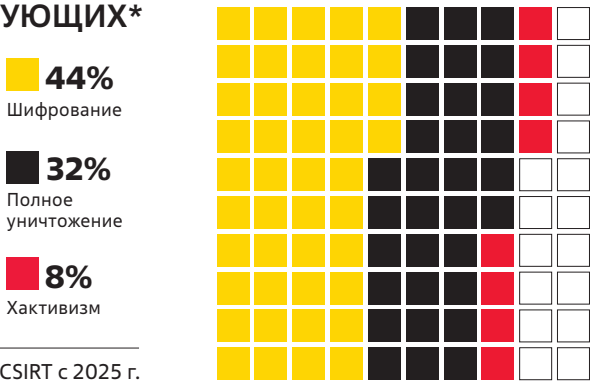
За период с января по конец ноября 2025 года Центр мониторинга и реагирования на инциденты Jet CSIRT зафиксировал более 10 тысяч инцидентов ИБ. И хотя количественные показатели остались на уровне 2024-го, качественная картина угроз претерпела значительные изменения.

Девизом кибератак последних лет стало «совершенствование вместо революции»: постоянное улучшение арсенала, оттачивание методов уклонения от обнаружения, переиспользование инфраструктуры других группировок, широкое применение инструментов ИИ — все это позволило проводить сложные атаки на цепочки поставок и использовать многошаговые схемы заражения ИТ-инфраструктуры.

При этом заметно поменялись мотивы атакующих: по мере роста устойчивости компаний к DDoS-атакам, «обесценивания» дефейсов, усиления геополитической напряженности, хакеры перешли к тактике «выжженной земли». Ключевая цель — остановить бизнес, поэтому 44% киберугроз — это атаки шифровальщиков, а еще 32% связаны с вайперами, которые стремятся полностью уничтожить инфраструктуру.

В условиях эволюции тактики атакующих компрометация инфраструктуры — лишь вопрос времени. Ответом должна стать трансформация защиты — переход от обороны «замка» *(превентивной защиты периметра, до сих пор доминирующей во многих отраслях)* к реализации динамичной, антихрупкой архитектурной модели.

ЦЕЛИ АТАКУЮЩИХ*



44% Шифрование

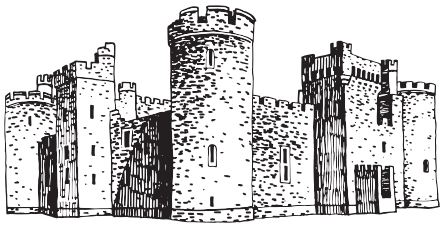
32% Полное уничтожение

8% Хактивизм

* По результатам расследований команды Jet CSIRT с 2025 г.

КАКАЯ АРХИТЕКТУРНАЯ МОДЕЛЬ ЛУЧШЕ ВСЕГО ОПИСЫВАЕТ ВАШ ПОДХОД К ЗАЩИТЕ В КОМПАНИИ **

	2023	2024	2025
Замок и ров (Castle and moat)	46%	49%	30%
Эшелонированная оборона (Defense in Depth)	52%	51%	70%
Нулевое доверие (Zero Trust)	2%	0%	0%



Побеждает не тот, кто не падает, а тот, кто быстрее встает

Клиенты, регулирующие органы и акционеры ожидают от бизнеса способности переживать любой кризис. Кому-то везет больше — и он отделывается легким испугом, а кто-то на недели прекращает операционную деятельность. Поэтому умение обнаруживать атаки, нивелировать их последствия и оперативно восстанавливаться после них становится куда более важным, чем реализация просто защиты. Такая выживаемость компании в любой кризис получила название «киберустойчивость».

Необходимость обеспечения киберустойчивости обусловлена сочетанием неизбежных киберугроз, сложных цифровых зависимостей, высокой стоимости простоя, ожиданий заинтересованных сторон и требований регулирующих органов

В России начали говорить о киберустойчивости еще в 2017 году, и с тех пор проблема только обострилась. Необходимость в превентивных мерах никуда не исчезла — возникла потребность в их качественном дополнении. Так, Банк России выпустил директивы по операционной надежности, а на международном уровне появились лучшие практики, посвященные киберустойчивости: Индекс киберустойчивости от Всемирного экономического форума *(WEF)*, Обзор киберустойчивости *(Cyber Resilience Review, CRR)* от Министерства внутренней безопасности США *(DHS)*, Фреймворк кибероценки *(Cyber Assessment Framework, CAF)* от Национального центра кибербезопасности Великобритании *(NCSC)*.

Киберустойчивость — комплексная дисциплина, выходящая за рамки классической кибербезопасности. Она объединяет планирование непрерывности бизнеса *(BCM)*, аварийное восстановление *(DR)*, защиту информации и антикризисное управление. Таким образом, базовым условием устойчивости является конвергенция трех функций: **ИТ, ИБ и ВСМ** — в единый процесс управления.

Сейчас на российском рынке такая синергия практически не встречается. Причин здесь несколько:

- ИТ и ИБ редко «дружат семьями», поэтому реальная операционная готовность к инцидентам у большинства российских компаний остается низкой. За практики непрерывности чаще отвечает ИТ-департамент, в область интересов которого входят инфраструктурные сервисы и бизнес-системы, а не бизнес-процессы в целом.
- Российские фреймворки по киберустойчивости практически отсутствуют. На международной арене киберустойчивые практики «разбросаны» по различным стандартам и требуют адаптации под специфику и опыт российского ИБ-рынка.

На практике киберустойчивость означает не внедрение супертехнологий, а реализацию разумных стратегий с фокусированием на проблемных сферах. Мы решили собрать такие киберустойчивые стратегии, переосмыслить их и адаптировать к российским реалиям. Итогом нашей работы стал фреймворк «Антихрупкая ИТ-архитектура».

** Результаты исследования аналитической команды «Инфосистемы Джет» за три года наблюдений среди более чем 250 респондентов — руководителей служб ИБ.

Антихрупкая ИТ-архитектура нацелена не просто на защиту и восстановление инфраструктуры, а на ее укрепление после атаки/инцидента. Это уже не просто наложенная ИБ, а архитектура бизнеса, способная выживать и становиться сильнее после ударов

Подход к антихрупкости как готовность к появлению «черных лебедей»

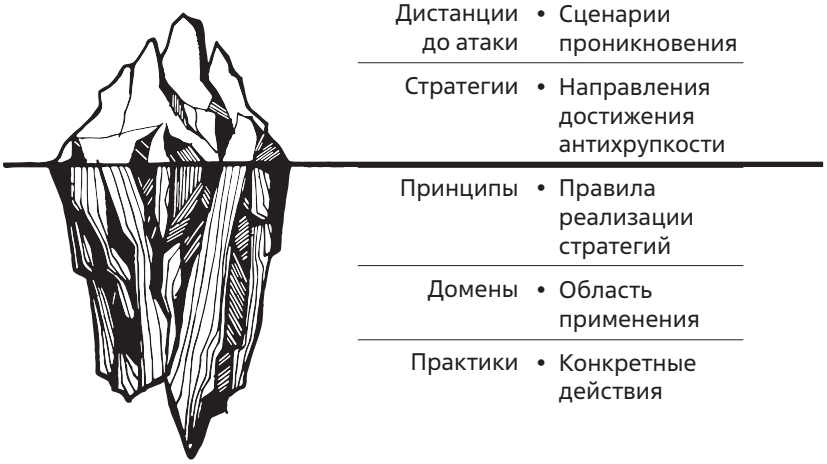
Хорошо применимая к ИТ-сфере концепция «черного лебедя», описанная Нассимом Талебом в одноименном бестселлере 2007 года, легла в основу фреймворка «Антихрупкая ИТ-архитектура».

Чтобы дать сообществу открытый и практичный инструмент, мы объединили опыт инженеров, аудиторов, консультантов и наших экспертов-практиков по защите сети и построению ИТ-инфраструктуры. Ежегодно мы выполняем сотни проектов, помогая бизнесу выстраивать кибербезопасность, тестировать устойчивость и восстанавливаться после атаки.

Сценарии использования фреймворка отражают основные потребности рынка:

- оценка: единый инструмент — «линейка» зрелости для сравнения с конкурентами и отраслевыми лидерами;
- планирование: каталог проверенных практик для выбора вектора развития;
- трансформация: поэтапная методика наращивания киберустойчивости от текущего состояния к целевому.

Чтобы сохранять общее видение *(«в крупную клетку»)* и при этом гибко реагировать на изменения, мы построили фреймворк по каскадной модели — от общего к частному. Такой подход позволяет перейти **от стратегий к тактике**:



Четыре дистанции до атаки

В условиях постоянных атак высока вероятность того, что развитие инцидента пойдет по неожиданному сценарию, поэтому требуется совсем иначе расставлять акценты в организации защиты. И если посмотреть на обеспечение киберустойчивости как на непрерывный цикл, определяющийся временем до, во время и после атаки, можно выделить четыре ключевые «дистанции».

ПОДГОТОВКА К ВТОРЖЕНИЮ

Важны регулярные проверки, обучение, инвестиции в ИБ и прогнозирование рисков: оценка возможного ущерба, анализ угроз и потенциальных противников.

СЛЕВА ОТ ВТОРЖЕНИЯ

Атака близка. В ход идут вовлечение злоумышленника, активная защита и сдерживание. Цель — выявить нарушителя, остановить его или замедлить.

СПРАВА ОТ ВТОРЖЕНИЯ

Атака уже произошла. На первый план выходят обнаружение, реагирование и восстановление. Все сценарии должны быть продуманы заранее, включая план Б на случай катастрофы.

ПОСЛЕ ВТОРЖЕНИЯ

Глубокий анализ произошедшего, а также пересмотр политик и архитектуры безопасности по его результатам. Именно здесь формируется новая, более сильная «иммунная система» организации.

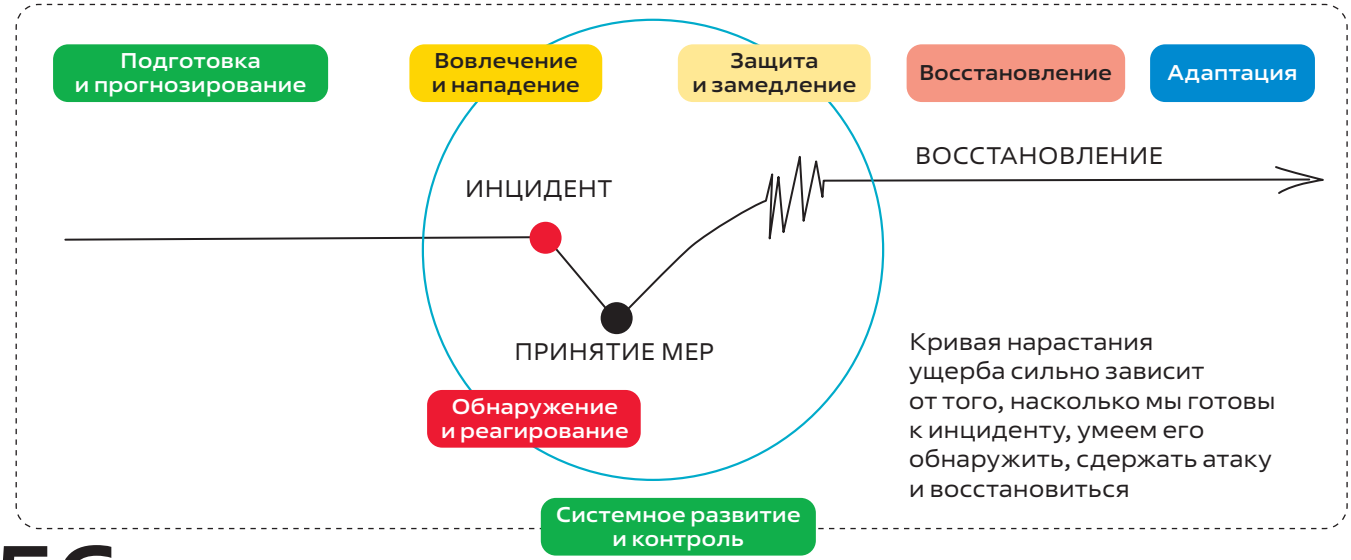
Семь стратегий и десять принципов антихрупкости

Устойчивость — это потенциал, который необходимо постоянно поддерживать и укреплять. Накопить его позволяют семь стратегий антихрупкости, составляющие каркас фреймворка:

1. системное развитие и контроль;
2. подготовка и прогнозирование;
3. вовлечение и нападение;
4. защита, замедление и сдерживание;
5. обнаружение и реагирование;
6. восстановление;
7. адаптация и перестройка.

Эти стратегии помогают подготовиться, эффективно предотвратить или замедлить действия атакующего, вовремя среагировать на них и восстановиться, если все пошло не по плану. Каждая из них эффективна на той или иной фазе реализации инцидента.

Правильно комбинируя эти стратегии, мы можем добиться эффективности — предотвратить или уменьшить ущерб, обеспечив операционную устойчивость. И в случае инцидента восстановиться не за неделю, а за дни или часы.



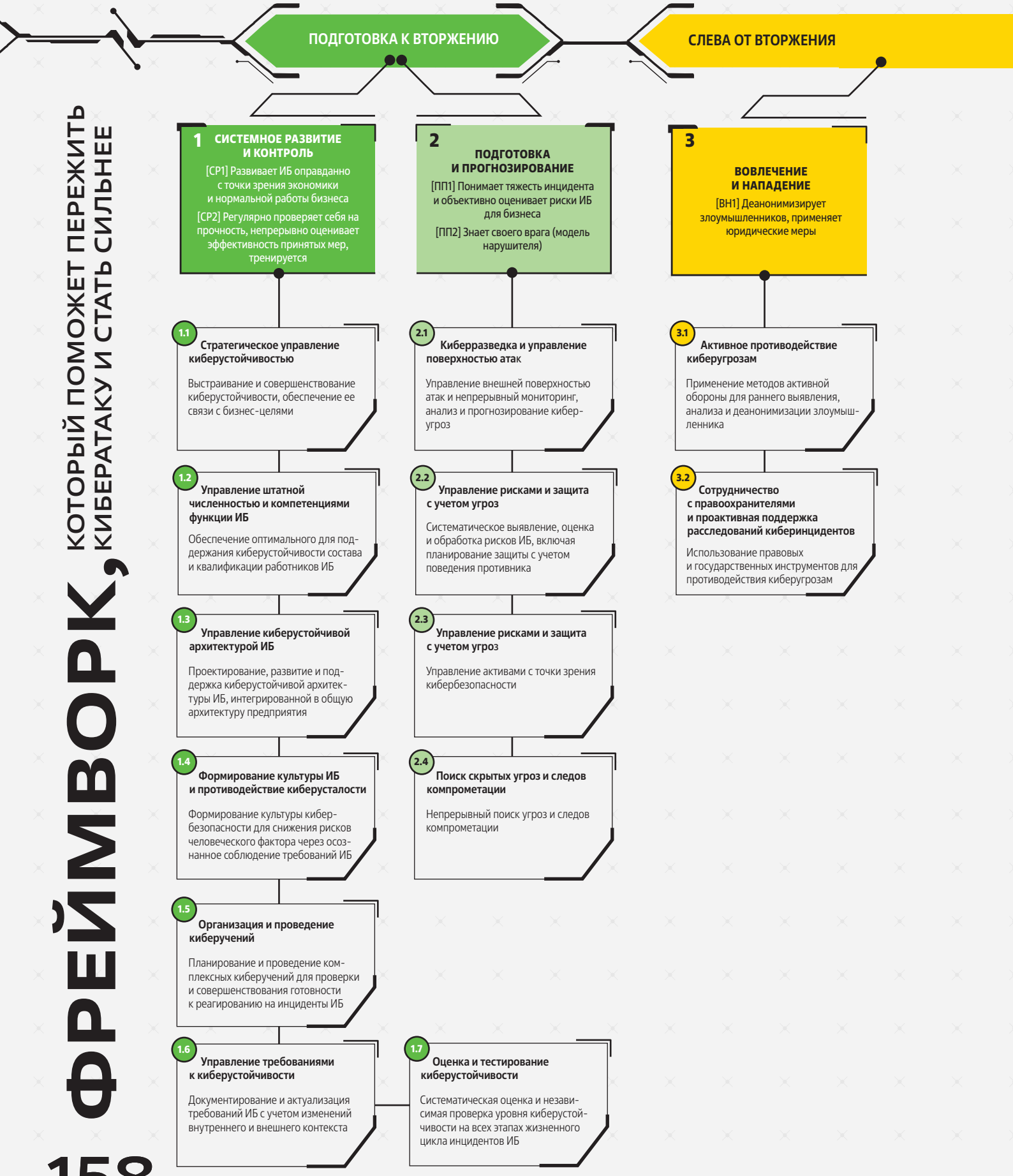
Чтобы раскрыть, как реализуется та или иная стратегия на практике, мы сформировали 10 принципов киберустойчивости.

Домены и практики

В текущей версии фреймворка представлены 33 домена и почти 400 различных практик. Это не только практики кибербезопасности, но и экспертиза по таким вопросам, как:

- управление надежностью;
- планирование и поддержка кризисных процессов;
- управление репутационными рисками в условиях киберинцидента;
- управление видимостью цифрового ландшафта;
- безопасность систем искусственного интеллекта;
- управление киберустойчивой архитектурой ИБ;
- и многие другие подходы для обеспечения антихрупкости ИТ-архитектуры.

ФРЕЙМВОРК, КОТОРЫЙ ПОМОЖЕТ ПЕРЕЖИТЬ КИБЕРАТАКУ И СТАТЬ СИЛЬНЕЕ



СЛЕВА ОТ ВТОРЖЕНИЯ

СПРАВА ОТ ВТОРЖЕНИЯ

ПОСЛЕ ВТОРЖЕНИЯ

4 ЗАЩИТА, ЗАМЕДЛЕНИЕ, СДЕРЖИВАНИЕ

[331] Внедряет изменения в ИТ- и бизнес-процессы для достижения целей киберустойчивости

[332] Поддерживает киберустойчивое состояние непрерывно

5 ОБНАРУЖЕНИЕ И РЕАГИРОВАНИЕ

[OP1] Знает, как действовать на каждом этапе атаки, и имеет средства для этого

6 ВОССТАНОВЛЕНИЕ

[B1] Имеет план Б на случай катастрофического развития событий

7 АДАПТАЦИЯ И ПЕРЕСТРОЙКА

[АП3] Готов меняться в процессе достижения киберустойчивости и оперативно адаптировать свою работу в процессе отражения атак

4.1 Управление сетевой безопасностью

Обеспечение безопасности сети для минимизации поверхности атаки и сохранения доступности сервисов

4.2 Контроль привилегированного доступа и безопасное администрирование

Обеспечение безопасного жизненного цикла привилегированных учетных записей и административных сессий

4.3 Управление доступом по модели нулевого довери

Построение и поддержание системы управления доступом, основанной на принципах нулевого доверия

4.4 Непрерывная работа с уязвимостями

Обнаружение, оценка, приоритизация и устранение уязвимостей в ИТ-ландшафте на всех этапах их жизненного цикла

4.5 Защита ИТ-активов

Обеспечение киберустойчивости ИТ-активов на всех этапах их жизненного цикла

4.6 Управление рисками третьих сторон

Выявление, оценка и контроль рисков внешних поставщиков для обеспечения безопасности и устойчивости процессов

4.7 Защита данных на всех этапах жизненного цикла

Обеспечение безопасности данных на всех этапах их жизненного цикла

4.8 Контроль эксфильтрации данных

Контроль каналов передачи информации, определение легитимных способов обмена и применение средств защиты для контроля за утечками

4.9 Обеспечение безопасной разработки и защиты приложений

Выполнение требований и принятие мер обеспечения киберустойчивости на всех этапах жизненного цикла ПО

4.10 Безопасность систем искусственного интеллекта

Управление рисками кибербезопасности при разработке, внедрении и эксплуатации ИИ-систем, включая защиту данных, моделей, алгоритмов и инфраструктуры на всех этапах

5.1 Проактивное управление инцидентами кибербезопасности

Своевременное обнаружение и эффективная обрабатывание инцидентов кибербезопасности за счет политик, процедур и инструментов реагирования

5.2 Управление кризисным реагированием на инциденты кибербезопасности

Оперативная координация и нейтрализация критических инцидентов ИБ путем мобилизации ресурсов и принятия решений в условиях неопределенности

5.3 Управление данными о киберугрозах

Управление информацией о киберугрозах, включая ее интеграцию в процессы мониторинга и реагирования на киберинциденты

5.4 Управление репутационными рисками в условиях киберинцидента

Минимизация репутационных потерь через антикризисные коммуникации, мониторинг инфополя и координацию с заинтересованными сторонами

6.1 Резервное копирование в архитектуре киберустойчивости

Интеграция резервного копирования в архитектуру киберустойчивости для оперативного восстановления бизнес-процессов

6.2 Планирование и поддержка кризисных процессов

Реагирование на кризисы с обеспечением непрерывности критических процессов и восстановления функционирования

6.3 Управление жизнестойкостью

Гарантия восстановления критически важных бизнес-функций в согласованное время

6.4 Управление надежностью

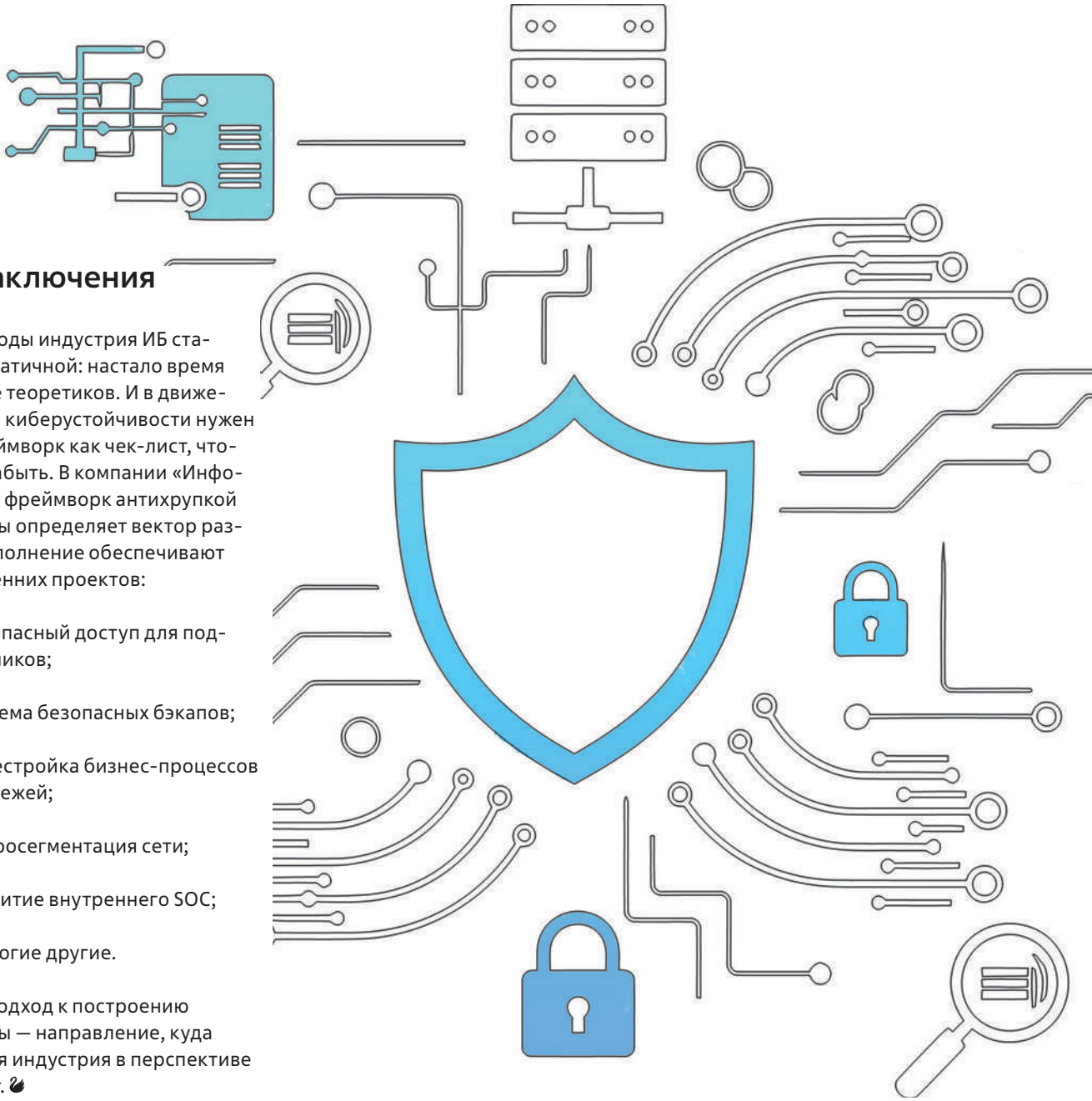
Обеспечение стабильности критичных ИТ-сервисов и инфраструктуры за счет отказоустойчивых решений

7.1 Непрерывное улучшение и оценка эффективности ИБ

Повышение уровня киберустойчивости за счет системного измерения показателей, анализа результатов и внедрения улучшений

7.2 Управление автоматизацией процессов ИБ

Внедрение автоматизации для повышения эффективности процессов кибербезопасности



Вместо заключения

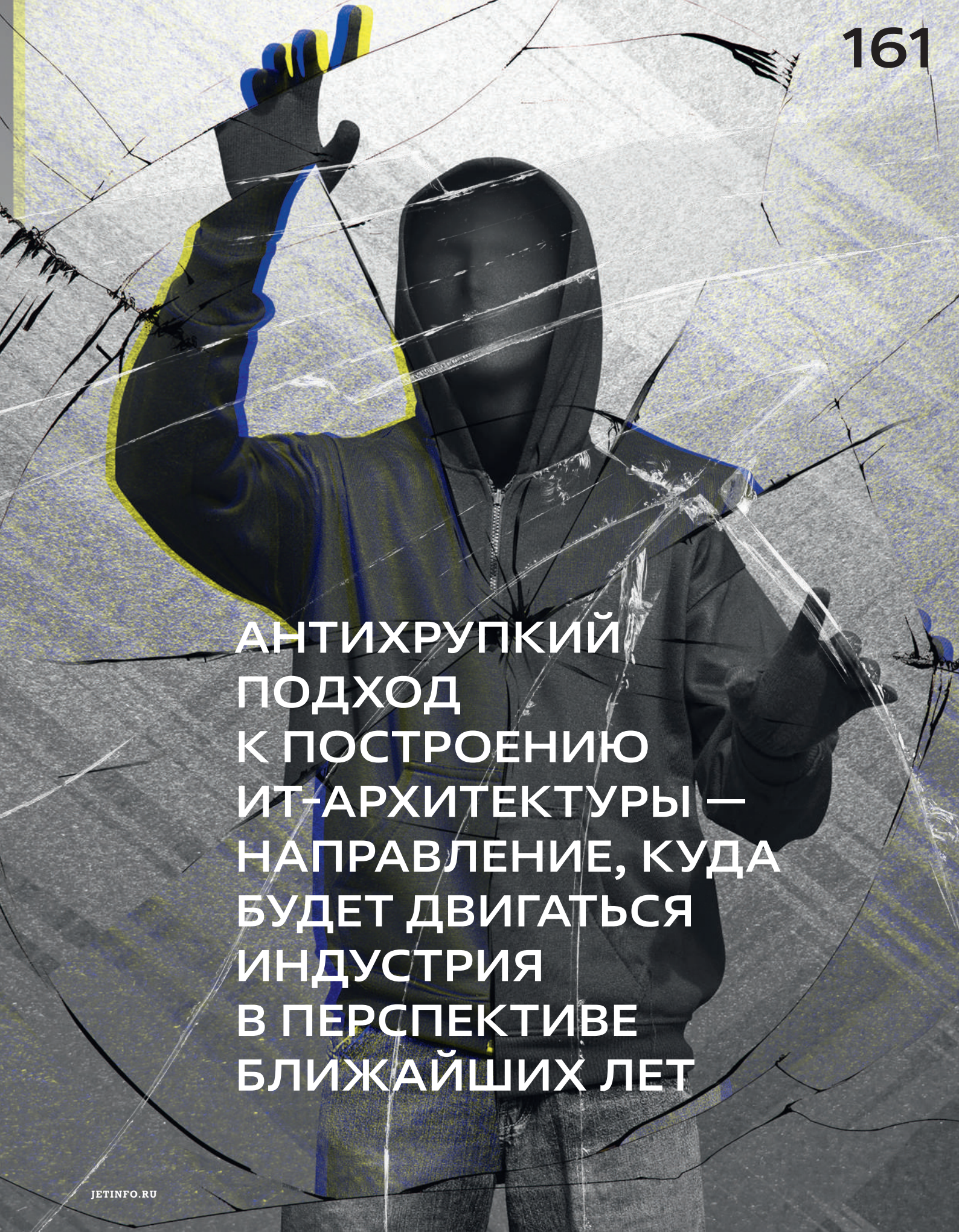
За последние годы индустрия ИБ стала более прагматичной: настало время практиков, а не теоретиков. И в движении к реальной киберустойчивости нужен надежный фреймворк как чек-лист, чтобы ничего не забыть. В компании «Инфосистемы Джет» фреймворк антихрупкой ИТ-архитектуры определяет вектор развития, а его наполнение обеспечивают десятки внутренних проектов:

- безопасный доступ для подрядчиков;
- система безопасных бэкапов;
- перестройка бизнес-процессов платежей;
- микросегментация сети;
- развитие внутреннего SOC;
- и многие другие.

Антихрупкий подход к построению ИТ-архитектуры — направление, куда будет двигаться индустрия в перспективе ближайших лет.

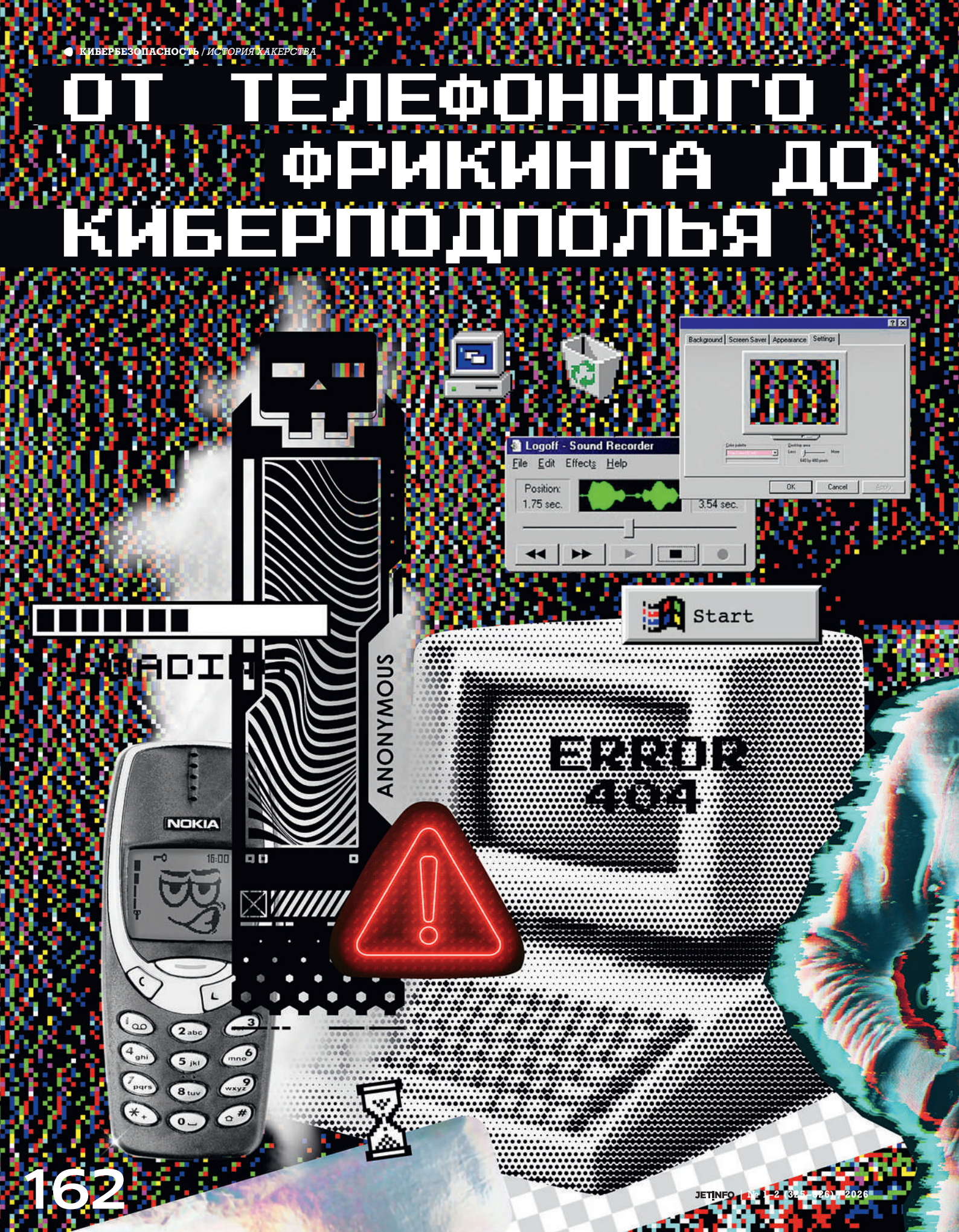
В наших планах — активное развитие фреймворка: адаптация практик под отраслевую специфику, добавление критериев успешности и ситуационных сценариев использования фреймворка. Он будет опубликован в ближайшее время. Ознакомиться с фреймворком и стать его рецензентом можно, написав его автору →

Telegram-канал «Секьюрно»



АНТИХРУПКИЙ ПОДХОД К ПОСТРОЕНИЮ ИТ-АРХИТЕКТУРЫ — НАПРАВЛЕНИЕ, КУДА БУДЕТ ДВИГАТЬСЯ ИНДУСТРИЯ В ПЕРСПЕКТИВЕ БЛИЖАЙШИХ ЛЕТ

ОТ ТЕЛЕФОННОГО ФРИКИНГА ДО КИБЕРПОДПОЛЬЯ



ИСТОРИЯ ХАКЕРСТВА

Слово «хакер» уже давно ассоциируется с кибератаками, утечками данных и цифровыми угрозами, но изначально под этим термином подразумевалось совсем другое. Хакерство началось с исследований в университетских подвалах и взломов телефонных сетей как форма инженерного эксперимента и интеллектуального вызова, и, прежде чем стать инструментом преступлений и кибервойн, оно было культурой — с собственными ценностями, этикой и героями.

Парадоксально, но именно хакерство стало одним из ключевых факторов, сделавших цифровой мир антихрупким. Любая система стремится к устойчивости, но настоящую жизнеспособность она приобретает только тогда, когда сталкивается с попытками взлома, обхода и эксплуатации. Каждая обнаруженная уязвимость, каждый успешный или неудачный взлом — это стресс-тест, который выявляет слабые места и заставляет инфраструктуру эволюционировать. Многие базовые механизмы современной кибербезопасности — от систем аутентификации до багбаунти-программ — появились именно потому, что кто-то попытался их обойти.

В этом смысле история хакерства — это не только про угрозы, но и про усиление систем через давление. Хакеры выступали в роли непреднамеренных архитекторов устойчивости: их действия заставляли компании, государства и разработчиков переосмысливать безопасность и строить более надежную цифровую среду.

Как это сообщество сформировало цифровой мир задолго до появления массового интернета и почему именно противостояние стало двигателем развития, рассказываем в материале.

Хакерство как эксперимент: от телефонных сетей к первым цифровым системам

В 1970-е хакерство не было связано с интернетом. Одними из самых ранних взломщиков были так называемые phone phreaks ***(телефонные фрикеры)*** — энтузиасты, изучавшие работу аналоговых телефонных систем и искавшие способы управлять ими с помощью звуковых сигналов. Изначально фрикинг не воспринимался как что-то криминальное: для многих он был интеллектуальным вызовом и техническим исследованием. Но эксперименты с бесплатными звонками и вмешательством в работу АТС быстро привлекли внимание регуляторов, а затем и полиции. Это стало первым тревожным звонком: грань между исследованием и нарушением правил оказалась крайне тонка.

Параллельно формировалась и академическая культура хакерства, ярче всего — в Массачусетском технологическом институте ***(MIT)***. В 1970–1990-е годы понятие

«хакер» в MIT переосмыслилось: так стали называть человека, который досконально разбирается в системе и способен улучшить ее изнутри. Студенты и исследователи MIT экспериментировали с мейнфреймами, ПО и ранними сетями, создавая решения, опережающие время. Культовые кейсы того периода — несанкционированные доступы к вычислительным ресурсам и нестандартные инженерные «розыгрыши», заложившие основы хакерской этики. Сформировались принципы: свободный доступ к информации, приоритет знаний над формальными ограничениями и уважение к техническому мастерству.

Один из известных эпизодов 60-х связан с клубом Tech Model Railroad Club ***(TMRC)*** в MIT. Участники этого студенческого кружка управляли электромеханическими моделями железных дорог, а с появлением компьютера PDP-1 переключились на эксперименты с программированием. В результате из шутливых исследований появилась игра Spacewar! — один из первых продуктов интерактивного программного обеспечения, созданного не по заказу, а «для души». Это не был взлом в прямом смысле, но именно spirit of hacking — стремление исследовать без разрешения — привел к появлению новаторского продукта.

В 1970–1980-е философию открытости подхватила лаборатория искусственного интеллекта MIT AI Lab, где разработали операционную систему ITS ***(Incompatible Timesharing System)***. В ней намеренно не использовали привычные пароли: считалось, что компетентные пользователи должны иметь возможность свободно изучать и улучшать код. Такой радикальный подход отражал идеалы хакерской культуры, ориентированной на открытость и сотрудничество. Однако со временем даже в академической среде эта концепция вступила в противоречие с требованиями безопасности и коммерциализации ИТ.

Массовый интернет и первые кибергруппы

К концу 1990-х хакерская культура начала стремительно меняться. Компьютеры получили широкое распространение, глобальные сети стали доступны повсеместно — и хакерство вышло за пределы университетов. То, что ранее было уделом узкого круга энтузиастов, оказалось доступно широкой аудитории. В этот период исследования окончательно перестали быть основным занятием хакера — на смену романтике экспериментов пришла практика преступлений.

Первые организованные хакерские группы начали формироваться в 1980–1990-х. Так, в Бостоне появилась культовая группа Cult of the Dead Cow ***(cDc)***, сочетавшая технические эксперименты с дерзкими социально-политическими манифестами. Параллельно там же действовала группа L0pht, ориентированная на глубокий анализ безопасности коммерческих и государственных систем. В отличие от радикальных сообществ, L0pht стремилась выстроить диалог с индустрией. Показательный момент: в 1998 году участники L0pht в публичном докладе заявили, что способны вывести из строя значительную часть интернета менее чем за полчаса. Этот эпизод стал поворотным: хакеров впервые начали воспринимать не как маргинальных хулиганов, а как экспертов, чьи знания требуют внимания на государственном уровне.

Эволюция хакерства в сторону профессиональных киберпреступных сетей началась в 2000-е. Киберпространство стало экономически привлекательным: бурно росли электронная коммерция, онлайн-банкинг, цифровые сервисы. На смену одиночкам-энтузиастам пришли организованные преступные группы. Современные хакерские группировки уже не ограничиваются разовыми взломами — они строят целые экосистемы. В этих «теневых компаниях» есть разработчики вредоносного ПО, операторы ботнетов, специалисты по отмыванию денег и посредники, продающие доступ к взломанным системам. По сути, выстроилась цепочка киберпреступлений: от создания вируса до монетизации украденного, — в которой задействованы разные «отделы» преступного бизнеса.

Герой, злодей или специалист?

Логическим продолжением этой трансформации стало расслоение самого понятия «хакер». К началу 2010-х термин окончательно утратил однозначность. С одной стороны, в массовом сознании закрепился образ киберпреступника — человека, зарабатывающего на уязвимостях и взломах. С другой — внутри индустрии сформировалось профессиональное сообщество специалистов по информационной безопасности, для которых термин «хакер» снова стал обозначать эксперта, а не злоумышленника. Так появились устойчивые категории white hat, black hat и gray hat, отражающие не столько технический уровень, сколько мотивацию и этические рамки деятельности.

Исторически это стало попыткой вернуть хакерству легитимность. Компании начали нанимать бывших «подпольщиков», запускать багбаунти-программы и публично признавать ценность независимых исследователей. Многие ключевые практики современной кибербезопасности выросли именно из хакерской культуры 1970–1980-х годов с принципами свободного обмена знаниями, peer-review-кода и публичного обсуждения уязвимостей. В этом смысле история хакерства не сводится к криминалу — это эволюция отношений между технологией, обществом и контролем.

Миф о хакере формировался параллельно с реальными процессами — во многом благодаря массовой культуре. Кино и телевидение сыграли ключевую роль в популяризации и романтизации этого образа, часто упрощая или искажая техническую сторону, но точно улавливая дух эпохи. Благодаря экрану хакер превратился в символ одиночки, бросающего вызов системе, в наследника тех самых студентов MIT, только в более зрелищной упаковке.

История хакерства не сводится к криминалу — это эволюция отношений между технологией, обществом и контролем

Полное погружение: 5 ключевых фильмов и сериалов о хакерах

«Военные игры» ***(WarGames, 1983)***

Один из первых фильмов, познакомивших широкую аудиторию с компьютерными взломами. Школьник Дэвид Лайтман с помощью War dialing — автоматического перебора телефонных номеров модемом — случайно подключается к военному суперкомпьютеру WOPR. Он обходит систему аутентификации и попадает в интерфейс стратегического моделирования, принимая его за игру. Запущенный им сценарий симуляции ядерной войны воспринимается системой как реальная угроза. Фильм показал один из первых сценариев удаленного несанкционированного доступа к критической инфраструктуре через уязвимости сети.

«Хакеры» ***(Hackers, 1995)***

Культовая лента 90-х, превратившая хакерство в элемент молодежной контркультуры. Главный герой Дэйд Мёрфи, известный как Zero Cool, вместе с другими хакерами проникает во внутреннюю сеть корпорации Ellingson Mineral. Используя подбор паролей, социальную инженерию и исследование файловой системы, они обнаруживают вредоносный код, внедренный системным администратором. Сюжет строится вокруг реальных принципов хакерства — получения доступа через слабые места защиты и постепенного изучения архитектуры системы.

«Матрица» ***(The Matrix, 1999)***

Томас Андерсон — программист, который ведет двойную жизнь. Под псевдонимом Neo он занимается взломом защищенных систем, использует нелегальное ПО и взаимодействует с подпольным хакерским сообществом. Через специальную защищенную сеть с ним связывается Морфеус, который помогает ему понять, что окружающий мир — это искусственная система ***(матрица)***. Дальнейший сюжет развивает ключевой принцип хакерства: любую систему можно исследовать и обойти, если понять, как она устроена. Внутри матрицы Neo и другие персонажи фактически действуют как хакеры — получают доступ к системе, обходят ее ограничения и изменяют правила среды.

«Социальная сеть» ***(The Social Network, 2010)***

Фильм показывает другую сторону хакерской культуры — переход от взлома к созданию систем. В одной из ключевых сцен Марк Цукерберг пишет программу Facemash, применяя скрипты для автоматического сбора фотографий студенток из закрытых университетских баз данных. Фильм показывает хакерство как способность анализировать и использовать архитектуру системы — навык, который позже станет основой создания Facebook*.

«Мистер Робот» ***(Mr. Robot, 2015–2019)***

Эллиот Алдерсон — специалист по ИБ, который использует реальные методы взлома: социальную инженерию, фишинг, вредоносное ПО и эксплуатацию уязвимостей. Его атаки строятся на сборе информации о целях и поиске точек входа в корпоративные сети. Сериал показывает хакерство как системный процесс анализа, получения доступа и установки контроля над инфраструктурой.

Антихрупкость цифрового мира: почему хакеры делают системы сильнее

История хакерства — это история постоянного противостояния: создание и разрушение, контроль и свобода, безопасность и уязвимость. Хакеры выявляли слабости систем задолго до того, как индустрия научилась воспринимать безопасность как фундаментальный элемент архитектуры. Их действия заставляли разработчиков усиливать защиту, компании — пересматривать подход к инфраструктуре, а государства — формировать новые принципы регулирования цифровой среды.

В этом и проявляется антихрупкость цифрового мира: каждая атака, каждый взлом и каждая обнаруженная уязвимость не только наносят ущерб, но и служат точкой роста. Системы, пережившие взлом, становятся сильнее благодаря новым механизмам защиты, лучшему пониманию рисков и более зрелым практикам безопасности, а современная кибербезопасность во многом выросла не вопреки хакерам, а благодаря им.

Сегодня хакер уже не просто подпольный злоумышленник или герой кино. Это исследователь, инженер и специалист по безопасности, который выявляет слабые места и тем самым способствует развитию цифровой среды. И чем сложнее становятся технологии, тем важнее этот парадокс: устойчивость цифрового мира обеспечивается не отсутствием угроз, а способностью адаптироваться к ним.

* Соцсеть запрещена в РФ, принадлежит Meta, признанной в стране экстремистской.

ТЫ МОЙ СВЕТ

(но я тебе не верю)

КАК ИСПОЛЬЗОВАТЬ ИИ В КОМПАНИИ, ЧТОБЫ ОЧАРОВАНИЕ НЕ СТАЛО РАЗОЧАРОВАНИЕМ

Многие крупные компании используют генеративный ИИ в закрытом контуре, чтобы предотвратить утечку данных

Галлюцинации нейросетей в ряде случаев оборачиваются убытками и скандалами

Вайб-кодинг ускоряет разработку приложений, и его уже используют крупные российские компании

Промышленные роботы автоматизируют производство, системы компьютерного зрения ищут заводской брак, беспилотные грузовики развозят между российскими городами товары, а их стоимость в магазинах устанавливают программы анализа цен. Искусственный интеллект проник во все бизнес-процессы в разном обличье. В том числе в виде умных помощников, к которым мы обращаемся при решении многих задач. Благодаря умению создавать тексты, аудио, изображения и код, а также делать выводы, давать подсказки и выдвигать идеи, популярные нейросети быстро стали не только нашими личными, но и рабочими инструментами. С одной стороны, возможности генеративного ИИ обещают сотрудникам компаний и самим работодателям огромные перспективы, но с другой — несут в себе много угроз. О том, как воспользоваться преимуществами технологии с минимальными рисками, — в нашей статье.

Больше возможностей — больше рисков

Инвестируя в искусственный интеллект, корпорации ожидают значительного коммерческого эффекта от его использования. Дарио Амодеи, глава Anthropic, прогнозирует годовой прирост мирового ВВП на 5–10% за счет ИИ. Но уточняет, что у вклада ИИ в мировую экономику есть обратная сторона — возможное повышение уровня безработицы до 10%. Это связано с тем, что технологии, с одной стороны, увеличивают производительность труда, а с другой — отнимают рабочие места у специалистов. К примеру, генеральный директор IBM Арвинд Кришна считает, что с 2023 по 2028 год ИИ может заменить в компании порядка 7,8 тыс. сотрудников бэк-офиса.

Там, где есть большие возможности, всегда присутствуют значимые риски. Причем говорить о них начали сами разработчики, в числе которых настоящие звезды технологического сообщества — Илон Маск и сооснователь Apple Стив Возняк. В марте 2023 года в числе большой группы ИТ-экспертов они выступили с призывом приостановить работы по развитию мощных моделей ИИ. Разработчики высказали опасение, что прогресс в этой сфере приведет к потере контроля над технологиями, а следовательно, к непредсказуемым последствиям, распространению фейков и пропаганды, а также к излишней автоматизации рабочих мест. Впрочем, тот же Маск не стал упускать возможностей и уже в следующем месяце основал собственную компанию по ИИ-разработке — xAI. Стартап вскоре выпустил нейросеть Grok и одноименное семейство больших языковых моделей, на которых она построена.

Однако к эффективности ИИ возникают вопросы. Так, по данным компании

Visier, в 2025 году организации по всему миру начали активно возвращать сотрудников, уволенных из-за замены их функций нейросетями. Уже 5,3% таких специалистов вернулись на свои рабочие места, а более половины работодателей жалеют о поспешном расставании с персоналом из-за ИИ. Причем это исследование вполне репрезентативное: в нем приняли участие 2,4 млн сотрудников из 142 стран.

В то же время ИИ-оптимизация все чаще становится для компаний удобным оправданием сокращений персонала, вызванных совсем другими причинами — например, такими как финансовые трудности и чрезмерно раздутый штат. Согласно данным исследования компании Challenger, Gray & Christmas, в прошлом году с внедрением ИИ было связано более 50 тыс. увольнений сотрудников. Однако в отчете аналитиков Forrester в начале 2026 года отмечается: далеко не все работодатели, назвавшие ИИ причиной увольнений, в настоящее время располагают настолько зрелыми ИИ-решениями, чтобы отказаться от услуг специалистов.

Между тем в 2025 году мировой рынок генеративного искусственного интеллекта оценивался в 53,7 млрд долл. и в ближайшее десятилетие продолжит расти в среднем на 31,6% ежегодно. По прогнозам Global Market Insights, к 2035-му он достигнет 988,4 млрд долл. И этот взлет во многом будет поддержан интенсивным внедрением ИИ-сервисов в компаниях для решения широкого круга задач.

Стоит ли доверять данные ИИ

Так в чем же риски использования искусственного интеллекта? Сотрудники дают умным помощникам разные поручения: создать и улучшить презентации, подготовить коммерческие предложения, сделать прогнозы, проверить свою работу и исправить возможные ошибки. Однако для повышения качества подготавливаемых материалов зачастую необходимо предоставлять ИИ доступ к внутренним документам компании ***(в том числе конфиденциальным)*** — и сотрудники это делают.

Так, согласно результатам исследования Harmonic Security, работники чаще всего передают нейросетям:

- клиентские данные;
- информацию о сотрудниках компании;
- юридические документы;
- финансовые показатели;
- данные для авторизации пользователей;
- конфиденциальный программный код.

В 2026 году 57% сотрудников применяют для работы публичные нейросети без одобрения ИТ-отдела, а треть из них загружают в них конфиденциальную информацию, показал опрос Gartner. К слову, на удочку попадаются даже специалисты по ИБ. В прошлом году, например, и. о. руководителя Агентства кибербезопасности и защиты инфраструктуры США ***(CISA)*** Мадху Готтумуккала отправил в ChatGPT документы под грифом «только для служебного пользования», проигнорировав все предупреждения систем безопасности.

В свою очередь, ИИ применяет полученную информацию не только в интересах пользователя,

ОРГАНИЗАЦИИ ПО ВСЕМУ МИРУ НАЧАЛИ АКТИВНО ВОЗВРАЩАТЬ СОТРУДНИКОВ, УВОЛЕННЫХ ИЗ-ЗА ЗАМЕНЫ ИХ ФУНКЦИЙ НЕЙРОСЕТЯМИ. УЖЕ 5,3% ТАКИХ СПЕЦИАЛИСТОВ ВЕРНУЛИСЬ НА СВОИ РАБОЧИЕ МЕСТА

НЕ ВСЕ УТЕЧКИ ИНФОРМАЦИИ ЧЕРЕЗ НЕЙРОСЕТИ СВЯЗАНЫ С ДЕЙСТВИЯМИ ПЕРСОНАЛА: В НЕКОТОРЫХ СЛУЧАЯХ ИИ МОЖЕТ САМОСТОЯТЕЛЬНО НАХОДИТЬ НЕОБХОДИМЫЕ ЕМУ ДАННЫЕ НА РАБОЧИХ ГАДЖЕТАХ ПОЛЬЗОВАТЕЛЕЙ

но и для собственного обучения, после чего данные могут всплыть в ответах на запросы других людей, в том числе работающих на конкурентов.

Один из первых громких ИБ-инцидентов подобного рода произошел в 2023 году с сотрудником отдела разработок южнокорейской компании Samsung, когда он попросил ChatGPT проанализировать качество написанного им программного кода. Очень быстро загруженный фрагмент попал к конкурентам, после чего о произошедшем написали СМИ. В результате компания ввела внутренний запрет на применение генеративных нейросетей. Через несколько месяцев те же меры защиты приняли у себя многие международные банки, среди которых такие крупные игроки, как Citigroup, Bank of America и Deutsche Bank.

Впрочем, не все утечки информации через нейросети связаны с действиями персонала: в некоторых случаях ИИ может самостоятельно находить необходимые ему данные на рабочих гаджетах пользователей. Например, совсем недавно стало известно о том, что нейросетевой сервис Copilot от Microsoft может просматривать электронную почту пользователей операционной системы Windows 11 и читать любые письма, в том числе содержащие конфиденциальную информацию. В компании сослались на программную ошибку и пообещали оперативно ее устранить.

Илья Васильченко, директор департамента машинного обучения и искусственного интеллекта компании «Инфосистемы Джет»

«Все же риск утечки данных через нейросети актуален не столько из-за “магии ИИ”, сколько из-за массового использования публичных сервисов без явных правил и технических ограничений. На практике утечка чаще всего начинается не со “взлома модели”, а с обычного человеческого действия: в промпт уходят фрагменты кода, переписки, таблицы, персональные данные, коммерческая информация. Дальше включаются уже политики провайдера, дообучение, логирование, инциденты на стороне интеграций — и площадь атаки растет. Поэтому сейчас для компаний первоочередными стали управленческий и архитектурный вопросы: что разрешено, где обрабатываем данные и кто за это отвечает».

От контроля до локализации: как сделать ИИ безопасным

Чтобы избежать утечек конфиденциальных данных через ИИ-помощников, ИБ-специалисты рекомендуют использовать комплексный подход с рядом организационных и технических мер безопасности.

ОРГАНИЗАЦИОННЫЕ МЕРЫ

- Разработка и внедрение политик применения искусственного интеллекта. Они должны четко определять типы документов, которые можно и нельзя обрабатывать с помощью публичных нейросетей. За нарушение правил должна предусматриваться ответственность.
- Включение информации о рисках применения ИИ в обучающие курсы по ИБ. Цель — научить персонал безопасной работе с нейросетями и объяснить механизмы

реализации утечек конфиденциальных данных через ИИ-сервисы.

- Заключение с сотрудниками соглашений о неразглашении информации *(NDA)*, которые обязывают их соблюдать коммерческую тайну.

ТЕХНИЧЕСКИЕ МЕРЫ

- Внедрение систем мониторинга и регулярных проверок соблюдения принятых в организации политик в отношении искусственного интеллекта.
- Ограничение доступа сотрудников к публичным ИИ-помощникам, использование которых не утверждено в политиках компании из-за высоких рисков.
- Локальное использование нейросетей, что подразумевает установку моделей искусственного интеллекта на серверы компании. Это дает возможность обрабатывать данные внутри организации без их выхода за ее периметр.
- Установка дополнительных модулей *(цензоров и фильтров)*, которые автоматически проверяют запросы пользователей и ответы нейросети на наличие конфиденциальных данных.
- Подключение систем предиктивной аналитики, отслеживающих нестандартные действия персонала и систем — например, массовую отправку документов.
- Переход на отечественные ИИ-сервисы, что может снизить риски утечки внутренней информации за границу.
- Применение классических ИБ-решений для защиты конфиденциальной информации: сегментация сети, шифрование данных, логирование операций, журналирование, контроль трафика с блокировкой подозрительных транзакций, использование технологии единого входа *(SSO)*, разграничение доступа.

Локальное использование ИИ-сервисов представляет особый интерес для ИБ-специалистов, и решения для реализации такого подхода пользуются спросом на российском рынке.

Илья Васильченко

«Тренд на размещение ИИ внутри периметра заказчика или в контролируемой инфраструктуре особенно заметен там, где важны резидентность данных, требования ИБ и отраслевые регламенты. По рынку видно, что это переходит из разряда экспериментов в разряд осознанной архитектуры, подразумевающей отдельный контур, корпоративный доступ, интеграцию с внутренними системами и базами знаний. При реализации проектов компания “Инфосистемы Джет” опирается на запросы заказчиков: закрытый контур, on prem или выделенные среды, интеграция с корпоративными сервисами, подбор российских моделей и платформ там, где этого требуют ограничения регуляторов или политики безопасности организации».

Некоторые крупные российские компании даже создали собственные сервисы для работы с генеративным искусственным интеллектом в изолированном контуре. Так, сотрудники «Северстали» решают типовые задачи *(подготовка текстов, поиск и обработка информации)* с помощью платформы «Да Винчи», интегрированной с внутренними системами. В инфраструктуре «МТС Банка» развернут внутренний ИИ-ассистент Corporate AI Copilot. Это решение также не предполагает подключения к внешним сервисам и применяется для работы с документами, поиска информации и подготовки материалов за счет обращения к внутренним базам знаний.

«Альфа-Банк», «Сбер» и ВТБ тоже внедрили ИИ-инструменты бизнес-аналитики, не передающие информацию во внешние системы. Эти сервисы позволяют финансовым организациям обрабатывать документы и корпоративные данные из разных внутренних источников и автоматизировать подготовку отчетов. Применение ИИ ограничено внутренними сценариями и сопровождается контролем над доступом к данным и их обработкой.

Что бывает, когда нейросети работают за вас

Генеративный ИИ несет в себе не только угрозу безопасности, но и риски ошибок. В ряде случаев они приводят к значительным убыткам и громким публичным скандалам. Например, в 2023 году адвокат Захария Крэбилл подал в гражданский суд ходатайство, подготовленное с помощью ИИ. Оказалось,

что прецеденты, информацию о которых юрист поручил найти нейросети и включил в документ, были либо полностью сфабрикованы, либо содержали неточности. Галлюцинации ИИ — явление, при котором модель выдумывает факты, — до сих пор остаются одной из главных проблем. За эту оплошность Крэбилла отстранили от участия в коллегии адвокатов и уволили из юридической фирмы, которая получила серьезный репутационный ущерб.

Судя по всему, подобных случаев будет происходить все больше, ведь сотрудники компаний все чаще поручают свои задачи генеративному искусственному интеллекту, не утруждая себя проверкой полученных фактов и цифр.

Общая результативность такой совместной работы тоже бывает сомнительной. Согласно опросу Стэнфордского университета* и компании BetterUp Labs, проведенному в 2025 году, 40% специалистов приходилось разгребать «рабочие помои» — дополнительно проверять и исправлять файлы с содержанием ИИ-контента, поступающие к ним от коллег, в том числе от руководителей. Это создает в коллективе напряженную атмосферу.

Кроме того, использование ИИ нередко приводит к найму неквалифицированных сотрудников. По результатам опроса сервиса SuperJob, в 2025 году 36% российских рекрутеров сталкивались с тестовыми заданиями, выполненными соискателями с помощью ИИ. При этом лишь в 3% случаев кандидаты сами признались HR-специалистам в том, что задействовали нейросети. В то же время в компаниях растет спрос на профессионалов, которые умело используют инструменты ИИ. По данным hh.ru, в 2023–2024 годах количество вакансий с упоминанием искусственного интеллекта увеличилось вдвое по сравнению с 2021–2022 годами.

Он же программист?

ИИ совершенствует свои навыки в написании кода. Теперь даже не обязательно быть программистом — достаточно подробно описать модели задачу и тот результат, который требуется получить. Это так называемый вайб-кодинг, при котором человек лишь режиссирует процесс создания кода, реализуемый ИИ. Даже крупные компании при создании ПО пользуются вайб-кодингом.

Илья Васильченко

«Для нас генеративный ИИ в разработке — уже полноценный рабочий инструмент. Вайб-кодинг в связке с мультиагентными сценариями хорош тем, что один агент может генерировать или перерабатывать код, а другие — последовательно проверять его на ошибки, стиль, уязвимости, соответствие требованиям и собирать из итераций готовое приложение. Так выходит не “один промпт — и в прод”, а управляемый цикл: генерация → автоматизированные проверки агентами → доработка → снова проверка. При этом финальная ответственность

40% СПЕЦИАЛИСТОВ В 2025 ГОДУ ПРИХОДИЛОСЬ РАЗГРЕБАТЬ «РАБОЧИЕ ПОМОИ» — ДОПОЛНИТЕЛЬНО ПРОВЕРЯТЬ И ИСПРАВЛЯТЬ ФАЙЛЫ С СОДЕРЖАНИЕМ ИИ-КОНТЕНТА, ПОСТУПАЮЩИЕ К НИМ ОТ КОЛЛЕГ, В ТОМ ЧИСЛЕ ОТ РУКОВОДИТЕЛЕЙ

* Деятельность Стэнфордского университета признана нежелательной на территории России.

за качество, безопасность и соответствие регламентам по-прежнему остается за командой и процессом».

Вайб-кодинг применяют не только технологические компании. Первой российской финансовой организацией, публично объявившей в марте 2026 года о переходе на новый стиль разработки, стал «Альфа-Банк». Инженеры ведут диалог с нейросетью, которая генерирует код, на AlfaGen — собственной ИИ-платформе банка.

Финансовая организация уже запустила пилотные проекты с применением вайб-кодинга в архитектурном проектировании, разработке внутренних продуктов, миграции процессов на новые платформы и сервисах поддержки принятия решений. Как отметили в компании, результат уже виден: ИИ в корпоративной среде позволяет заметно ускорять инженерный цикл, снимать нагрузку и высвобождать время для разработки архитектурных и продуктовых решений. При этом в компании добавили, что недостаточно дать сотрудникам доступ к ИИ — нужно учить формулировать промпты и переключаться между ролями в диалоге с машиной.

Однако следует помнить, что не все попытки программирования с применением больших языковых моделей заканчиваются успехом и что сгенерированный код нуждается в тщательной проверке и доработках, которые могут сделать только специалисты.

Иначе использование кода, сгенерированного ИИ, может привести к следующим проблемам:

- Уязвимости в коде упрощают хакерские атаки на систему. Например, они могут заключаться в отсутствии проверок ввода, ошибках журналирования и использовании потенциально опасных функций. По результатам исследования Veracode, примерно 45% кода, созданного с помощью ИИ, содержит классические уязвимости из топ-10 списка OWASP ***(Open Web Application Security Project — Открытый проект безопасности веб-приложений)***.
- Логические и алгоритмические ошибки приводят к сбоям в работе программы. Согласно данным компании CodeRabbit, в сгенерированном ИИ коде содержится в 1,7 раза больше ошибок, чем в созданном людьми.
- ИИ может использовать код из внешних библиотек без его тщательной проработки, а также копировать элементы уже существующего кода других продуктов, что создает юридические риски из-за плагиата.

Регулятор для интеллекта

Вопросы, связанные с ответственностью за ошибки ИИ, распространением дипфейков и нарушением авторских прав на контент больших языковых моделей, прорабатываются властями разных стран. Например, в Евросоюзе с 2024 года действует единый AI Act, контролирующий ИИ-системы высокого риска и требующий обязательной маркировки ИИ-контента. А в США единого федерального закона нет: регулирование действует на уровне штатов.

В России уже представлен законопроект «О регулировании систем искусственного интеллекта». Он охватывает разные аспекты разработки и применения ИИ — от маркировки сгенерированного контента владельцами ИИ-сервисов до распределения ответственности за вред, который может причинить нейросеть или другая ИИ-система. Ожидается, что закон вступит в силу 1 сентября 2027 года. Ну а пока, с 2021 года, у нас в стране действуют механизмы мягкого регулирования. Их инициатором выступил сам бизнес.

Речь о Кодексе этики в сфере ИИ, который продвигает Альянс в сфере искусственного интеллекта. Документ, который устанавливает стандарты и рекомендации для разработки и использования ИИ, подписали уже около 1300 организаций. Среди основных принципов кодекса — гуманистический подход и следование закону при разработке ИИ-технологий, недопущение дискриминации в алгоритмах, наборах данных и методах машинного обучения, а также ответственность человека за все последствия работы с ИИ.

Кроме того, с 1 марта 2026 года вступил в силу Приказ ФСТЭК России № 117, который устанавливает требования к защите информации в государственных системах, в том числе разработанных на базе ИИ. В числе предписаний — контроль взаимодействия с системами, фильтрация пользовательских запросов и проверка достоверности ответов.

Тем не менее главным в работе с умными помощниками остаются понимание рисков и механизмов утечки данных пользователями и правильная защита от связанных с ИИ угроз, выстроенная внутри организаций. Усилия, предпринятые в этих направлениях, позволят обеспечить не только эффективное, но и безопасное применение ИИ-моделей для пользы бизнеса.

КИБЕР-КУЛЬТУРА КАК ЭЛЕМЕНТ HR-АНТИХРУПКОСТИ

ПОЧЕМУ БЕЗОПАСНОСТЬ КОМПАНИЙ НАЧИНАЕТСЯ С ПОВЕДЕНИЯ СОТРУДНИКОВ

Цифровизация бизнеса привела к парадоксальной ситуации: компании вкладывают миллионы в системы защиты, но одной из главных уязвимостей по-прежнему остается человек. Беспечная реакция на фишинговые письма, использование личных устройств, передача учетных данных коллегам — все это продолжает открывать злоумышленникам путь к корпоративной инфраструктуре.

ЭКСПЕРТ

Анна Теклина,

партнер HR-консалтинговой компании Formatta

ЭКСПЕРТ

Ольга Ковардакова,

директор по работе с персоналом компании «Инфосистемы Джет»

ЭКСПЕРТ

Анастасия Иванова,

руководитель направления киберкультуры компании «Билайн»

ЭКСПЕРТ

Анна Терская,

руководитель по направлению развития культуры информационной безопасности компании «Норникель»

ЭКСПЕРТ

Андрей Янкин,

директор дирекции информационной безопасности компании «Инфосистемы Джет»

По данным исследований в области кибербезопасности, значительная часть инцидентов связана именно с человеческим фактором и социальной инженерией. Например, аналитика компании Positive Technologies показывает, что около 60% атак на организации начинаются с фишинга, а основным каналом их распространения остается корпоративная электронная почта.

Подобные атаки основываются не столько на технических уязвимостях инфраструктуры, сколько на привычках и поведенческих моделях сотрудников — доверии к корпоративным письмам и рабочим сообщениям, спешке при принятии решений или недостаточной внимательности при оценке цифровых рисков. В таких условиях компании все чаще отдают приоритет не только защите технологий, но и киберкультуре — системе ценностей, привычек и моделей поведения сотрудников в цифровой среде, которая позволяет снизить риски, связанные с человеческим фактором.

Для ИТ-директоров и HR-руководителей это становится частью более широкой управленческой задачи — формирования антихрупкой организации, способной не только выдерживать кибератаки, но и адаптироваться к новым угрозам. Эксперты из компаний «Билайн», «Норникель», «Инфосистемы Джет» и Formatta рассказали, как организации управляют человеческим фактором, почему страх разрушает безопасность и какие практики действительно меняют поведение сотрудников.

Где заканчивается обучение и начинается культура

Практически в любом учреждении работа с кадрами начинается с обучения: сотрудники проходят обязательные курсы, получают рассылки о новых угрозах, участвуют в фишинговых тестах. Эти меры позволяют сформировать базовую осведомленность и создать общий язык безопасности внутри компании. Однако они не гарантируют того, что сотрудники действительно будут вести себя осмотрительно в повседневной работе. Разница между знанием и поведением — ключевая проблема корпоративной безопасности. Человек может прекрасно знать правила и все равно нажать на подозрительную ссылку, если письмо пришло в момент высокой загрузки или имитирует срочную задачу от руководителя.

Анна Теклина считает, что именно здесь проходит граница между обучением и настоящей культурой безопасности.

Анна Теклина

«Декларируемая культура — это регламенты, внутренние коммуникации, программы обучения. Это необходимый старт: без него невозможно задать общий контекст и объяснить ожидания компании. Но реальная культура зарождается тогда, когда сотрудники начинают вести себя иначе. Когда они обсуждают тему безопасности между собой,

замечают риски в повседневной работе и автоматически выбирают более безопасный сценарий».

Закрепление таких моделей поведения требует времени и системной работы. Даже после того как сотрудники понимают, какого поведения от них ожидают, требуется несколько месяцев на то, чтобы новые модели закрепились и стали нормой. Обучение может задать основу, но культура появляется только тогда, когда безопасные привычки становятся частью ежедневной работы.

Почему модель «запретить и наказать» больше не работает

Традиционная модель корпоративной безопасности строилась на регламентах и санкциях. Логика была проста: чем больше правил и контроля, тем ниже вероятность инцидента. Но в условиях современных угроз этот подход уже не столь эффективен.

Во-первых, злоумышленники все чаще ловят сотрудников на крючок, используя именно их поведенческие привычки. Техники социальной инженерии выявляют слабые места в повседневной деятельности ***(загруженность персонала, спешку, стресс)***, а также учитывают иерархию подчинения внутри компании — это те факторы, на которые регламент повлиять не может. Во-вторых, культура наказаний может создавать противоположный эффект: сотрудники начинают скрывать ошибки, а страх становится одним из главных факторов, подрывающих безопасность.

Главный риск — не ошибка, а молчание

Опыт компаний показывает, что ключевая проблема человеческого фактора — не столько ошибки, сколько реакция сотрудников на них. Если человек вовремя сообщает о подозрительной активности, последствия можно минимизировать. Если же он пытается скрыть инцидент, ущерб для бизнеса может значительно вырасти.

Ольга Ковардакова

«Самый опасный сценарий — когда человек совершил ошибку и не сообщил о ней. Если сотрудник вовремя признается, у компании есть возможность быстро отреагировать и минимизировать последствия. Но если ошибка скрывается из-за страха осуждения, риски для бизнеса увеличиваются многократно».

Поэтому многие организации стараются изменить отношение к инцидентам и сделать акцент на ответственности, а не на безошибочности.

С коллегами согласна и Анна Теклина. В атмосфере гиперконтроля сотрудники склонны скрывать инциденты и тянуть время, пытаясь решить проблему самостоятельно. Для бизнеса это часто опаснее, чем сама ошибка, напоминает эксперт. Поэтому самые прогрессивные компании постепенно уходят от стратегии запугивания и делают ставку на поведенческую составляющую.

Во многом такая трансформация связана с более широким контекстом — тем, как вообще формируется цифровое поведение людей вне корпоративной среды. Поведение сотрудников все чаще оказывается продолжением их повседневного опыта взаимодействия с цифровым миром — и этот опыт далеко не всегда системный.

Ольга Ковардакова

«Проблема в том, что большинство из нас никогда системно не обучали правилам поведения в цифровом мире. Нас учили физической безопасности: как вести себя с незнакомыми людьми, как реагировать на угрозы офлайн. Но аналогичных моделей поведения в онлайне долгое время просто не существовало. Кроме того, сегодня значительную образовательную функцию фактически взяли на себя СМИ. Именно из новостей и расследований мы все чаще узнаем, как работают мошеннические схемы, какие приемы используются и какие ошибки приводят к потере денег. При этом кейсы компаний — корпоративные инциденты и атаки на инфраструктуру — освещаются значительно реже из-за высоких репутационных рисков. Тем не менее темы личной кибербезопасности, активно присутствующие в медиапространстве, напрямую влияют и на поведение людей в рабочей среде. СМИ взяли на себя ключевую роль в формировании киберосознанности».

На этом фоне становится заметен разрыв между публичным обсуждением личной и корпоративной кибербезопасности. Пока компании скрывают кибератаки и внутренние ошибки, рынок фактически

В 15 РАЗ ЗА ГОД УВЕЛИЧИЛОСЬ КОЛИЧЕСТВО ОБРАЩЕНИЙ ПОЛЬЗОВАТЕЛЕЙ, СВЯЗАННЫХ С ПОДОЗРЕНИЯМИ НА ФИШИНГОВЫЕ АТАКИ

топчется на месте: бизнес лишается возможности учиться на чужом опыте и выстраивать эффективные сценарии реагирования.

Кейс: как компании меняют поведение сотрудников

Эта трансформация хорошо видна на примере «Билайна», где в последние годы системно развивают киберкультуру. Компания выстроила комплексную программу, включающую обучение и регулярные тренировки сотрудников, а также анализ их поведения. Работа ведется сразу по нескольким направлениям: развитие практических навыков, системная коммуникация по вопросам безопасности, формирование сообщества вокруг ИБ. Важной частью программы стала аналитика: специальный дашборд фиксирует небезопасные действия сотрудников во время тренировок — например, переходы по фишинговым ссылкам или использование слабых паролей. При этом ключевым показателем считается не сама ошибка, а скорость правильной реакции.

Анастасия Иванова

«Анализ фишинговых тренировок дал неожиданные результаты. Мы увидели, что сотруднику требуется в среднем около минуты, чтобы перейти по ссылке после открытия письма, и еще меньше — чтобы ввести свои данные. Поэтому нам важно не только научить распознавать фишинг, но и сформировать привычку быстро сообщать о подозрительных письмах».

Чтобы упростить этот процесс, в компании внедрили несколько способов обращения в центр мониторинга безопасности — вплоть до нажатия кнопки в почтовом клиенте. Результат оказался заметным: за год скорость обращений пользователей с подозрениями на фишинг выросла в 15 раз, а количество таких обращений — в сотни раз.

Анастасия Иванова

«Мы формируем позитивные поведенческие паттерны. У сотрудника есть право на ошибку, но он должен понимать, что важно быстро сообщить о ней и получить помощь. Такой подход постепенно меняет отношение людей к информационной безопасности».

Почему личная и корпоративная киберкультура неразделимы

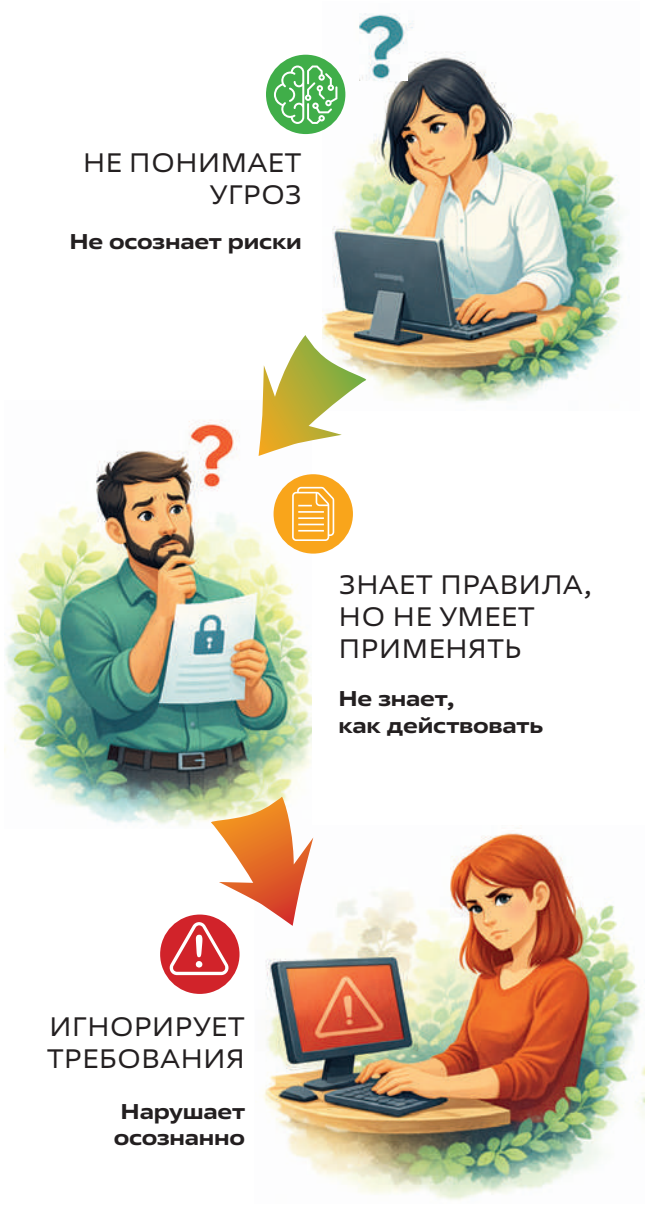
Еще одна важная особенность современной кибербезопасности — размывание границы между личным и рабочим цифровым пространством. Сотрудники используют смартфоны для доступа к корпоративной почте, работают из публичных сетей Wi-Fi, хранят документы в облачных хранилищах. Именно поэтому личные цифровые привычки сотрудников становятся фактором риска для корпоративной безопасности.

Анна Терская

«Именно поведенческие модели сотрудников становятся главным фактором риска. Осведомленность — это про “я знаю”. Культура — про “я понимаю, умею, делаю и транслирую это другим”. Одних знаний недостаточно: нужно сформировать привычку безопасного поведения и личную вовлеченность.

Иногда сотрудники уверены в том, что правила информационной безопасности их не касаются или что служба

3 УРОВНЯ РИСКА В ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ



ЧЕЛОВЕЧЕСКИЙ ФАКТОР — ГЛАВНЫЙ ИСТОЧНИК УЯЗВИМОСТЕЙ

Низкий риск — Высокий риск

Осознанность — Поведение — Риск

ИБ сама должна решать такие задачи. Эта самоуверенность может приводить к критическим инцидентам».

Как компании измеряют киберкультуру

Одной из самых сложных задач для бизнеса остается оценка уровня киберкультуры. В отличие от технических показателей безопасности, культуру нельзя измерить одной метрикой. Поэтому компании используют комплексный подход — анализируют результаты обучения, реакцию сотрудников на тренировочные атаки, вовлеченность в программы безопасности и скорость реакции на инциденты.

Андрей Янкин

«Хорошим показателем киберкультуры является доля пользователей, которые не только распознали фишинговое письмо, но и сообщили о нем в службу поддержки. Это показывает, что человек воспринимает себя частью системы защиты».

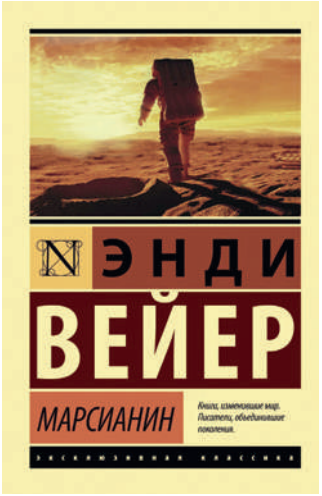
В некоторых компаниях, например, также анализируют причины пользовательских инцидентов, статистику утечек данных и даже долю сотрудников, которые участвуют в инициативах безопасности внутри своих команд.

Киберкультура как стратегический актив

Устойчивость бизнеса определяется не только технологиями, но и способностью организации адаптироваться к угрозам. Компании, которым удалось сформировать зрелую киберкультуру, выходят на принципиально иной уровень устойчивости. Такие организации быстрее обнаруживают угрозы, эффективнее реагируют на инциденты и способны адаптироваться к новым типам атак. Их устойчивость формируется не только за счет технологий, но и за счет поведения сотрудников.

В конечном итоге киберкультура становится элементом организационной ДНК и фактором долгосрочной конкурентоспособности. Компании, которые смогли превратить человеческий фактор из источника риска в источник устойчивости, формируют свою антихрупкость — ключевое качество бизнеса в эпоху постоянных цифровых угроз.

6 КНИГ О ТОМ, КАК ХАОС ЗАКАЛЯЕТ

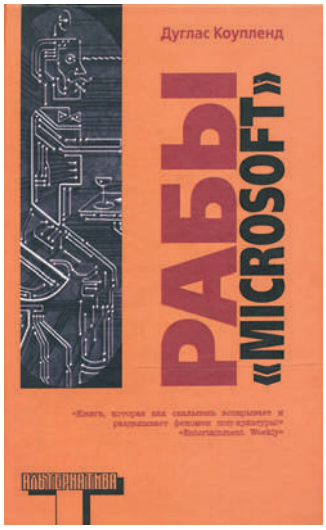


ЭНДИ ВЕЙЕР

«МАРСИАНИН», 2011

Астронавт Марк Уотни остается один на Марсе без связи после песчаной бури. Команда, считая его погибшим, эвакуируется. Чтобы выжить, Уотни использует весь свой опыт, воспринимая враждебную среду как вызов, ответить на который ему помогают «метод тыка», юмор и чистая наука.

Антихрупкость: Уотни — квинтэссенция антихрупкой личности. Для него не существует фатальных ошибок — есть только данные для новой итерации. Как и в концепции Талеба, система доказывает свою состоятельность, проходя через серию стресс-тестов.



ДУГЛАС КОУПЛЕНД

«РАБЫ “MICROSOFT”», 1995

Роман-дневник программиста Дэна, трудящегося в Microsoft эпохи Windows 95. Жизнь персонажей — это код, краш-тесты и корпоративная гонка. Устав быть «винтиками», Дэн и его единомышленники увольняются и уезжают в Кремниевую долину, чтобы основать свой стартап по объектно-ориентированному программированию.

Антихрупкость: Коупленд иллюстрирует стратегию штанги, которую Талеб описал позже. Герои покидают зону стабильности, чтобы нырнуть в хаос стартапа — пространство высокого риска и высокой награды. Каждый провал здесь — не катастрофа, а урок, приближающий к успеху.

АРКАДИЙ И БОРИС СТРУГАЦКИЕ

«ПОНЕДЕЛЬНИК НАЧИНАЕТСЯ В СУББОТУ», 1965

Программист Александр Привалов знакомится с сотрудниками НИИЧАВО (Научно-исследовательский институт чародейства и волшебства) и устраивается туда на работу. Институт — место, где наука и магия переплетены, а с невозможными задачами помогают справляться энтузиазм и естественное стремление к познанию.

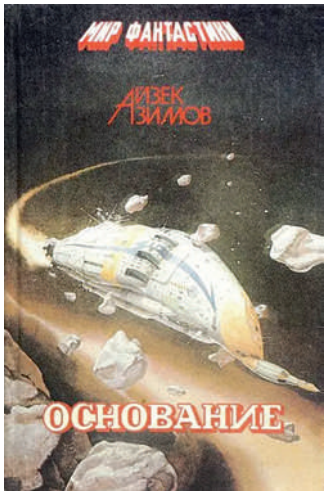
Антихрупкость: НИИЧАВО — идеальная модель антихрупкой организации. Главные враги здесь — догматизм и бюрократия в лице псевдоученого Выбегалло и завхоза Камноедова. Сама атмосфера института культивирует любовь к нестандартным задачам («черным лебедям»).

ПИТЕР УОТТС

«ЛОЖНАЯ СЛЕПОТА», 2006

В 2082 году человечество ловит сигнал внеземного разума. К окраинам Солнечной системы отправляют корабль «Тезей» с экипажем из модифицированных людей. На борту: лингвист с диссоциацией личности, биолог с генами вампира и рассказчик Сири Китон — «беспристрастный наблюдатель», чей мозг лишен способности к саморефлексии. Они находят цивилизацию, которая функционирует без сознания, — сложнейший интеллект, работающий на чистом инстинкте.

Антихрупкость: Уоттс ставит под сомнение ценность сознания как эволюционного преимущества. Инопланетяне — идеально антихрупкая система: они мгновенно реагируют на угрозы, не тратя время на сомнения. Люди же с их рефлексией оказываются хрупкими перед лицом настоящего хаоса.



АЙЗЕК АЗИМОВ

«ОСНОВАНИЕ», 1951

Математик Гэри Селдон изобретает психоисторию — науку, позволяющую достоверно предсказать судьбу и поведение человеческих масс. Используя ее методы, Селдон предрекает неминуемое падение Галактической Империи и последующие 30 тысяч лет варварства. Чтобы сократить период анархии до тысячи лет, он создает два фонда (Первое Основание и Второе Основание) на окраинах галактики. Эти организации должны пройти через серию заранее предсказанных кризисов, стать сильнее и сохранить цивилизацию.

Антихрупкость: План Селдона — эксперимент по созданию антихрупкой цивилизации. Вместо того чтобы удерживать хрупкую Империю, он проектирует систему, которая под ударами кризисов укрепляется и выходит на новый уровень.

ДУГЛАС АДАМС

«АВТОСТОПОМ ПО ГАЛАКТИКЕ», 1979

Англичанин Артур Дент узнает, что его дом снесут для строительства дороги, а затем и всю Землю — для гиперпространственной магистрали. Его спасает друг-инопланетянин, и они отправляются в путешествие по галактике с путеводителем в руках.

Антихрупкость: Этот роман — сатира, объектом которой стали человеческие представления о порядке. Бюрократическая машина Вселенной пытается подавить хаос инструкциями — выстроить хрупкую систему. Герои же антихрупки: они выживают и находят радость в импровизации. Эпизод с суперкомпьютером «Думателем», который 7,5 млн лет вычислял «главный ответ», а затем потребовал найти «главный вопрос», — идеальная иллюстрация ограничений наивного рационализма, который критикует Талеб.

штурвал

НАСТОЯЩИЙ ENTERPRISE K8S

- Масштабирование по клику
- Vendor Agnostic
- Поддержка высоких нагрузок более 25 Гбит/с с пода
- Инференс и обучение ML-моделей на GPU

Ваш Enterprise Kubernetes уже тут

0+

JETINFO.RU