

JET!NFO

SINCE 1995

№ 3 (327) 2026 JETINFO.RU



НЕПРЕРЫВНОСТЬ 2.0

Нить, ведущая к восстановлению

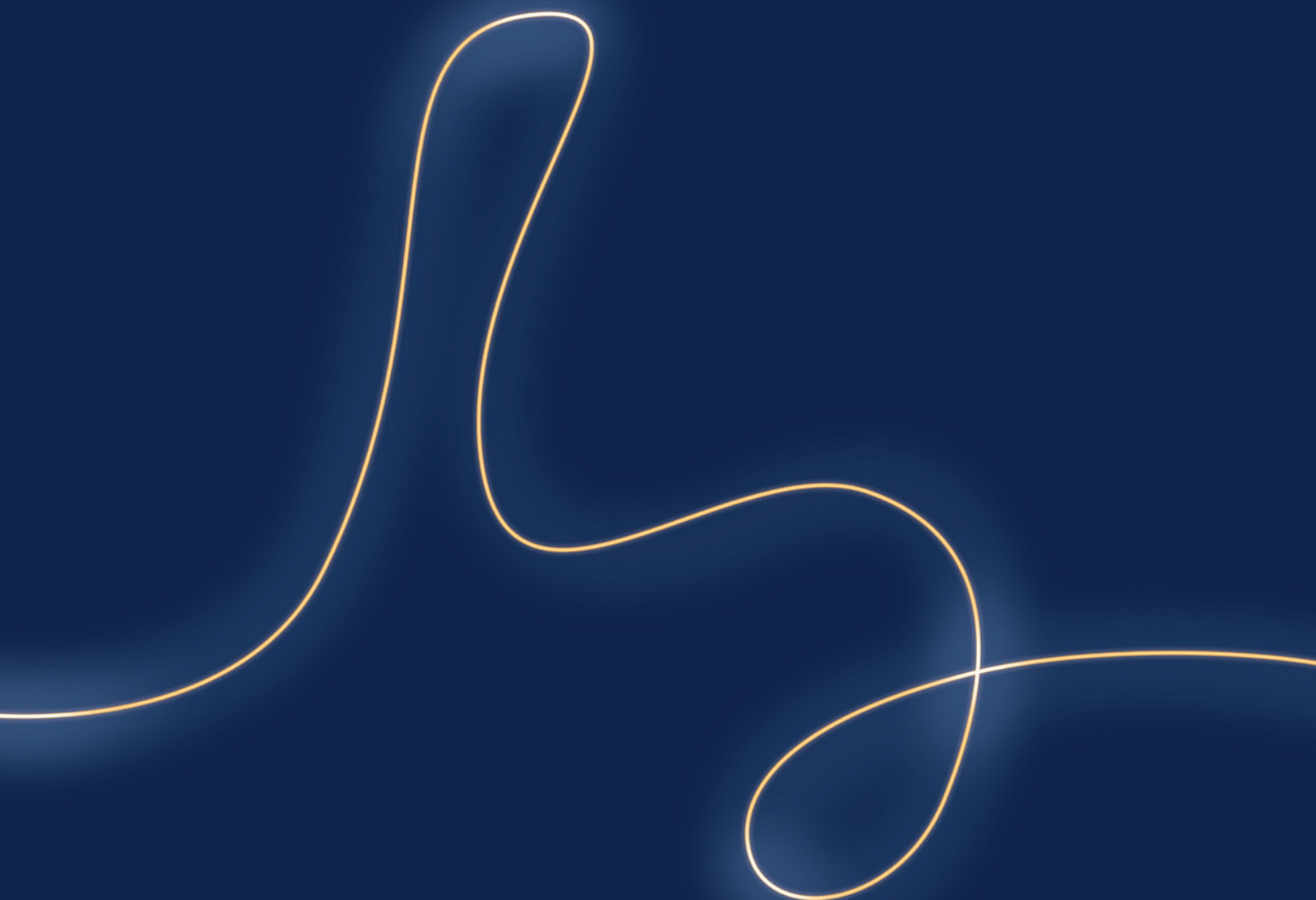
Что должно быть
в современном DR-плане

Защита от Минотавра

Как «Бункер» и «Цитадель»
удерживают бизнес вне зоны
поражения

Как быстрее выйти из лабиринта

Верные шаги и типичные ошибки
в первые 48 часов после кибератаки



«Возьми этот клубок, — сказала Ариадна, — привяжи его у входа и иди. Нить выведет тебя назад».

Нить Ариадны не делала Лабиринт безопаснее. Она давала Тесею главное — ориентир, позволяющий идти вперед и не терять дорогу назад.

Эта метафора точно описывает классический подход к обеспечению непрерывности бизнеса. Мы не можем гарантировать, что кибератака или масштабный ИТ-сбой никогда не произойдут. Поэтому строим защиту, резервируем инфраструктуру, готовим планы восстановления — и оставляем себе нить, которая должна вывести к исходной точке.

Но что, если входа в Лабиринт больше нет?

Современный Лабиринт постоянно меняется. Это живая киберфизическая среда, где стены движутся каждую миллисекунду, а Минотавр — кибератака или неконтролируемый сбой — идет за нами по пятам.

Поэтому непрерывность нового поколения — это уже не способность найти дорогу назад. Это способность пересобрать Лабиринт вокруг себя, быстро восстановив критически важные функции и сделав систему устойчивее после удара.

Нить Ариадны превращается из плана восстановления в петлю обратной связи — механизм адаптации в реальном времени. Мы уходим от культа безаварийности к стратегии антихрупкости — способности меняться под воздействием кризиса. Учимся использовать ярость Минотавра как источник энергии для перезагрузки.

Так начинается эпоха Непрерывности 2.0. Мы перестаем быть Тесеем, ищущим прежний выход, и становимся архитекторами, способными перекраивать Лабиринт на ходу.

Что это означает на практике? Локализовать последствия инцидентов, создавая подушки безопасности. Изолировать доверенные резервные копии и критические системы в «Бункере» и «Цитадели». Проектировать бизнес-процессы так, чтобы в кризис сохранить главное, отказавшись от второстепенного. И учитывать, что после серьезного инцидента возвращение к состоянию «как было» может быть невозможно — и не всегда необходимо.

Об этом — от подготовки к кризису до восстановления и трансформации после него — наш номер. Нить Ариадны проходит через него буквально и метафорически. Для нас она стала символом не абсолютной защищенности, а способности сохранять направление, когда привычные ориентиры исчезают. 🧶



12+

РЕДАКЦИЯ ЖУРНАЛА

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

Арт-директор: **Наталья Васильева**

Директор по маркетингу: **Дарья Пенчилова**

Выпускающий редактор: **Эвелина Кегелик**
ed.kegelik@jet.su

Корректор: **Ирина Карпушина**

PR: **Ольга Проколопова**

Фотограф: **Карэн Эгнатосян**

Иллюстраторы: **Наталья Васильева, Эвелина Кегелик, Мария Майдунова, Вера Подерская**

Изображения: **Shutterstock, ChatGPT, Midjourney, Nano Banana, GPT Image 2, Claude, Nano Banana Pro, Grok, Magnific, Clarity**

Авторы и эксперты

Андрей Абашев, Олег Абелев, Сергей Андронов, Андрей Блинов, Всеволод Воробьев, Евгений Гаранин, Дмитрий Герасимов, Антон Голощапов, Станислав Гордеев, Дмитрий Горохов, Александр Гуляев, Никита Гусев, Дмитрий Деев, Дмитрий Дементьев, Антон Елизаров, Владимир Елисеев, Константин Ильютченко, Александр Карпенко, Эвелина Кегелик, Дарья Керценбаум, Антон Клочков, Борис Конаков, Екатерина Ларина, Роман Лебедь, Сергей Левашов, Антон Мерцалов, Федор Момот, Александр Морковчин, Аскар Мусаев, Денис Непочатых, Алексей Пигачев, Михаил Рубинчик, Александр Сабуров, Ринат Сагиров, Георгий Старостин, Александр Сулима, Павел Тесленко, Александр Тоцкий, Наталья Травова, Роман Фролов, Роман Шапиро, Александр Шестопалов, Антон Шипулин, Игорь Шконда, Дмитрий Якоб, 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

24 августа 2026 г.

Издатель

АО «Инфосистемы Джет»

Адрес издателя:

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

Распространяется бесплатно по подписке, также журнал представлен в бизнес-зале «Сбера» в аэропорту Шереметьево, «Кибердоме» (Москва) и на ИТ-мероприятиях

Оформить подписку на журнал:
jetinfo@jet.su

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

Журнал издается с 1995 г. компанией «Инфосистемы Джет»

Права на публикуемые материалы принадлежат компании «Инфосистемы Джет». Перепечатка и воспроизведение материалов, а также любых фрагментов из них возможны лишь с письменного разрешения редакции журнала JETINFO.

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.



6

Элементы

Ничего личного — просто простой

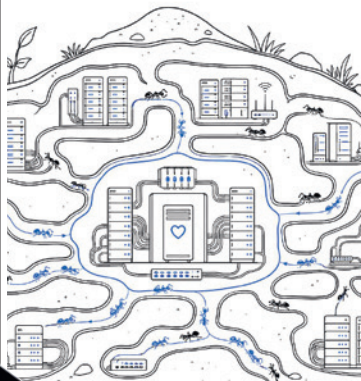
Что ИТ-эксперты из разных отраслей вкладывают в понятие «непрерывность бизнеса»

20

ИТ-инфраструктура

Нить, ведущая к восстановлению

Как устроен современный DRP



10



Элементы

Минута на миллион

Что стоит за простым бизнесом и как перейти от цифр к действиям



41

18

Инфографика

Корабль «Непрерывность 2.0». Новая Надежда»

31

ИТ-инфраструктура

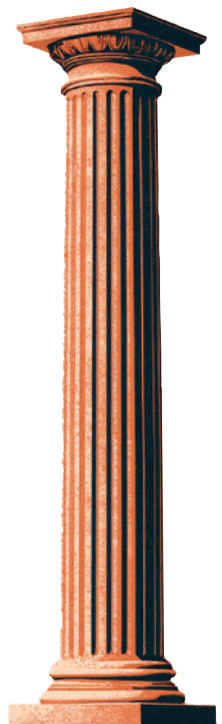
Стальная закалка

Как харденинг усложняет путь киберпреступников

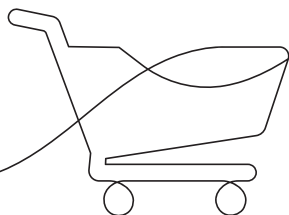
ИТ-инфраструктура

Защита от Минотавра

Как «Бункер» и «Цитадель» удерживают бизнес вне зоны поражения после кибератаки



48



ИТ-инфраструктура

Как не рухнуть с пика

Колонка Дмитрия Герасимова
(управляющий директор
по ИТ Lamoda)



54

ИТ-инфраструктура

Стратегия предвидения

Роль предиктивного ИИ
в бесперебойной работе
предприятий

62

Сетевые решения

Эволюция телеком-магистралей

Как и зачем операторы
переходят на
архитектуру Telco Cloud

70

Сетевые решения

Все за одного

Промышленный подход
к геораспределению
ЦОД

76

Репортаж

«Остался только свет»

На ЦИПР-2026 обсудили
непрерывность бизнеса
в эпоху кибертерроризма

82

Кибербезопасность

Отрицать нельзя признать

Как компании говорят
о кибератаках



90

Кибербезопасность

«Мы в своей открытой позиции видим вклад в общую кибербезопасность»

Интервью с Романом
Фроловым (член Совета
директоров Страхового
Дома ВСК)



100

Кибербезопасность

Как киберриски влияют на инвестиционный ландшафт

Колонка Олега Абелева
(начальник аналитического
отдела инвестиционной
компании «Риком-Траст»)



Кибербезопасность

Всё по-настоящему

Колонка Романа Шапиро
(руководитель дирекции
ИБ «Почты России»)

106

Кибербезопасность

Нервный срыв производства

С чего начинается
киберустойчивость
АСУ ТП



114



120

Кибербезопасность

Искусственный интеллект атакует!

Колонка Романа
Лебеда (руководитель
центра защиты
приложений
в «Т-Банке»)

126

Кибербезопасность

Как быстрее выйти из лабиринта

Верные шаги и типичные
ошибки в первые
48 часов после кибератаки

134

Книжная полка

Природа непрерывности

6 книг о том, как выживают
сложные системы



НИЧЕГО ЛИЧНОГО — ПРОСТО ПРОСТОЙ

ЧТО ИТ-ЭКСПЕРТЫ ИЗ РАЗНЫХ
ОТРАСЛЕЙ ВКЛАДЫВАЮТ В ПОНЯТИЕ
«НЕПРЕРЫВНОСТЬ БИЗНЕСА»

Непрерывность бизнеса — понятие многогранное: оно включает в себя и доступность критичных сервисов, и готовность к восстановлению инфраструктуры, и способность компании выполнять свои обязательства в нештатной ситуации. Но какие же процессы действительно нельзя останавливать? И насколько длительным может быть простой, с которым бизнес готов смириться?

Мы обратились с вопросом «Что для вас означает непрерывность бизнеса?» к представителям программного комитета конференции IT Elements и попросили их обсудить эту тему с учетом отраслевого профессионального опыта.

Эксперты рассказали о возможных последствиях сбоев, о том, насколько важно иметь протестированные планы по обеспечению непрерывности бизнеса (BCP) и аварийного восстановления (DRP), а также о балансе инвестиций в защиту ИТ-инфраструктуры и в ее восстановление после киберинцидентов.

Специалисты из разных сфер: банковского сектора, авиации, промышленности и ИТ — рассмотрели непрерывность бизнеса с учетом своей отраслевой специфики, поэтому за одним понятием оказываются разные риски и приоритеты.



АЛЕКСАНДР САБУРОВ,
директор департамента больших данных
«Россельхозбанка»

Для меня непрерывность бизнеса — это способность компании сохранять работу ключевых сервисов независимо от технологических сбоев, киберинцидентов, отказов оборудования или изменений ИТ-ландшафта. Сегодня уже недостаточно иметь только резервное оборудование или запасную площадку: устойчивость должна закладываться на этапе проектирования архитектуры данных и информационных систем.

Для банка это особенно важно, поскольку от доступности ИТ зависят платежи, дистанционное обслуживание, операции по счетам и кредитные процессы. К критичным также относятся системы обработки данных и формирования отчетности, платформы аналитики, управления рисками и решения на базе ИИ. Из-за высокой связанности инфраструктуры сбой одного компонента может затронуть сразу несколько процессов.

Поэтому при развитии платформы больших данных мы уделяем внимание распределенной архитектуре, резервированию критичных компонентов, импортонезависимому технологическому стеку и возможности проводить обновления без остановки бизнеса. Сегодня зрелость инфраструктуры определяется не отсутствием изменений, а способностью проводить их безопасно, сохраняя доступность сервисов.

BCP и DRP должны быть не формальными документами, а рабочими инструментами, которые отражают реальную архитектуру и взаимосвязи систем. Их необходимо регулярно актуализировать и проверять на практике — только так можно выявить ограничения и подтвердить готовность к восстановлению в установленные сроки. Защиту и восстановление при этом нельзя противопоставлять — это части единой стратегии устойчивости.



JETINFO.



АНТОН КЛОЧКОВ,
руководитель направления отдела разработки
архитектурных решений компании «Базис»

Для меня непрерывность бизнеса — это способность компании пережить «черный вторник» без потери клиентов и денег. На практике она начинается с RTO и RPO, согласованных с бизнесом, а не придуманных ИТ-службой. Для нашей платформы виртуализации это 15 минут для RTO и 5 минут для RPO.

Однако цифры в документах сами по себе ничего не гарантируют. Мы не верим бумажкам: регулярно моделируем отказ отдельного узла или целого ЦОД. Если не уложились в заданные сроки, идем разбираться, а не ждем, пока «жареный петух клюнет». А кроме того, непрерывность неотделима от безопасности: нужно встраивать защиту на этапе проектирования, а не латать дыры постфактум.

Критичными мы считаем систему управления виртуализацией, CI/CD и репозитории, где хранятся более 6000 пакетов. Остановка конвейера сборки означает, что мы не можем выпускать обновления, а значит, рискуем безопасностью клиентов. Техническая поддержка также должна быть доступна постоянно. DNS, AD, VPN, NTP и DHCP мы дублируем, резервируем SAN и сетевую связность на уровнях L2 и L3.

План без проверок — макулатура. Раз в квартал мы проводим tabletop-учения, ежемесячно используем Chaos Engineering, а раз в полгода устраиваем внезапные проверки: «Через пять минут сервис упадет — восстанавливайте». После каждого сценария планы корректируются. Такой же баланс мы стараемся сохранять и между предотвращением инцидентов и готовностью к восстановлению. Около 70% инвестиций направляется на защиту (*Secure SDLC, пентесты и собственные средства защиты*), еще 30% — на восстановление (*резервные ЦОД, бэкапы по схеме 3-2-1 и обучение*). Для нас это обязательный «страховой полис».



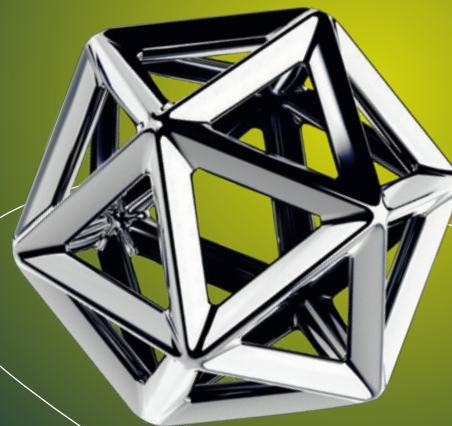
СЕРГЕЙ ЛЕВАШОВ,
заместитель генерального директора по ИТ
и цифровой трансформации Государственного научно-
исследовательского института гражданской авиации

Для нас непрерывность бизнеса — это синоним операционной устойчивости. В авиации нет понятия «временно остановились на профилактику»: рейс либо выполняется, либо нет. Его отмена влечет серьезные последствия для авиакомпаний, аэропорта и пассажиров. Поэтому непрерывность — это прежде всего способность ключевых цифровых систем сохранять функциональность при кибератаке, отказе оборудования или человеческой ошибке.

В первую очередь это касается процессов, от которых зависят безопасность пассажиров и организация полетов: регистрация, обработка багажа, управление аэропортом, контроль доступа в защищенные зоны, обмен данными между аэропортом, перевозчиками и государственными информационными системами, а также аэронавигационное обслуживание. Остановка любого из них может запустить цепочку трудно прогнозируемых последствий.

Именно поэтому BCP и DRP необходимы не как согласованные документы в папке на полке, а как отработанные сценарии действий. Мы проводим командно-штабные учения для руководства, чтобы отработать процесс принятия решений, и технические — чтобы протестировать переключение на резервные системы и реагирование на инциденты ИБ. Периодичность зависит от конкретной критичной системы, но принцип один: план, который ни разу не проверяли «в бою», остается документом, а не рабочим инструментом.

По той же причине нельзя ограничиваться только превентивной защитой. Основные вложения действительно направляются на привлечение квалифицированных специалистов, организацию защиты и мониторинг, но резервирование и восстановление остаются обязательной частью устойчивости. Атакующие постоянно совершенствуют свои методы, поэтому минимизировать потери позволяет только комплексный подход.



ДМИТРИЙ ДЕЕВ,
руководитель отдела ИТ-
инфраструктуры и сервисов компании
«Ви.Тех»

Для меня непрерывность бизнеса — это способность компании продолжать выполнять основные функции и предоставлять услуги во время возможных инцидентов и после их завершения. Главная цель всех мероприятий в этой области — минимизировать влияние инцидентов и сократить время восстановления систем.

Мы разделяем информационные системы по уровню критичности — от Office Productivity до Mission Critical. К категориям Mission Critical относятся основные системы, которые обеспечивают работу базовых процессов продаж. Именно для них особенно важно заранее определить порядок действий в случае сбоя и в сценарии восстановления.

Поэтому BCP и DRP должны быть обязательно разработаны и внедрены. Они позволяют быстрее и с минимальными потерями восстановить работоспособность компании. При этом планы необходимо проверять на практике по основным и критичным сценариям отказов. Все выявленные во время тестирования недочеты должны фиксироваться, а затем последовательно устраняться.



АЛЕКСАНДР ТОЦКИЙ,
руководитель департамента
инфраструктуры и сопровождения
систем «Совкомбанка»

Для нас непрерывность бизнеса начинается со способности сохранять доверие клиентов и выполнять обязательства в любой ситуации — даже когда системы испытывают повышенную нагрузку или сталкиваются со сбоями. В банковской отрасли это напрямую зависит от доступности платежных систем, автоматизированной банковской системы и каналов дистанционного обслуживания: допустимый простой core banking исчисляется минутами.

Чтобы сократить влияние таких инцидентов, необходимо иметь адаптивную инфраструктуру, способную самостоятельно подстраиваться под изменяющиеся условия. Часть рутинных операций уже берет на себя автоматизация на базе ИИ, а самовосстанавливающиеся системы устраняют отдельные сбои без участия человека. Однако идеальной защиты не существует, поэтому не менее важно заранее подготовиться к восстановлению.

Именно для этого нужны BCP и DRP. Критичные системы проходят DR-тестирование от одного до трех раз в год с реальным переключением, когда боевая и резервная среды меняются ролями. Кроме того, ежегодно мы проводим имитационные учения по потере ЦОД.



АНДРЕЙ АБАШЕВ,
директор по развитию функции ИБ, департамент
защиты информации и ИТ-инфраструктуры компании
«Норильский никель»

Непрерывность бизнеса я понимаю как способность организации сохранять работу критически важных функций без недопустимых пауз. Компания обязана продолжать предоставлять клиентам продукты и услуги на заранее согласованном уровне, в соответствии с определенными качественными и количественными показателями, даже если произошла кибератака, обнаружен отказ ИТ-компонентов, случился природный катаклизм или другой серьезный сбой.

При этом непрерывность бизнеса нельзя сводить только к информационной безопасности. ИБ создает условия для безопасной работы и защищает цифровые активы, но конечной целью остается не сама защита, а выполнение бизнесом своих обязательств. В отдельных случаях критически важные функции могут временно поддерживаться и без ИТ — с помощью бумажного документооборота, телефонной связи или ручных расчетов. Более того, необходимые меры защиты: изоляция сети, блокировка учетных записей, отключение систем и пр. — сами способны на время ограничить работу. Поэтому при инциденте в центре внимания должно оставаться восстановление бизнес-функций, а не отдельных ИТ- или ИБ-сервисов.

Отсюда следует и необходимость более широкого взгляда на риски. Чтобы обеспечить непрерывность бизнеса, нужно не только учитывать киберугрозы, но и предусмотреть проблемы с персоналом, оборудованием, помещениями, электроснабжением, а также трудности в коммуникации с партнерами или поставщиками. Полноценная система управления непрерывностью бизнеса охватывает все критические ресурсы и предусматривает альтернативные способы выполнения процессов. В первую очередь это относится к функциям, остановка которых может привести к человеческим жертвам, экологическим последствиям или существенным финансовым потерям. ●

МИНУТА НА МИЛЛИОН

ЧТО СТОИТ ЗА ПРОСТОЕМ БИЗНЕСА И КАК ПЕРЕЙТИ ОТ ЦИФР К ДЕЙСТВИЯМ

Кибератаки утвердились в статусе главного риска для непрерывности бизнеса. В 2025 году они впервые обошли ИТ-сбои (42% против 33% инцидентов) на российском рынке, показало исследование команды Jet Security компании «Инфосистемы Джет». В то же время опасно недооценивать все остальные угрозы, которые никуда не исчезли. Локальные отказы оборудования, природные катаклизмы и техногенные сбои, вызванные в том числе ошибками персонала, — эти события по-прежнему способны парализовать компанию за считанные минуты. Полностью защититься от инцидентов нельзя. А что можно? Оценить возможные последствия и сделать выход из критической ситуации предсказуемым, плавным и менее стрессовым. Как из потенциальных угроз рождаются конкретные цифры, а из цифр — четкие инструкции, читайте в материале.

Угрозы непрерывности бизнеса в разных отраслях

Эксперты программного комитета конференции IT Elements 2026 назвали главные риски для непрерывности бизнеса. Их перечни оказались похожими по составу угроз, но разными по расстановке приоритетов.

Киберугрозы: от фишинга до атак через поставщиков

Киберинциденты могут привести к компрометации данных, недоступности сервисов, нарушению производственных процессов и даже к полному уничтожению ИТ-инфраструктуры. Защититься на 100% от ИБ-угроз сегодня невозможно, при этом мотивы злоумышленников меняются: финансовая выгода все чаще уступает место хактивизму — политически мотивированным деструктивным атакам. Эксперты из разных отраслей ставят киберугрозы на первое место среди рисков.

Сергей Левашов (Государственный научно-исследовательский институт гражданской авиации)

«Отраслевая статистика по авиации и аэропортам в целом фиксирует ощутимый рост числа и сложности инцидентов за последний год. Атаки становятся более точными и часто связаны не только с финансовыми убытками, но и с репутационными потерями».

DDoS-атаки и программы-вымогатели не знают отраслевых границ — с ними сегодня сталкиваются все сегменты бизнеса. Финансовый сектор принимает на себя около трети всех DDoS-атак, и они постоянно эволюционируют, отмечает Александр Тоцкий («Совкомбанк»). Для промышленности одним из главных рисков становятся вирусы-шифровальщики, указывает Андрей Абашев

(«Норильский никель»). А в авиации наблюдается резкий рост активности обоих типов атак, констатирует Сергей Левашов (Государственный научно-исследовательский институт гражданской авиации).

Вместе с тем сразу несколько экспертов подчеркнули, что атаки все чаще совершаются не напрямую, а через подрядчиков или поставщиков.

Одним из основных векторов проникновения злоумышленников в инфраструктуру компаний, вне зависимости от отрасли, остаются фишинг и другие приемы социальной инженерии. Эта тенденция подтверждается и на глобальном уровне: согласно отчету Verizon 2025 Data Breach Investigations Report (DBIR), на долю внешних угроз, социальной инженерии и атак на веб-приложения приходится 96% всех утечек данных. При этом, как показывают сразу несколько международных исследований, фишинговые письма чаще всего генерируются ИИ.

Антон Клочков («Базис»)

«В нашей компании практикуется принцип zero trust, используется обязательная двухфакторная аутентификация, выполняются ежемесячные тестовые фишинговые рассылки. Один сотрудник все же попался — теперь учим всех на его ошибках, а не прячем голову в песок».

Впрочем, человеческий фактор проявляется и в типичных ошибках администрирования — например, когда инженер открывает порт в интернет ради удобства, без согласования со службой ИБ.

Важно учитывать, что на практике ИБ-угрозы часто пересекаются и комбинируются, образуя комплексные векторы атак, напоминает Андрей Абашев («Норильский никель»). Так, социальная инженерия запускает целый каскад: обман сотрудника → компрометация цепочки поставок → атака на бизнес-процесс → атака на производственный процесс.

Андрей Абашев

«Подобная каскадность и взаимное усиление угроз делают непрерывность бизнеса критически важной дисциплиной: система управления непрерывностью должна учитывать не просто отдельные инциденты ИБ, а комплексные

сбоев, затрагивающие временно людей, процессы, технологии и внешних партнеров. Такая система должна обеспечивать восстановление критически важных функций на приемлемом уровне и в согласованные сроки».

Технические сбои и масштабные ИТ-инциденты

Технические сбои — еще одна группа рисков. В сложной экосистеме, такой как современный банк, отказ одного компонента способен повлиять на выполнение сразу нескольких критически важных бизнес-процессов. Поэтому требуется соответствующая архитектура, предусматривающая резервирование, отказоустойчивость и отсутствие единичных точек отказа, подчеркивает Александр Сабуров («Россельхозбанк»).

Большие перемены: релизы, миграции, импортозамещение

Третья группа рисков связана с плановыми, но сложными изменениями — и здесь банковский сектор оказался одним из самых чувствительных.

Александр Тоцкий («Совкомбанк»)

«По открытым данным, 38% крупных инцидентов в банках связаны с ИТ-изменениями — релизами, миграциями, интеграциями. Поэтому критичны и защита, и управление изменениями: поэтапные релизы, автореверсии, возможность быстрого отката».

Александр Сабуров («Россельхозбанк») добавляет, что переход на отечественное ПО, миграция данных, обновление платформ и внедрение новых технологий, включая решения на базе искусственного интеллекта, должны производиться так, чтобы банк работал без перебоев и не нарушал требования регуляторов.

Набор основных угроз универсален. Но оборачиваются эти угрозы разными

последствиями. Для банка — остановкой платежей, для авиакомпании — сбоем в расписании полетов, для промышленности — остывшими печами и сорванными контрактами. И у каждого простоя — своя цена.

Как бизнес оценивает последствия инцидентов

Зачем оценивать последствия сбоев и инцидентов? Для начала — это требование регуляторов для ряда отраслей. Законодательство предписывает организациям количественно измерять риски, ущерб и время восстановления.

Сергей Левашов

«Использование формул для подсчета рисков и оценки ущерба является прямым требованием нормативных актов. В частности, вступивший в силу 1 марта 2026 года Приказ ФСТЭК России № 117 вводит обязательную количественную методологию для этих целей. При оценке защищенности государственных информационных систем (ГИС) больше не применяются статичные классы. Вместо них вводится коэффициент защищенности информации (КЗИ) — числовой показатель от 0 до 1, который рассчитывается по строгой методике и применяется для того, чтобы оценить текущие риски в организации и принять меры по защите».

В основе оценки бизнес-последствий любых инцидентов — от кибератак до отключения электричества — лежит BIA (*Business Impact Analysis*). Это универсальный инструмент, который помогает измерить потенциальный ущерб от простоев критических процессов. С его помощью аналитики определяют, остановка каких процессов и как быстро причинит компании недопустимый ущерб, какие ресурсы, в том числе ИТ-активы, критичны для этих процессов.

Независимо от того, что вы оцениваете — последствия кибератаки, технического сбоя или ошибки персонала, — основой любого анализа станут три универсальные метрики.

MTPD (*Maximum Tolerable Period of Disruption*) — максимально допустимое время остановки процесса. Это самый жесткий показатель. Проще говоря, это «потолок»



В ОСНОВЕ ОЦЕНКИ БИЗНЕС-ПОСЛЕДСТВИЙ ЛЮБЫХ ИНЦИДЕНТОВ ЛЕЖИТ ВИА, ОН ПОМОГАЕТ ИЗМЕРИТЬ ПОТЕНЦИАЛЬНЫЙ УЩЕРБ ОТ ПРОСТОЕВ КРИТИЧЕСКИХ ПРОЦЕССОВ

времени простоя. MTPD устанавливается руководством на основе анализа как минимум финансовых, репутационных и регуляторных последствий из-за простоя. Например, для платежного шлюза MTPD может исчисляться минутами, а для внутренней системы отчетности — часами.

RTO (Recovery Time Objective) — целевое время восстановления после инцидента. Критическое правило: RTO всегда должно быть меньше или равно MTPD.

RPO (Recovery Point Objective) — допустимая потеря данных (*в пересчете на время*). Этот показатель напрямую влияет на стратегию резервного копирования: если RPO составляет 15 минут, значит, бэкапы должны создаваться не реже чем каждые 15 минут.

Это не просто цифры в Excel. Эти метрики определяет ВИА для каждого критического процесса, и российские компании активно их используют. Именно эти метрики, а не абстрактные суммы убытков ложатся в основу ВСР: устанавливают, какие процессы резервировать в первую очередь, какие сроки восстановления закладывать в контракты и сколько инвестировать в защиту.

Александр Тоцкий

«RTO и RPO — это база, но нужно видеть всю цепочку зависимостей клиентского пути: сеть, ЦОД, API, поставщиков. Важнее измерять не доступность отдельных систем, а работоспособность пути в целом. Клиенту важно, что платеж прошел, а не где именно случился сбой. AIOps позволяет прогнозировать отказы

заранее, сокращая реакцию с часов до секунд».

В «Совкомбанке» считают стоимость часа простоя, вероятность инцидента, регуляторные и репутационные риски. А ИИ-аналитика выявляет нетривиальные корреляции между поведением пользователей и рисками сбоев, переводя абстрактные угрозы в конкретные финансовые показатели.

Как рассказал **Дмитрий Деев**, в компании «Ви.Тех» применяют детализированные матрицы, которые учитывают возможные убытки, критичность процессов, степень влияния и вероятность инцидентов.

Для расчета непосредственно стоимости простоя — независимо от его причины — используется модель TCoDT (*Total Cost of Downtime*).

TCoDT (за час) = Прямые денежные потери за час (Выручка + Зарплаты + Восстановление + Штрафы).

Дополнительно (*риск-корректировка*): репутационные потери и потеря лояльности рассчитываются отдельно как вероятностные отложенные убытки и прибавляются к годовой сумме риска, а не к часовой ставке.

Если рассматривать формулу более развернуто, получаем такую схему TCoDT:

- **Потеря дохода:** Годовая выручка / 525 600 минут в году × Количество минут простоя.
- **Потери от простоя сотрудников:** Средняя почасовая оплата × Количество сотрудников × Часы простоя × Коэффициент восстановления 1,4. Коэффициент 1,4 учитывает посткризисное падение продуктивности: после серьезного сбоя сотрудникам требуется в среднем 23 минуты, чтобы вернуть фокус.
- **Затраты на восстановление:** сколько потратили на зарплату специалистов, которые устраняли сбой, и на оборудование/услуги.
- **Штрафы:** штрафные санкции, которые компания выплачивает немедленно или в короткий срок: по SLA перед

клиентами, за нарушение сроков восстановления, а также штрафы регуляторов (*например, за недоступность сервисов*).

- **Потеря лояльности клиентов:** часть клиентов может уйти к конкурентам. Потерю выручки умножаем на процент повторных продаж.
- **Репутационные потери:** негатив в соцсетях и на сайтах-отзовиках, из-за чего новые клиенты не придут. Потенциальную потерю клиентов умножаем на пожизненную ценность клиента.

Результат этих расчетов — это денежная оценка фактического простоя. Однако сами по себе эти цифры не дают ответа на вопрос, насколько эффективно компания управляет процессом восстановления. Поэтому на основе полученных данных и целевых показателей (*RTO, RPO*), определенных в ходе BIA, проводится GAP-анализ. Он позволяет сравнить фактическое положение дел (*реальное время восстановления, фактические потери*) с целевым (*утвержденные RTO и RPO*) и увидеть расхождения.

Например, если фактическое среднее время восстановления (*MTTR*) систематически превышает целевой *RTO*, GAP-анализ покажет, где и насколько компания отклоняется от плана. Это становится основой для корректировки стратегий восстановления и пересмотра бюджетов на защиту.

Сергей Левашов подчеркивает, что каждая компания решает сама, как именно управлять рисками остановки бизнес-процессов. Например, кто-то закладывает бюджет на выплаты вымогателям за разблокировку, а кто-то полностью игнорирует возможность реализации ИБ-угроз. В то же время активно развивается рынок киберстрахования и страховые компании уже выплачивают пострадавшим серьезные суммы.

BCP: от цифр к действиям

Расчетная стоимость простоя помогает понять масштаб риска, но сама по себе не обеспечивает непрерывность. Даже зная, что час недоступности сервисов обходится бизнесу в миллионы рублей, компания не восстановит продажи, обслуживание клиентов или производство автоматически. Финансовые показатели должны превращаться в конкретные сценарии действий — именно эту задачу решает план обеспечения непрерывности бизнеса (*Business Continuity Plan, BCP*).

BCP — это документ, в котором определены конкретные шаги, осуществление которых позволит компании продолжать выполнять ключевые задачи во время сбоя и быстро вернуться в норму после него.

По сути, это стратегическая инструкция, которая отвечает на главный вопрос: как мы будем работать, пока устраняем последствия проблемы?

Важно не путать BCP с планом аварийного восстановления (*Disaster Recovery Plan, DRP*).

Их различия принципиальны.



DRP VS BCP

ПЛАН АВАРИЙНОГО ВОССТАНОВЛЕНИЯ

ПЛАН НЕПРЕРЫВНОСТИ БИЗНЕСА

ГЛАВНЫЙ ВОПРОС

Как восстановить ИТ-инфраструктуру?

Как продолжить работу бизнеса?

ФОКУС

Технологии:
серверы, данные, сети

Процессы:
люди, поставщики, операции

РЕЗУЛЬТАТ

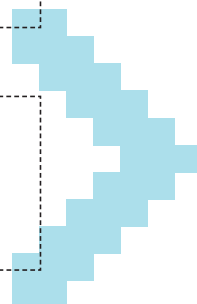
Восстанавливает системы до рабочего состояния

Обеспечивает работу бизнеса, пока системы восстанавливаются

МОМЕНТ ЗАПУСКА

Обычно запускается после инцидента

Запускается одновременно с инцидентом



Другими словами, DRP восстанавливает ИТ, а BCP сохраняет бизнес. Если серверы вышли из строя, DRP описывает, как их поднять. BCP описывает, как сотрудники продолжают обрабатывать заказы вручную, куда они переедут работать и как объяснить клиентам задержки.

Содержание плана варьируется от компании к компании, но ключевые элементы остаются неизменными:

- **кто, что и когда делает** (*ответственная команда, контакты*);
- **сценарии активации и работы** (*критерии активации BCP — например, если простой платежного шлюза превысил 10 минут; пошаговые и временные процедуры*);
- **ресурсы для работы в кризис** (*резервные офисы и поставщики*);
- **коммуникации** (*кто и в какие сроки информирует сотрудников, партнеров, клиентов, СМИ, регуляторов*).

Разработка BCP — это не разовое мероприятие, а непрерывный процесс, состоящий из пяти этапов:

- 1 Анализ.** Выполняется BIA и оцениваются риски. Результаты BIA определяют критичные процессы и их MTPD/RTO/RPO, а оценка рисков — угрозы (*кибератаки, отключения электричества, сбои поставщиков*) для этих процессов.
- 2 Разработка.** На основе анализа создаются стратегии восстановления: резервирование мощностей, ручные обходные пути, переезд на альтернативные площадки. Формируется документ BCP с перечнем всех процедур и списком ответственных.
- 3 Внедрение.** План доводится до всех сотрудников, команды



проходят обучение, вводятся регламенты, интегрирующие BCP в повседневные процессы.

- 4 Тестирование.** Проводятся учения: семинары, обсуждение сценариев за столом переговоров и полномасштабные симуляции с реальным переключением на резервные мощности. Тестирование выявляет слабые места плана.
- 5 Актуализация.** BCP — «живой» документ. Он пересматривается и обновляется при изменении бизнес-процессов, ИТ-архитектуры, ландшафта угроз или смене кадров.

Почему BCP обязателен: регуляторный контекст

О требованиях к количественной оценке рисков мы уже говорили выше в разделе о расчетах. Здесь же подчеркнем: для многих компаний BCP — не рекомендация, а обязанность. В первую очередь к BCP предъявляются требования в финансовой отрасли. Для банков это Приложение 5 к Положению Банка России № 242-П, которое устанавливает обязательные требования к непрерывности критических процессов: определение RTO/RPO для каждой системы, наличие и регулярное тестирование планов восстановления. Наряду с этим ЦБ планомерно развивает регуляторную базу в сфере операционной надежности, вводя новые требования к оценке зрелости BCP и переходя от формальной проверки документов к проверке их практической реализуемости.

Таким образом, BCP — это документ, который связывает количественную оценку рисков с конкретными управленческими решениями. На основе утвержденных RTO и RPO он определяет приоритеты восстановления, распределение ресурсов и зоны ответственности команд, обеспечивая предсказуемый выход из кризиса.



ЭКСПЕРТ

Аскар Мусаев,

эксперт
по непрерывности
бизнеса компании
«Инфосистемы Джет»



Самое сложное в построении работающей системы управления непрерывностью бизнеса — не расчеты и не документы, а согласования и честный диалог с бизнесом. В начале пути критичным кажется всё, но после проведения честного BIA остается десяток процессов, остановка которых неминуемо приведет к недопустимым потерям выручки, уходу ключевых клиентов или проблемам с регулятором.

Многие на практике пытаются закрыть этот вопрос резервированием всего, что только можно, но сталкиваются с опасным заблуждением: «У нас есть резервный ЦОД, значит, мы защищены». Непрерывность куда шире вопроса «Как быстро поднять ключевые системы?», потому что вопросы «А кто будет принимать решение о переключении в 3 часа ночи?», «Как сотрудники будут принимать заказы первое время?» и «Что мы скажем клиентам в первые полчаса?» не менее важны, и только комплексный подход делает компанию по-настоящему готовой к любой катастрофе и сбою.

Что же можно предпринять в первую очередь?

Я бы выделил эти простые шаги, с которых надо начать:

- Определить, что для компании является недопустимым ущербом.
- Выделить 8–10 процессов с недопустимым ущербом за кратчайшее время простоя.
- Зафиксировать для каждого из них MTPD, RTO и RPO в числовых значениях, а не в виде формулировки «как можно быстрее».
- Описать зависимости: люди, системы, площадки, подрядчики. Кстати, очень часто на данном этапе выясняется, что главный риск для процесса — увольнение инженера, знающего все нюансы работы, или находится поставщик, которому нет альтернативы.
- Взять один сценарий и провести по нему настоящие учения с участием топ-менеджмента.

После такой работы план начнет расти сам: учения покажут, чего в нем не хватает. И это будет гораздо продуктивнее, чем бесконечная разработка идеального документа. 📌



КРИЗИСНЫЙ ШТАБ

Задаёт курс и принимает ключевые решения во время инцидента



АНТИХРУПКОСТЬ

Стратегия, помогающая системе не только выдерживать сбои, но и становиться устойчивее после них

НЕПРЕРЫВНОСТЬ 2.0 НОВАЯ НАДЕЖДА



ХАРДЕНИНГ

Укрепляет инфраструктуру и сокращает количество возможностей для атаки



ОТКАЗООУСТОЙЧИВАЯ АРХИТЕКТУРА

Позволяет системе продолжать работу при отказе отдельных узлов благодаря наличию нескольких зон доступности (active-active/active-passive), как при геораспределении ЦОД



СИСТЕМЫ РЕЗЕРВНОГО КОПИРОВАНИЯ

Сохраняют данные для восстановления после сбоя или кибератаки



МОНИТОРИНГ/ НАБЛЮДАЕМОСТЬ

Помогают вовремя заметить отклонения и понять, что происходит с системой



ВСП

Определяет, как возобновить критичные бизнес-процессы во время сбоя или атаки



DRP

Определяет, как и в какой последовательности восстанавливать ИТ-инфраструктуру и ИС



ТЕСТИРОВАНИЯ

(tabletop-учения, пентесты, хаос-инжиниринг, тестовые восстановления ИС, проверка DRP)

Проверяют готовность людей и процессов к атаке или сбою



КИБЕРУСТОЙЧИВОСТЬ

Объединяет практики, процессы и технологии, которые позволяют бизнесу работать даже при атаке



БУНКЕР

Сохраняет доверенные резервные копии, которые дают возможность восстановиться даже при компрометации основной инфраструктуры

ИЗОЛИРОВАННЫЙ КОНТУР



ЦИТАДЕЛЬ

Безопасная среда с уже запущенными или подготовленными к запуску ИТ-системами для быстрого возвращения к работе после атаки

НИТЬ, ВЕДУЩАЯ К ВОССТАНОВЛЕНИЮ

КАК УСТРОЕН СОВРЕМЕННЫЙ DRP





АВТОР

**Александр
Шестопалов,**

консультант
по ИТ-аудиту компании
«Инфосистемы Джет»



АВТОР

**Федор
Момот,**

консультант
по ИТ-аудиту компании
«Инфосистемы Джет»



По нашему проектному опыту, сегодня лишь примерно в одной компании из двадцати существует полноценный план аварийного восстановления и только небольшой процент компаний из этого числа регулярно проверяют возможности его применения. Между тем любой серьезный сбой в ИТ-инфраструктуре влечет за собой не только технические проблемы, но и финансовые потери — из-за простоев, нарушения обязательств перед клиентами и репутационного ущерба. Объем убытков напрямую связан со скоростью возвращения ИТ-систем в рабочее состояние, которая зависит от того, как команда будет действовать в случае инцидента: хаотично или по заранее подготовленным и отработанным сценариям. А при кибератаке любое промедление и вовсе может стать фатальным.

Как продолжать взаимодействовать с клиентами, предоставлять услуги, проводить оплату и выполнять другие контрактные и социальные обязательства, если бизнес-системы и ИТ-инфраструктура «лежат» после инцидента? А ведь пока не восстановлена работа баз данных, приложений (*включая смежные системы*), каналов связи или корпоративных сервисов, полноценно возобновить деятельность компании невозможно.

Сегодня почти любой бизнес-процесс зависит от технологий. И стоимость простоя ИТ-систем в отдельных отраслях достигает миллионов долларов в час: для финансовых сервисов — 5–9 млн долл., для E-commerce-компаний — 2–4 млн долл. А на производстве последствия могут быть еще серьезнее: остановка технологических линий способна привести к срыву поставок, остановке отгрузок и приемки. В итоге — потеря репутации, уход клиентов и более печальные исходы.

За быстрое возвращение к работе ИТ-систем отвечает план аварийного восстановления (*Disaster Recovery Plan, DRP*) — это один из ключевых инструментов планирования непрерывности бизнеса (*Business Continuity Plan, BCP*). Оба плана взаимосвязаны, и их правильно организованная реализация обеспечивает выживание компании при значительном происшествии.

Если затраты на DRP меньше потенциальных потерь за два-три дня простоя, то это не расход, а страховка для бизнеса. Компании тратят миллионы на железо и лицензии, но экономят на разработке регламентов, хотя именно регламенты минимизируют время восстановления.

DRP и BCP не стоит смешивать — это разные документы. BCP описывает восстановление бизнес- и производственных процессов и ИТ-инфраструктуры обычно никак не касается. А DRP — это план восстановления информационных систем, то есть он целиком фокусируется на ИТ-составляющей бизнес-процесса.

Какие инциденты требуют запуска DRP

DR-план — это набор регламентов и сценариев, определяющих порядок восстановления ИТ-систем после серьезного инцидента. При этом важно понимать, что он охватывает не все технические сбои, которые могут затронуть инфраструктуру. На практике механизмы аварийного восстановления и отказоустойчивости нередко смешивают, хотя они решают разные задачи.

Например, выход из строя блока питания, отказ диска или контроллера в системе хранения данных, потеря канала связи или недоступность одного из узлов кластера высокой доступности (*High Availability, HA*) еще не означают необходимости запускать механизмы DRP.

Эти сценарии относятся к обеспечению высокой доступности. Задача HA заключается в том, чтобы локальный отказ отдельного компонента не привел к остановке сервисов. Если один из них

выходит из строя, его нагрузку принимает соседний. При отказе одного канала связи трафик автоматически переключается на резервный маршрут, а при сбое экземпляра приложения система оркестрации запускает новый. В идеале пользователь даже не замечает, что произошел какой-то сбой.

Disaster Recovery же начинается там, где возможностей отказоустойчивой архитектуры уже недостаточно. Когда автоматическое переключение не помогает, сервисы останавливаются, а для их восстановления требуется приглашать специалистов, принимать решения на высоком уровне и выполнять заранее подготовленный план. Именно в этом принципиальная разница.

Кто запускает DRP? В критической ситуации решение о запуске плана восстановления должен принимать CEO или лицо, указанное в DRP. Кратковременный простой, связанный с ручным переключением на резервный ЦОД, в таких условиях может обойтись компании дешевле, чем бездействие и ожидание того, что автоматические механизмы справятся с проблемой самостоятельно. Поэтому важно заранее определить список людей, принимающих решение.

Примеры сценариев, способных повлечь остановку сервисов и попадающих в область действия плана аварийного восстановления:

- потеря работоспособности площадки (из-за взрыва, пожара, потопа, обесточивания, аварийного отказа кондиционирования, аварийного отказа инженерных систем и т. д.);
- авария на линиях связи, в сети, нарушение корректной работы сети;
- авария на ключевом вычислительном или коммуникационном оборудовании площадки;
- отказ кластера без автоматического механизма резервирования (HA);

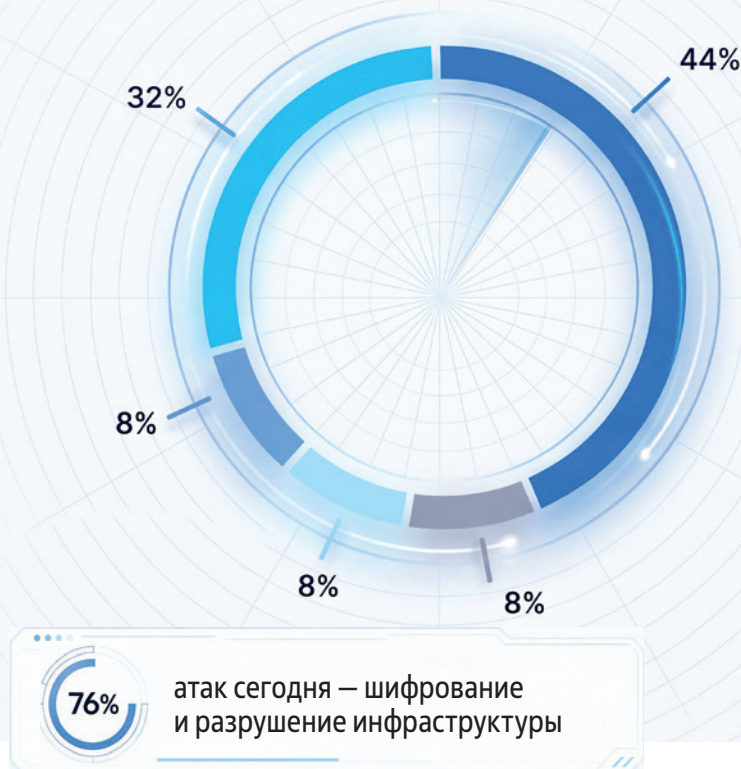
- заражение инфраструктуры вирусом-шифровальщиком, взлом, проникновение посторонних лиц в ЦОД;
- отказ ПО, на котором работает сервис (*баг, ошибка обновления, повреждение данных и т. д.*);
- отказ смежной ИС (*невозможность получить данные и, как следствие, остановка сервиса*);
- любая другая авария, регламентное решение которой выходит за пределы допустимых RTO и RPO, — например, отказ компонентов, не покрытых HA (*даже если это блок питания, но он один и сервер единственный*);
- нарушение балансировки нагрузки — неконтролируемое или по неясным причинам (*например, возможная DDoS-атака или отказ балансировщиков*).

DRP не применяется в следующих случаях:

- падение плеча автоматического HA-кластера active-active (*несколько узлов одновременно обслуживают нагрузку*), active-passive (*один узел работает, второй — находится в резерве и включается при отказе основного*);
- отказ компонентов оборудования, не влекущий остановку сервисов;
- отказ компонентов, приводящий к остановке сервиса, однако устранение проблемы укладывается в допустимые показатели RTO и RPO (*например, если вышел из строя единственный блок питания, а его замена занимает несколько минут*);
- нарушение балансировки нагрузки, не требующее переключения на резервную площадку;
- действия, выполняемые после переезда сервисов на резервную площадку: выяснение причин, восстановление работоспособности основной площадки, возврат сервисов обратно.

Действия в случаях локальных отказов должны быть описаны в инструкции ИТ-администратора.

ТОП киберугроз — 2025



Когда главным риском стала кибератака

Если раньше основными причинами запуска аварийного восстановления считались пожар в серверной, потеря питания или отказ оборудования, то в последние годы ими стали кибератаки. Причем их цели тоже изменились: кража информации как таковой теперь интересует преступников все реже.

По данным исследования Jet CSIRT, посвященного популярным тактикам и техникам нарушения киберустойчивости российских компаний, цель 76% всех атак — остановить бизнес. Для этого злоумышленники используют программы-вайперы (*вредоносное ПО для уничтожения данных*). Соответственно, меняется и роль резервной площадки — взломщики проникают и в ее инфраструктуру. Поэтому простое переключение на резервный ЦОД уже не гарантирует успешного восстановления.

Вместе с тем использование кибератак вынуждает менять и саму последовательность аварийного восстановления. Если при пожаре, отказе оборудования или другой физической аварии

главная задача — как можно быстрее вернуть систему в работу, то после взлома этого уже недостаточно. Прежде чем запускать сервисы, необходимо убедиться в том, что инфраструктура очищена от последствий компрометации и злоумышленник больше не имеет к ней доступа. Иными словами, восстановление после киберинцидента — это уже не возврат к состоянию «как было», а контролируемый процесс построения доверенной среды.

Сначала — лабораторная чистота

Восстановление после кибератаки начинается не с запуска сервисов, а с проверки так называемой лабораторной чистоты инфраструктуры, данных и систем. То есть, прежде чем возвращать системы в работу, необходимо убедиться в том, что вредоносное ПО полностью удалено, механизмы закрепления злоумышленника устранены, а резервные копии действительно безопасны для восстановления.

Удостоверившись в том, что данные не заражены, можно переходить ко второму этапу —

восстановлению сервисов в изолированном контуре. И только затем — постепенно возвращать системы в эксплуатацию.

Есть еще одно важное отличие. Последствия физической аварии, как правило, ограничены самим событием. Киберинцидент же может развиваться даже после его обнаружения, потому что преступники иногда месяцами находятся в инфраструктуре и закрепляются в ней, что увеличивает возможный масштаб компрометации и усложняет процесс восстановления. Пока компания анализирует ситуацию, злоумышленники продолжают перемещаться по инфраструктуре. Поэтому действовать приходится зачастую намного быстрее, чем при классической аварии, — ведь каждая потерянная минута увеличивает потенциальный ущерб.

Отсюда следует важный вывод: процедуры восстановления после кибератаки и после классической аварии — совершенно разные. Меняется все: от подготовки резервных копий до последовательности запуска сервисов и критериев готовности инфраструктуры к возвращению в эксплуатацию. Поэтому современные DR-планы все чаще разрабатываются с учетом того, что главная чрезвычайная ситуация для бизнеса — не отказ оборудования из-за технических сбоев и аварий, а компрометация инфраструктуры злоумышленниками.

DRP, который никогда не работал

Наличие DR-плана само по себе и готовность к восстановлению — далеко не одно и то же. Лишь немногие компании успешно проходят реальный инцидент. На практике часто оказывается, что под DR-планом понимается что угодно: набор инструкций от вендоров, несколько страниц в корпоративной базе знаний или таблица с контактами сотрудников на случай ЧП.

Одна из главных проблем заключается в том, что компании имеют расплывчатое представление о собственной инфраструктуре. За годы развития ИТ-ландшафт обрывает новыми системами, интеграциями и сервисами, а изменения в документацию вовремя не вносят. В результате в критический момент выясняется, что никто не может быстро ответить на простые вопросы: какой сервер за что отвечает, где находятся резервные копии, какие сервисы зависят друг от друга, кого необходимо подключить к восстановлению и что вообще нужно запускать в первую очередь.

Ситуацию усугубляет и то, что значительная часть критически важных знаний хранится не в документации, а в головах сотрудников. Пока все работает в штатном режиме, это редко приводит к проблемам. Однако во время серьезного инцидента внезапно оказывается, что:

- ключевой специалист находится в отпуске;
- архитектор уволился;
- сбой тестового сервера серьезно влияет на промышленную среду;
- многие зависимости между сервисами никогда не фиксировались должным образом.

Даже существующие DR-планы очень часто не проверяются на практике. А ведь DRP — это не PDF-файл и не набор инструкций в корпоративной базе знаний. Это навык команды восстанавливать инфраструктуру в условиях кризиса — **сегодня это фактически один из важнейших ИТ-процессов**. А любой навык требует закрепления — то есть регулярной практики.

Зрелый DR-план — это не только документ, но и регулярные учения, актуализация после изменений в инфраструктуре и постоянная проверка выполнимости каждого шага. Любое изменение архитектуры, внедрение нового сервиса или перенос системы на другую платформу могут сделать часть плана неактуальной. Поэтому даже развитая инфраструктура отказоустойчивости сама по себе не гарантирует готовности к восстановлению. Согласно данным исследования компании «Инфосистемы Джет» по оценке уровня зрелости ИТ-инфраструктуры российских компаний, около 60% предприятий используют локальные средства высокой доступности, 48% применяют глобальную кластеризацию и резервный ЦОД с автоматизацией переключения. При этом более четверти владельцев РЦОД не проводят DR-тесты, а значит, их DRP со временем теряют практическую эффективность.

Только тестирование позволяет увидеть объективную картину. Лишь оно показывает реальное время восстановления RTO, реальные зависимости между системами, реальные узкие места инфраструктуры и реальные проблемы коммуникации внутри команды. Более того, именно во время проверок обычно обнаруживаются

РЦОД ≠ эффективный DR



* По данным исследования компании «Инфосистемы Джет»: <https://jet.su/analytical-research/>

** Создание трех копий данных, на двух разных носителях, одной копии на удаленном или отчуждаемом носителе.

ошибки в последовательности действий, которая на бумаге выглядит абсолютно логичной.

На практике разрыв между плановым и реальным RTO может быть очень заметным. Согласно статистике компании «Инфосистемы Джет», среднее время восстановления критичных бизнес-процессов составляет 15,4 рабочего дня, а в крупных организациях может достигать 38 дней. В отдельных случаях компании не возвращаются к полноценной работе даже спустя год после инцидента.

Инфраструктура почти никогда не восстанавливается так, как это нарисовано на схемах. Даже при наличии подробного плана в документации процесс выглядит линейным и предсказуемым, однако во время тестирования выясняется, что:

- один сервис зависит от другого;
- запуск отдельного компонента требует дополнительных условий;
- часть критически важных связей нигде не зафиксирована.

Поэтому зрелый DRP — это всегда цикл: аудит, разработка плана, тестирование, корректировка, учения, актуализация и снова тестирование.

Приведем показательный пример из практики. Во время восстановления финансовой компании после масштабного инцидента выяснилось, что их DR-план не учитывал зависимость ключевых банковских систем от смежных компонентов, в том числе от инфраструктурных сервисов. В результате восстановление, которое

должно было занять около двух часов, растянулось почти на сутки.

Форматы проверок могут быть разными. Самый простой вариант — tabletop-учения, когда команда пошагово разбирает сценарий аварии и свои действия. Следующий уровень — вычитка плана по ролям. Это помогает обнаружить устаревшие сведения, неучтенные зависимости и ошибки в распределении ответственности.

Наиболее приближенным к реальности сценарием является тестовое восстановление в отдельной среде, где команда может проверить работоспособность плана без риска для продуктивной инфраструктуры. Для бизнес-критичных систем такие проверки желательно проводить не реже одного раза в полгода.

Бутылочное горлышко аварийного восстановления

Согласно теории управления процессами, бутылочное горлышко — это участок, который ограничивает скорость работы всей системы. Когда речь заходит о DRP, основное внимание обычно уделяют технологиям, однако практика показывает, что узкое место в процессе любого восстановления создают не особенности инфраструктуры, а люди. Именно от их решений, координации действий и скорости реакции зависит, насколько быстро компания сможет вернуться к работе.

С ростом числа кибератак, когда возвращение систем к работе перестало быть исключительно внутренней задачей ИТ и превратилось в задачу бизнеса, круг участников процесса восстановления расширился.

Теперь, помимо ИТ-специалистов, в него вовлекаются руководители компании, начальники профильных подразделений, специалисты по ИБ и другие заинтересованные стороны. В ряде случаев именно высшее руководство должно принять решение о временной остановке систем, чтобы не допустить еще большего ущерба.

По этой причине в зрелых организациях еще до возникновения инцидента заранее формируется кризисный штаб и распределяются роли всех участников восстановления. В DR-плане должно быть четко определено, кто принимает решение о запуске аварийного режима, кто отвечает за восстановление инфраструктуры, кто

координирует работу команд и кто взаимодействует с руководством и бизнесом.

Во время кризиса люди не должны думать, что делать. Они должны выполнять заранее отработанные роли. Без такой подготовки даже идеально написанный DRP — бесполезный документ.

Универсального рецепта не существует

После знакомства с принципами аварийного восстановления у многих может возникнуть соблазн найти универсальный шаблон DR-плана и адаптировать его под свои задачи. Тут важно понимать, что DRP, подходящего для всех компаний, не существует.

Сценарий восстановления всегда определяется особенностями конкретной компании: ИТ-архитектурой, перечнем критически важных сервисов, требованиями к непрерывности бизнеса, в том числе регуляторными, и допустимым уровнем риска. Поэтому каждая организация выстраивает план с учетом собственных процессов, технологий и приоритетов.

Более того, внутри одной организации не бывает единого сценария восстановления для всех систем. Каждая критичная для бизнеса система имеет собственные зависимости, приоритеты и порядок запуска. Общий DRP должен включать множество DR-планов — для каждой из систем, а также очередность их восстановления и условия, при которых команда переходит к следующему этапу.

Это особенно важно, потому что во время реального инцидента ресурсы всегда ограничены. Времени мало, часть специалистов может быть недоступна, а выполнять все работы одновременно невозможно. Если приоритеты не определены заранее, команда начинает восстанавливать те системы, с которыми проще или привычнее работать, а не те, от которых непрерывность бизнеса зависит в первую очередь.

В конечном итоге качество DR-плана определяется не объемом документации и не количеством схем. Единственный универсальный критерий остается неизменным: если план ни разу не проверяли на практике, его не существует.

Типовая очередность запуска информационных систем:

сначала
опорная сеть

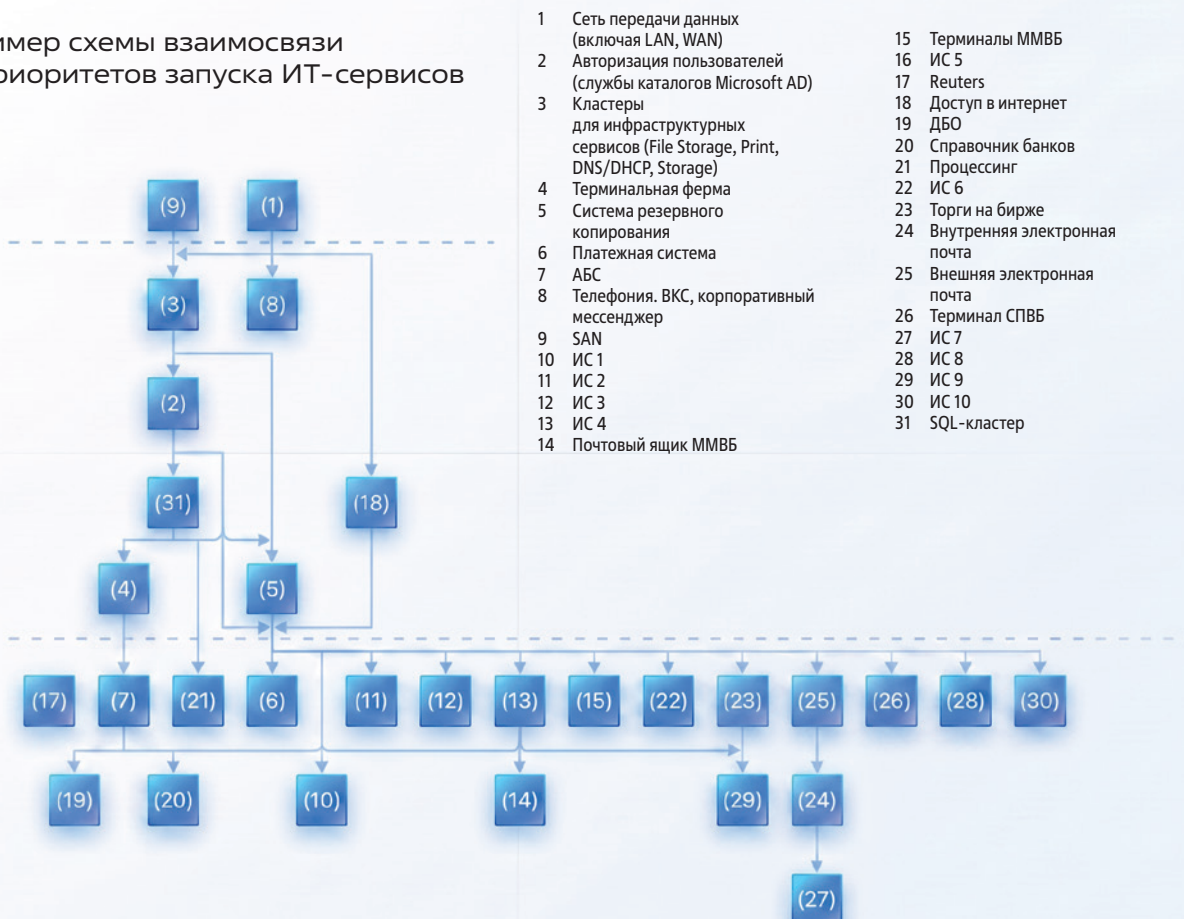


затем опорная
инфраструктура



в конце ИТ-сервисы в заранее
определенной последовательности

Пример схемы взаимосвязи
и приоритетов запуска ИТ-сервисов



Что должно быть в DRP

Матрица ролей:

- кто принимает решение о запуске восстановления;
- кто отвечает за инфраструктуру;
- кто отвечает за резервное копирование;
- кто взаимодействует с ИБ;
- кто выполняет шаги по восстановлению систем.

Пошаговые инструкции:

- порядок выполнения технологических шагов;

- ориентировочные временные интервалы;
- приоритеты выполнения операций;
- критерии перехода между шагами DRP;
- зависимости между операциями;
- проверки успешности выполнения восстановления систем.

Матрица коммуникаций:

- кого оповещать и в каком порядке;
- резервные контакты;
- замещающие сотрудники. 📞



САМОПРОВЕРКА

ГОТОВНОСТИ КОМПАНИИ К ВОССТАНОВЛЕНИЮ ПОСЛЕ ЧС

1. Существует ли утвержденный и актуальный DR-план с инструкциями по восстановлению информационных систем?
☐ ДА ☐ НЕТ ☐ ЧАСТИЧНО
2. Определены ли критичные информационные системы, без которых бизнес не сможет работать уже в первые минуты после аварии?
☐ ДА ☐ НЕТ ☐ ЧАСТИЧНО
3. Согласованы ли с бизнесом и ИТ максимально допустимое время восстановления (*RTO*) и допустимый объем потери данных (*RPO*) для каждой критичной системы?
☐ ДА ☐ НЕТ ☐ ЧАСТИЧНО
4. Определена ли и согласована с ИТ, ИБ и бизнесом очередность восстановления систем с учетом зависимостей между ними? Другими словами, существует ли план координатора аварии?
☐ ДА ☐ НЕТ ☐ ЧАСТИЧНО
5. Сможет ли команда получить DR-план, контакты и инструкции при недоступности корпоративной сети, почты, файловых ресурсов и системы управления документами?
☐ ДА ☐ НЕТ ☐ ЧАСТИЧНО
6. Определено ли конкретное должностное лицо, имеющее право объявить аварийный режим и запустить DR-план (*например, CEO*)?
☐ ДА ☐ НЕТ ☐ ЧАСТИЧНО
7. Установлены ли в компании измеримые критерии, в соответствии с которыми обычный инцидент признается чрезвычайной ситуацией и запускается DR-план?
☐ ДА ☐ НЕТ ☐ ЧАСТИЧНО
8. Назначены ли ответственные за восстановление систем и их заместители на случай отпуска, болезни, увольнения и других причин недоступности основных специалистов?
☐ ДА ☐ НЕТ ☐ ЧАСТИЧНО
9. Существует ли актуальный список аварийных контактов сотрудников, подрядчиков, операторов связи, ЦОД и поставщиков?
☐ ДА ☐ НЕТ ☐ ЧАСТИЧНО
10. Существуют ли альтернативные сценарии восстановления на случай недоступности резервной площадки, основных резервных копий или штатного способа восстановления?
☐ ДА ☐ НЕТ ☐ ЧАСТИЧНО



11. Предусмотрен ли отдельный сценарий восстановления после кибератаки, отличающийся от сценариев технического отказа, пожара или потери ЦОД?

☐ ДА ☐ НЕТ ☐ ЧАСТИЧНО

12. Определено ли, кто и по каким критериям подтверждает чистоту инфраструктуры и резервных копий после кибератаки и можно ли начать восстановление системы в изолированном доверенном контуре?

☐ ДА ☐ НЕТ ☐ ЧАСТИЧНО

13. Определены ли проверяемые критерии успешного восстановления каждой системы, включая подтверждение ее работоспособности владельцем бизнес-процесса?

☐ ДА ☐ НЕТ ☐ ЧАСТИЧНО

14. Есть ли резервные копии, которые нельзя удалить или зашифровать с помощью скопрометированных административных учетных записей основной инфраструктуры?

☐ ДА ☐ НЕТ ☐ ЧАСТИЧНО

15. Используется ли для хранения резервных копий принцип «3-2-1»?

☐ ДА ☐ НЕТ ☐ ЧАСТИЧНО

16. Может ли резервная площадка обеспечить работу критичных систем под реальной производственной нагрузкой?

☐ ДА ☐ НЕТ ☐ ЧАСТИЧНО

17. Разделены ли основная и резервная среды так, чтобы злонамеренное использование единой административной учетной записи и домена управления, а также ошибка или атака не могли вывести из строя одновременно обе площадки и резервные копии?

☐ ДА ☐ НЕТ ☐ ЧАСТИЧНО

18. Сохранится ли доступ к журналам, мониторингу и средствам диагностики при недоступности основной площадки или доменной инфраструктуры?

☐ ДА ☐ НЕТ ☐ ЧАСТИЧНО

19. Проверены ли сценарии отказа критичных внешних сервисов и закреплены ли в договорах с поставщиками сроки реакции, порядок аварийной эскалации и обязательства по восстановлению?

☐ ДА ☐ НЕТ ☐ ЧАСТИЧНО

20. Проводилось ли за последние шесть месяцев практическое восстановление критичных систем целиком (*не отдельных компонентов*), подтвердившее достижимость установленных RTO, RPO и критериев успешного восстановления?

☐ ДА ☐ НЕТ ☐ ЧАСТИЧНО

21. Проводятся ли учения с участием ИТ, ИБ, руководства и владельцев бизнес-процессов и актуализируется ли DR-план после тестов, изменений инфраструктуры и реальных аварий?

☐ ДА ☐ НЕТ ☐ ЧАСТИЧНО

22. Известна ли стоимость часа простоя критичных информационных систем (*финансовые, репутационные и другие потери*)?

☐ ДА ☐ НЕТ ☐ ЧАСТИЧНО

РЕЗУЛЬТАТЫ:

- **5 и более ответов «Нет»** — признак существенных пробелов в аварийном восстановлении.
- **Большое количество ответов «Частично»** — сигнал о том, что готовность компании пока нельзя считать полностью подтвержденной.
- **Отсутствие практических восстановлений и учений** — главный маркер того, что DR-план существует скорее как бюрократический документ, а не рабочий инструмент.



СТАЛЬНАЯ ЗАКАЛКА

КАК ХАРДЕНИНГ
УСЛОЖНЯЕТ ПУТЬ
КИБЕРПРЕСТУПНИКОВ





ЭКСПЕРТ

Антон Шипулин,

руководитель
отдела комплексных
проектов компании
«Инфосистемы Джет»



ЭКСПЕРТ

Игорь Шконда,

руководитель
направления
систем резервного
копирования компании
«Инфосистемы Джет»



ЭКСПЕРТ

Дмитрий Горохов,

директор департамента
виртуализации и
контейнеризации
компании
«Инфосистемы Джет»



ЭКСПЕРТ

Антон Голощапов,

руководитель
направления
инфраструктурных
сервисов Linux
компании
«Инфосистемы Джет»

Киберпреступники больше не ограничиваются выведением из строя отдельных систем. Все чаще они стараются лишить компанию самой возможности восстановиться. Взломщики разбираются в работе систем резервного копирования и популярного программного обеспечения, например Microsoft и VMware (платформы для виртуализации). Под ударом оказываются учетные записи, серверы, системы управления и бэкапы. Поэтому защита требует укрепления инфраструктуры на каждом уровне — именно эту задачу решает харденинг.

Цена разрушительных инцидентов измеряется не только потерей данных, но и простоем ключевых процессов. Например, в июле 2025 года хакерская атака на «Аэрофлот» привела к сбою информационных систем, задержкам и массовой отмене рейсов. На следующий день проблемы возникли у аптечной группы «Неофарм»: часть аптек сетей «Столички» и «Неофарм» приостановили работу, клиентам стали недоступны заказы лекарств и привилегии программы лояльности. Похожий сценарий пережил бренд 12 Storeez: после атаки временно перестали работать сайт и приложение, возникли сбои на кассах, а нарушения в работе магазинов продолжались два дня. Компания оценила совокупный ущерб примерно в 48 млн руб.

Не существует универсальной технологии, которая способна предотвратить подобные риски. Антивирус и системы мониторинга помогают обнаруживать и блокировать угрозы, резервные копии дают основу для восстановления, а харденинг — процесс усиления безопасности информационных систем — сокращает поверхность атаки и ограничивает возможности злоумышленника, если ему все же удалось проникнуть внутрь инфраструктуры. Харденинг стоит рассматривать не как замену другим средствам защиты, а как один из базовых элементов киберустойчивости и непрерывности бизнеса.

Безопасность не надстраивается, а встраивается

Харденинг — это системная работа с конфигурациями, правами доступа и архитектурой ИТ-систем. Одна из распространенных ошибок — воспринимать безопасность как отдельный слой, который можно добавить поверх уже построенной инфраструктуры. Однако, если базовые архитектурные решения изначально создают лишние точки входа или дают слишком широкие полномочия, настройки безопасности не помогут.

Антон Шипулин

«Харденинг — это не панацея, а только часть защиты. Если система плохо спроектирована, плохо настроена или плохо реализована, одними настройками безопасности проблему не решить. Поэтому мы всегда говорим заказчикам о том, что харденинг нужно рассматривать вместе с архитектурой. Он эффективен, если созданы условия, при которых злоумышленник, даже попав внутрь сети, не сможет быстро получить привилегированные права и нанести критический урон компании».

Усиление защиты основной ИТ-инфраструктуры — часть комплексного подхода «Непрерывность 2.0» компании «Инфосистемы Джет». Задача харденинга не в том, чтобы добиться абсолютной неуязвимости, а в том, чтобы усложнить действия злоумышленника и прервать цепочку атаки, а также сделать происходящее в инфраструктуре более прозрачным для мониторинга и быстрого реагирования на события.

Для этого харденинг должен охватывать все ключевые слои — от физического оборудования,

сети передачи данных, операционных систем (ОС) и служб каталогов до систем виртуализации, резервного копирования и системного ПО. Многие компании ошибочно рассматривают харденинг как задачу усиления безопасности одного конкретного компонента, который считают наиболее уязвимым, но на практике защищать нужно всю цепочку. И каждое ее звено требует специфических мер. Главное, что харденинг — не разовое мероприятие, это постоянный процесс, он должен стать нормой и правилом при эксплуатации ИТ-инфраструктуры наряду с установкой обновлений и патчей.

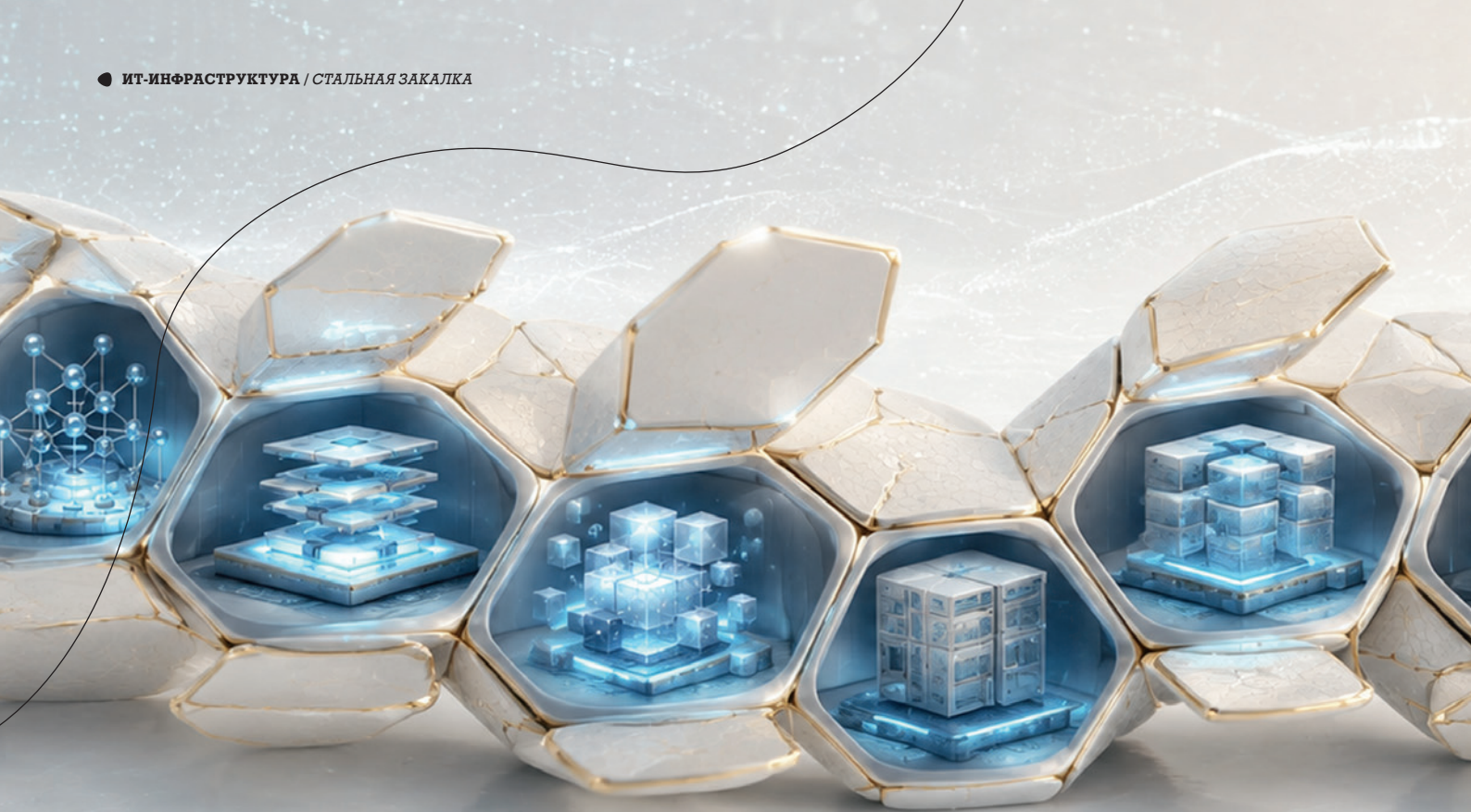
Харденинг платформ виртуализации

Виртуализация пронизывает практически все слои ИТ-инфраструктуры, поэтому такой среде следует уделить отдельное внимание: компрометация контура управления может открыть злоумышленнику доступ сразу ко множеству виртуальных машин и сервисов. Здесь основные риски зачастую связаны не со спецификой самой платформы виртуализации, а с тем, насколько защищен административный доступ к ней.

Дмитрий Горохов

«Отсутствие публичных кейсов взлома российских платформ виртуализации не означает отсутствия угроз. Основные риски сегодня связаны с угоном учетных данных администраторов и атаками на гипервизоры, поэтому мы рекомендуем начинать с простых, но эффективных действий: внедрения многофакторной аутентификации (2FA), ограничения доступа к сети управления и регулярного обновления компонентов».

Эксперт предупреждает, что в первую очередь взламывают популярные решения, такие как VMware, поэтому именно они требуют наиболее тщательной настройки безопасности и регулярного аудита.



Если вы на VMware

Держим в уме



Наличие доступа к командной строке ESXi-сервера — прямая возможность для атаки



Аномалии по дисковой активности на виртуальных дисках VM / датасторах



Массовое выключение VM на гипервизоре для шифрования/порчи файлов VM (vmdk)

Делаем



Отключить SSH-доступ к гипервизору



Не выставлять интерфейсы управления напрямую в интернет, изолировать сеть управления



Использовать RBAC, следить за членством в доменных группах



Собирать и анализировать логи с гипервизоров/платформы



Установить актуальные обновления



Использовать лучшие практики по защите:

- VMware Security Configuration Guide (Hardening Guide)
- STIG

Платформа виртуализации состоит из двух основных программных слоев:

- 1 **гипервизор** (*исполнительный слой*), на котором непосредственно запускаются виртуальные машины;
- 2 **система централизованного управления** (*управляющий слой*), которая объединяет гипервизоры в кластеры, отвечает за интеграцию со службами каталогов, ролевую модель доступа и распространение настроек.

Компрометация любого из этих слоев означает потерю контроля над всей виртуальной инфраструктурой. Харденинг каждого слоя мешает атакующему «перепрыгнуть» с одного уровня на другой и позволяет компании сохранить контроль над виртуальной инфраструктурой.

Рекомендации по защите системы централизованного управления:

- ограничить доступ к сети управления;
- не предоставлять доступ к системе управления из сети Интернет;
- установить корпоративные сертификаты безопасности;
- интегрировать со службой каталогов по безопасному протоколу (*LDAPS*) или не интегрировать совсем;
- использовать двухфакторную аутентификацию;
- настроить тайм-ауты сессий;
- настроить сбор и анализ логов.

Рекомендации по защите гипервизора:

- ограничить доступ к гипервизору (*настройки SSH, изоляция сети управления*);

- не устанавливать сторонние пакеты;
- настроить пароль для загрузчика;
- регулярно устанавливать обновления от вендора.

Дмитрий Горохов отмечает, что платформы виртуализации — это не основной источник проблем. Чаще всего инфраструктуру ломают изнутри: злоумышленники просачиваются через службы каталогов и дальше уже шифруют данные внутри виртуальных серверов. Поэтому особенно важно предотвратить распространение зловредного кода и проникновение в другие виртуальные серверы. Для этого необходимо ограничить взаимодействие между виртуальными серверами с помощью микросегментации.

Дмитрий Горохов

«В основе микросегментации лежит распределенный файрвол, который применяет политики безопасности непосредственно на уровне виртуального сетевого интерфейса виртуальной машины и ограничивает взаимодействие виртуальных серверов в пределах одной сети. Мы как-то строили VDI (инфраструктуру виртуальных рабочих столов) на 14 тыс. рабочих мест. Представьте себе потенциальную поверхность атаки! Без микросегментации одна зараженная ВМ моментально могла заразить остальные в пределах одного большого сетевого сегмента. Современная информационная безопасность в виртуальной инфраструктуре без микросегментации просто немыслима».

Отдельного внимания заслуживает сеть взаимодействия с системами хранения данных: например, при использовании iSCSI (*протокола подключения к СХД по IP-сети*) ее также необходимо сегментировать и защищать от несанкционированного доступа. Важно разделять задачи отказо- и киберустойчивости. Репликация помогает сохранить доступность сервисов при сбоях, но не защищает, если преступник контролирует административные системы.

Харденинг СРК

Системы резервного копирования сегодня под прицелом киберпреступников. Они изучают

архитектуру СРК, учетные записи и политики хранения, чтобы удалить бэкапы еще до атаки. А вместе с ними — и последнюю надежду компании на восстановление ИТ-инфраструктуры.

Игорь Шконда

«Когда все идет не по плану, ни отказоустойчивые кластеры, ни репликация уже не спасают — у вас остается только резервная копия. В этот момент возникает вопрос: получится ли вообще восстановиться? Мы исходим из того, что нужно заранее готовиться к сценарию, в котором часть защиты уже не сработала, а часть инфраструктуры взломана. Задача СРК — пережить этот момент, даже если домен или административные учетные записи захвачены».

Главная ошибка — держать СРК в том же контуре, что и основную среду, используя те же учетные записи. Современный подход требует изоляции. На практике это выглядит как создание двух контуров СРК: рабочего (*в продуктивной инфраструктуре*) и максимально изолированного, который в компании «Инфосистемы Джет» называют «Бункером». Его основная задача — получить и сохранить доверенные резервные копии, даже если все вокруг разрушено.

Рекомендации по харденингу системы резервного копирования

1 Внедряйте минимальные привилегии и ролевую модель

Используйте фиксированный набор ролей (*например, как в «Кибербэкапе»*), предусмотрев отдельную роль для специалистов ИБ с правами только на просмотр. Помните: если агент СРК на Linux работает из-под root, компрометация ОС автоматически ведет к компрометации всей системы — поэтому одновременно усиливайте и ПО СРК, и саму операционную систему.

2 Изолируйте СРК от домена

Интеграция со службами каталога (*например, MS AD, FreeIPA*) упрощает управление, но создает риск: при компрометации домена атакующий получает доступ к компонентам СРК, в частности к ПО.

Поэтому выделите второй, максимально изолированный домен с собственными учетными записями, строгой парольной политикой, полностью независимый от основной службы каталогов. Или используйте локальные учетные записи в небольших инфраструктурах!

3 Используйте неизменяемые хранилища

Применяйте WORM-хранилища или Object Lock на S3 — механизмы, которые защищают резервные копии от удаления и перезаписи в течение заданного срока. Выбирайте режим в зависимости от требований: Governance (*параметры срока хранения можно скорректировать специальной учетной записью*) или Compliance (*изменение невозможно даже с правами администратора*). Сроки хранения задавайте заранее: изменить их задним числом нельзя. Для ленточных библиотек также можно использовать WORM-ленты — в таком случае их необязательно отчуждать из ленточной библиотеки.

4 Шифруйте резервные копии и храните ключи отдельно

Включайте шифрование (*AES*) в настройках задания или через командную строку (*CLI*). Никогда не храните ключи ни в системе управления, ни в самих копиях: их потеря делает восстановление невозможным.

5 Сегментируйте сеть и используйте безопасные протоколы

Управляющий сервер, медиасерверы и агенты резервного копирования требуют открытия портов, но открывайте только реально используемые соединения. Размещайте СРК в отдельном VLAN с жесткими правилами межсетевого экрана. Отключайте неиспользуемые порты и не используйте небезопасные протоколы (*telnet, ftp и т. д.*) для управления СРК и хранения резервных копий.

6 Регулярно проверяйте целостность и восстанавливаемость данных

Выполняйте CRC-проверки (*контрольные суммы*) для подтверждения

ГЛАВНАЯ ОШИБКА — ДЕРЖАТЬ СРК В ТОМ ЖЕ КОНТУРЕ, ЧТО И ОСНОВНУЮ СРЕДУ, ИСПОЛЬЗУЯ ТЕ ЖЕ УЧЕТНЫЕ ЗАПИСИ. СОВРЕМЕННЫЙ ПОДХОД ТРЕБУЕТ ИЗОЛЯЦИИ

целостности данных — эту ресурсоемкую операцию выносите в отдельные планы. Для виртуальных машин проводите тестовый запуск из бэкапа с проверкой отклика (*VMware Tools / Hyper-V Heartbeat*).

7 Включайте активную защиту от шифровальщиков

На агентах и медиасерверах активируйте встроенные модули (*например, Active Protection, Ransomware Protection*), которые в реальном времени отслеживают аномальную активность (*массовое шифрование, нетипичную нагрузку*) и могут автоматически остановить подозрительный процесс, оповестив при этом администратора СРК.

8 Настройте аудит и мониторинг событий

Ведите журнал ключевых событий (*запуск заданий, удаление копий, изменения конфигурации*). Настройте передачу этих событий во внешние SIEM-системы через протокол syslog (*в том числе в формате CEF*) — это необходимо для расследования инцидентов.

Харденинг СРК — это комплексная оперативная мера, включающая сегментацию компонентов СРК, минимизацию привилегий, шифрование и неизменяемость хранилищ. Однако решающую роль играют регулярные процессы: проверки

копий и тестовые восстановления. Но даже лучшие настройки не дают полной гарантии, если система остается в общем контуре. Полную устойчивость способен обеспечить только полностью изолированный «Бункер». Именно эта резервная копия становится последним «выжившим», когда основная инфраструктура скомпрометирована.

Харденинг ОС и служб каталогов

Харденинг операционных систем и служб каталогов — это последняя линия обороны. Злоумышленники проникают в системные сервисы, когда остальные рубежи уже пройдены.

Антон Голощапов

«Харденинг — это подход, основанный на культуре проактивной защиты и принципе минимализма. Если компонент не нужен системе, его следует отключить. Если пользователю не требуются дополнительные права, их не нужно выдавать. Обязательным элементом является внедрение мандатного контроля доступа (например, SELinux, AppArmor или PARSEC) как дополнительного рубежа, ограничивающего действия даже привилегированных процессов и администраторов. Его настройка действительно требует времени и экспертизы, но отключать этот механизм ради упрощения

администрирования — распространенная ошибка, которая заметно ослабляет защиту системы».

Для харденинга операционных систем Linux эксперт рекомендует:

- настроить права на точки монтирования и отключать автоматическое монтирование устройств;
- включить журналирование событий;
- настроить авторизацию для однопользовательского режима;
- отключить службы и сервисы, которые не используются;
- настроить параметры сети и отключать неиспользуемые протоколы;
- настроить контроль целостности;
- регулярно обновлять версии ОС;
- настроить доступ, аутентификацию и авторизацию;
- ограничить права на основные конфигурационные файлы.

Службы каталогов — Active Directory (AD) или ее альтернативы на базе Samba и FreeIPA — требуют отдельного внимания, поскольку через них злоумышленник может получить дополнительные привилегии и перемещаться по инфраструктуре. Здесь применяются строгие парольные политики и ролевая модель, меняются административные пароли после первичной настройки, отключаются устаревшие протоколы и анонимный bind LDAP (операция аутентификации пользователя в службе каталогов), а обычный LDAP (протокол доступа к службе каталогов) заменяется на LDAPS (защищенная версия с шифрованием соединения).

При этом универсального набора настроек для всех сред не существует. Требования

зависят от конкретной платформы и ее реализации. Поэтому изменения сначала проверяют на стенде, максимально близком к среде заказчика, и только после тестирования переносят в продуктив.

Антон Голощапов

«Харденинг — это отчасти творческий процесс, ведь технологии взлома и техники атаки зачастую универсальны для различных операционных систем, но при этом конкретным сервисам присущи уникальные нюансы. Решение на базе Samba имеет одни недостатки, а на базе FreeIPA — совершенно другие. Поэтому мы сначала обязательно занимаемся стендированием: создаем копию среды заказчика, выдвигаем требования, отработываем их в тестовой среде и только потом переносим в продуктив. Если в скоуп добавляются новые ОС, мы повторяем процесс индивидуально для каждого компонента».

Эксперт также отмечает, что на уровне оборудования и операционных систем харденинг начинается с соблюдения баланса между безопасностью и функциональностью. Если максимально закрутить «гайки» и внедрять все требования ИБ, сервисы будут хорошо защищены, но с большой вероятностью перестанут работать.

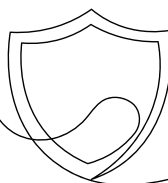
Гонка без финиша

Эксперты подчеркивают, что харденинг — это процесс, он требует постоянной работы: инфраструктура меняется, появляются новые системы и сервисы, обновляются конфигурации и права доступа. Поэтому настройки безопасности необходимо регулярно пересматривать и проверять, в том числе с помощью пентестов и тестовых стендов.

Антон Голощапов добавляет, что для системного подхода к харденингу необходимо регулярно проводить аудит и мониторинг угроз. Харденинг бесполезен, если вы не видите попыток взлома.

Отслеживать эволюцию угроз и обновлять методы защиты помогают несколько авторитетных источников:

- **MITRE ATT&CK** (attack.mitre.org) — глобальная база знаний, систематизирующая тактики, техники и процедуры,



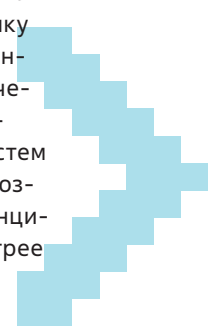
ХАРДЕНИНГ — ЭТО ПРОЦЕСС, ОН ТРЕБУЕТ ПОСТОЯННОЙ РАБОТЫ: НАСТРОЙКИ БЕЗОПАСНОСТИ НЕОБХОДИМО РЕГУЛЯРНО ПЕРЕСМАТРИВАТЬ И ПРОВЕРЯТЬ, В ТОМ ЧИСЛЕ С ПОМОЩЬЮ ПЕНТЕСТОВ И ТЕСТОВЫХ СТЕНДОВ

- которые используют злоумышленники на всех этапах атаки;
- **MITRE D3FEND** (d3fend.mitre.org) — каталог контрмер и защитных техник для каждой атаки;
 - **Банк данных угроз безопасности информации ФСТЭК** (bdu.fstec.ru) — российский государственный реестр угроз и уязвимостей, обязательный к применению при построении моделей угроз для государственных информационных систем, объектов КИИ и систем персональных данных;
 - **CIS Benchmarks** (cisecurity.org) — международный стандарт безопасной конфигурации, который переводит общие принципы харденинга в конкретные, проверяемые настройки для операционных систем, СУБД, облачных платформ и сетевого оборудования.

При этом эксперты компании «Инфосистемы Джет» подчеркивают, что оценивать на уязвимость важно не отдельные компоненты, а всю возможную цепочку атаки — от этапа разведки инфраструктуры до действий по целям (*к примеру, критичным системам и резервным копиям*).

Один из вариантов такой комплексной проверки — «Месячник харденинга», который объединяет мероприятия по защите ИТ-инфраструктуры от проникновения, развития атаки и ее возможных последствий.

Харденинг не исключает саму возможность атаки, но на практике усложняет злоумышленнику путь внутри инфраструктуры и снижает потенциальный масштаб инцидента. В конечном счете в этом и заключается его роль в обеспечении непрерывности бизнеса: чем меньше систем окажется скомпрометировано, тем больше возможностей у компании в случае реального инцидента сохранить критичные процессы и быстрее восстановиться.



Оперативные действия:

МЕСЯЧНИК ХАРДЕНИНГА

ДЛЯ ЗАЩИТЫ
ОТ ПРОНИКНОВЕНИЯ



- Поиск утечек легитимных аутентификационных данных
- Сканирование сетевого периметра на уязвимости (в том числе мисконфигурации)
- Анализ безопасности способов удаленного подключения к инфраструктуре (в том числе подрядных организаций)
- Сканирование сетевого периметра подрядчиков на уязвимости (в том числе мисконфигурации)

ДЛЯ ЗАЩИТЫ
ОТ РАЗВИТИЯ АТАКИ



- Анализ сетевых доступов (ACL) на предмет широких разрешающих правил сетевого доступа
- Аудит безопасности корпоративного домена
- Анализ NTDS.dit по радужным таблицам на предмет нестойких паролей
- Анализ безопасности реализованных практик администрирования
- Поиск сетевых ресурсов с неограниченным доступом

ДЛЯ ЗАЩИТЫ
ОТ ВОЗМОЖНЫХ
ПОСЛЕДСТВИЙ



- Анализ безопасности контура системы резервного копирования
- Уточнение приоритета восстановления с учетом критичности бизнес-процессов
- Тестовое восстановление из резервных копий для оценки времени восстановления
- Разработка кризис-менеджмент-плана и сценариев реагирования на кризисные ситуации
- Проработка и тестирование (tabletop) плана кризисного реагирования

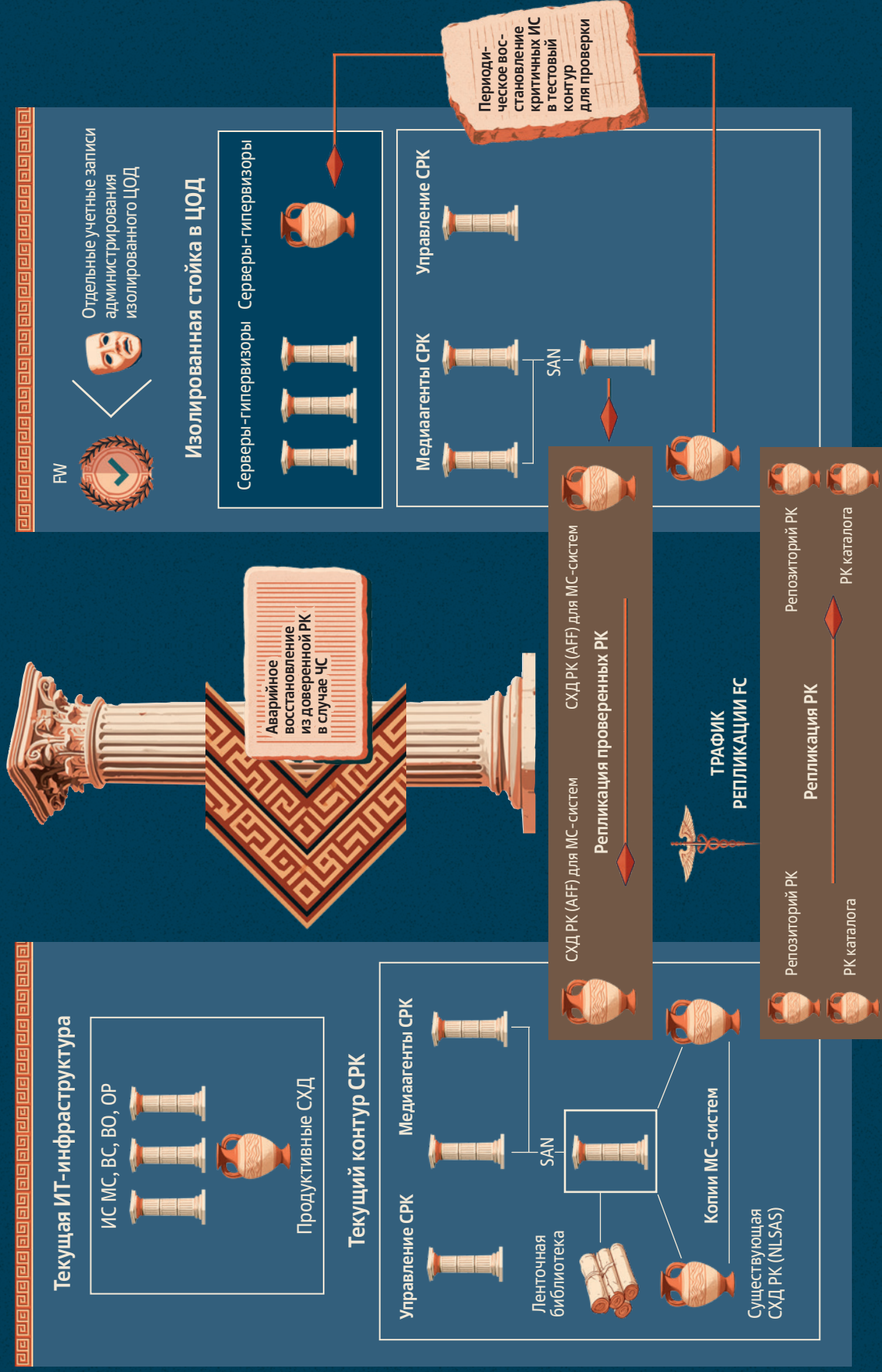
Определение профиля возможных техник, эмуляция отдельных сценариев (C2 Connects, WMI Backdoor, LSASS Dump, Recon Activity, Scheduled Task Creation и др.)

Compromise Assessment (выявление следов компрометации инфраструктуры)

Тестирование на проникновение (фишинг, компрометация корпоративного домена, системы резервного копирования, компрометация подрядчика) ●

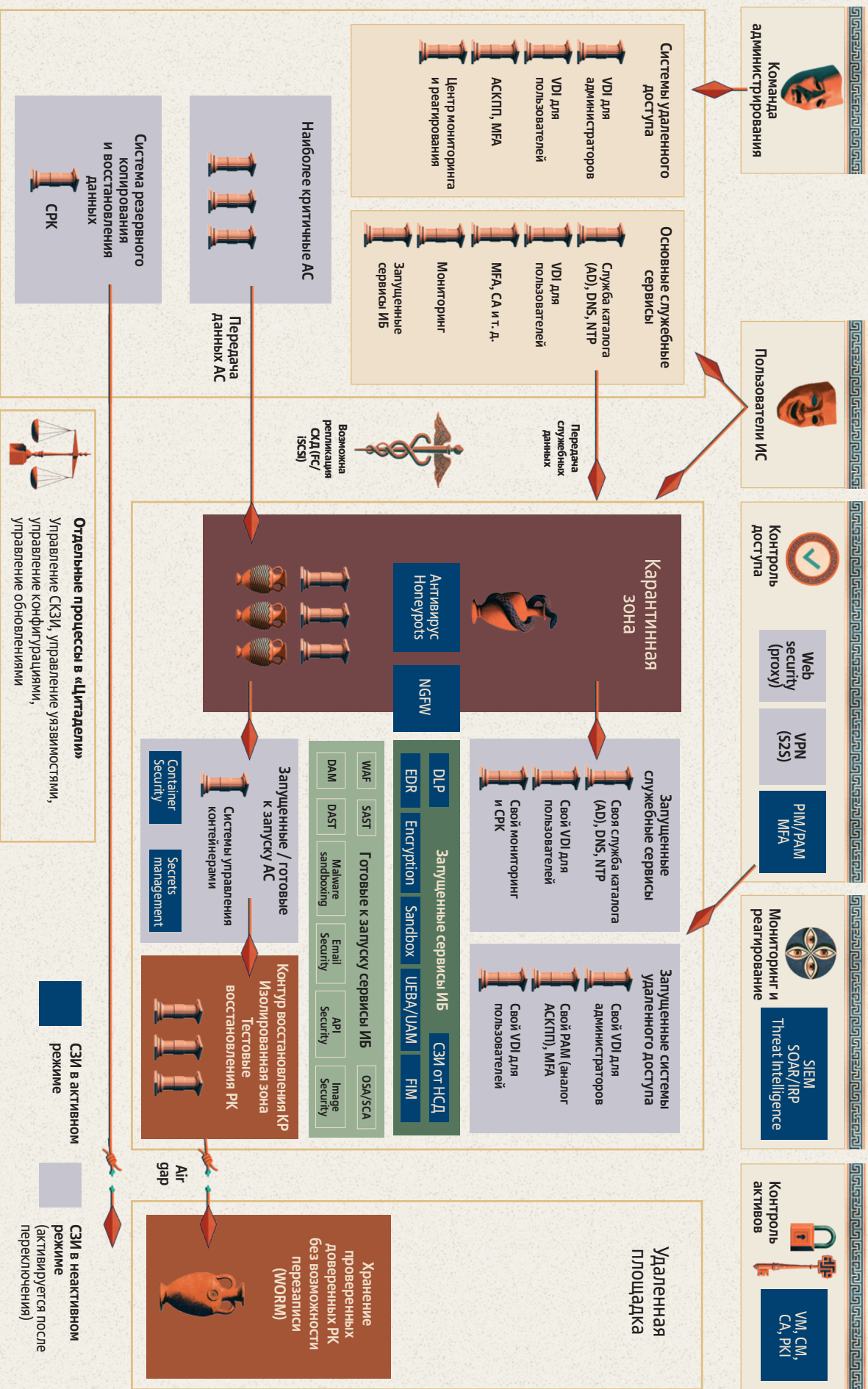
БУНКЕР

ЕДИНСТВЕННАЯ ГАРАНТИЯ ТОГО,
ЧТО ВАШИ ДАННЫЕ ОСТАНУТСЯ НЕВРЕДИМЫ



ЦИТАДЕЛЬ

ЕДИНСТВЕННАЯ ГАРАНТИЯ ТОГО, ЧТО ВАШИ СИСТЕМЫ ВЫЖИВУТ



ЗАЩИТА ОТ МИНОТАВРА

КАК «БУНКЕР»
И «ЦИТАДЕЛЬ» УДЕРЖИВАЮТ
БИЗНЕС ВНЕ ЗОНЫ
ПОРАЖЕНИЯ ПОСЛЕ
КИБЕРАТАКИ



Раньше архитектуру аварийного восстановления (DR) проектировали преимущественно на случай отказа оборудования, а также для возобновления работы после происшествий на площадке и стихийных бедствий. Сегодня главной угрозой для компаний стали кибератаки. И все чаще Минотавр устремляется в сердце цифрового лабиринта — в систему управления резервным копированием, чтобы уничтожить саму возможность восстановления. В новых условиях непрерывность бизнеса требует комплексного подхода, в рамках которого доверие к резервным копиям не менее важно, чем их сохранность, что позволяет запускать сервисы в максимально короткий срок после инцидента. Именно для решения этой задачи мы сконструировали «Бункер» и «Цитадель». Они дополняют традиционные меры защиты, которых теперь уже недостаточно.



АВТОР

Игорь Шконда,

руководитель направления систем резервного копирования компании «Инфосистемы Джет»



АВТОР

Антон Шипулин,

начальник отдела комплексных проектов компании «Инфосистемы Джет»

Классическая стратегия DR, опирающаяся на правило резервного копирования «3-2-1» (*три копии, два типа носителей, одна копия вне основной площадки*), а также наличие основного и резервного ЦОД с настроенной репликацией перестали быть универсальной защитой бизнеса. Современные кибератаки нацелены на остановку работы компаний: используя программы-шифровальщики и вайперы, преступники в первую очередь пытаются проникнуть в систему резервного копирования, чтобы заразить или уничтожить все резервные копии данных и лишить бизнес возможности их использовать для восстановления после того, как будут стерты все основные данные. По результатам расследований Jet CSIRT (*центра кибербезопасности компании «Инфосистемы Джет»*) с 2025 года, в 96% инцидентов целенаправленная атака на бэкапы проводилась заранее — до перехода к активной фазе.

При таком сценарии резервный ЦОД, имеющий постоянную сетевую связность с основной инфраструктурой, сам становится частью зоны поражения. Если

злоумышленник получает административные права в домене, под угрозой оказываются обе площадки. Восстанавливать приходится уже не только данные или сервисы, но и доверие к самой инфраструктуре. Именно этот опыт, через который проходят многие компании, сподвиг нас пересмотреть классические способы защиты резервных копий и СРК.

Разумеется, в нашем новом подходе по-прежнему важны заранее подготовленные планы возвращения к работе ИТ-систем (*DRP*) и бизнес-процессов (*BCP*). Кроме того, существенную роль играет и харденинг — базовая мера по повышению устойчивости ИТ-инфраструктуры. Однако даже хорошо защищенная среда не исключает успешной атаки, поэтому мы добавили в концепцию «Непрерывность 2.0» создание двух изолированных контуров — «Бункера» и «Цитадели» — для хранения данных и восстановления систем.

«Бункер»: доверенная среда для восстановления

Вот первые вопросы, на которые необходимо получить ответ после кибератаки: получил ли злоумышленник административный доступ и сохранились ли резервные копии, которым можно доверять? Если доступ получен, обычная система резервного копирования оказывается такой же скомпрометированной, как и продуктивная среда.

Чтобы обеспечить гарантированное восстановление, мы спроектировали «Бункер» — киберустойчивую систему резервного копирования (*СРК*). Физически она может располагаться как на удаленной площадке, так и в любом из ЦОД, потому что принципиальное значение имеет не место ее размещения, а независимость и логическая изоляция от продуктивной инфраструктуры.

Главная задача «Бункера» — хранить доверенные резервные копии, пригодность которых подтверждена заранее, и быть средой для тестового восстановления. Его основное отличие от традиционной СРК — не в используемом оборудовании, а в архитектуре. Это полностью автономный контур с собственными серверами управления системой резервного копирования, базой каталогов, медиаагентами, SAN (*сетью для подключения внешних устройств хранения данных*) и инфраструктурными сервисами, такими как:

ПОСТУЛАТЫ ДОВЕРЕННОЙ РЕЗЕРВНОЙ КОПИИ

Размещена в
незаменимом/
отчужденном
хранилище

Используется
внешнее
шифрование РК

Выполнена
валидация
чек-сумм
образов РК
на целостность

РК актуальна
на конкретную
дату

Из РК можно
восстановиться

РК и процесс РК
документированы



- **Active Directory (AD)** — служба каталогов, управляющая учетными записями и правами доступа;
- **Domain Name System (DNS)** — система, преобразующая имена серверов в IP-адреса;
- **Dynamic Host Configuration Protocol (DHCP)** — протокол для автоматической выдачи сетевым устройствам IP-адресов и настроек.

«Бункер» оснащен средствами защиты информации разных классов: антивирусной защитой, межсетевыми экранами, песочницами (*sandbox*), EDR, — а также имеет изолированное управление (*терминальный доступ, второй фактор, специальные учетные записи*).

Отдельные административные учетные записи, предназначенные для управления «Бункером», никак не связаны с продуктивным доменом. Это исключает ситуацию, когда компрометация основной инфраструктуры автоматически начинается компрометацию резервной площадки. На архитектурной схеме «Бункера» хорошо видно, что контур резервного копирования отделен от продуктивной среды не только логически, но и административно.

По другому принципу организована и передача данных между продуктивной средой и «Бункером». Мы используем асинхронную репликацию по Fiber Channel, поскольку она значительно устойчивее к сетевым атакам. После завершения резервного копирования резервные копии на уровне блочных устройств реплицируются в изолированный контур, а затем соединение между площадками разрывается — программно или физически. Постоянной сетевой связности между средами нет. После передачи в «Бункер» резервные копии восстанавливают (*это актуализирует DRP и повышает компетенцию команды*) и проверяют на полноту, актуальность и консистентность — вплоть до запуска отдельных экземпляров приложений.

До завершения расследования кибератаки нельзя возвращать системы к работе. Однако «Бункер» позволяет начать восстановление немедленно, поскольку у компании остается независимый источник доверенных данных. Благодаря этому целевое время восстановления (*Recovery Time Objective, RTO*) сокращается.

Этот процесс включает:

- «зачистку» прода и развертывание ключевой инфраструктуры (*виртуализация, AD, перенастройка СХД*);
- восстановление данных критичных ИС из последней доверенной копии (*All-Flash + SAN дают максимальную скорость*);
- проверку и запуск систем.

Как упоминалось выше, «Бункер» не только служит хранилищем данных, но и используется для тестового восстановления критичных информационных систем. В изолированном контуре запускаются виртуальные машины, проверяется целостность баз данных, отрабатываются процедуры DRP. На схеме этот этап выделен как отдельный процесс: только после проверки резервные копии становятся доверенными и могут использоваться при аварийном восстановлении. Таким образом, можно заранее убедиться в их пригодности, и ИТ-команда уже будет знать, что именно восстанавливать, и не станет во время атаки тратить время на проверку работоспособности копий.

«Цитадель»: ЦОД последней надежды

Хотя «Бункер» решает проблему сохранности данных, возвращение сервисов к работе занимает время: нужно развернуть инфраструктуру, восстановить системы и проверить их работоспособность. А что делать, если бизнесу важно возобновить работу критичных информационных систем за считанные часы? В некоторых отраслях даже пара часов простоя означает серьезные финансовые потери. И вот здесь не обойтись без «Цитадели» — доверенного ЦОД последней надежды.

По сути, «Цитадель» — это отдельный изолированный контур, который, в отличие от резервного ЦОД, проектируется как безопасная среда, готовая принять нагрузку после серьезной чрезвычайной ситуации, в том числе киберинцидента, в результате которого основная инфраструктура заказчика стала недоступна или была скомпрометирована.

Основной актив «Цитадели» — уже запущенные и подготовленные к запуску экземпляры

ПРИНЦИПЫ РЕАЛИЗАЦИИ «ЦИТАДЕЛИ»

ТЕКУЩАЯ ИНФРАСТРУКТУРА

Центр мониторинга и реагирования

Команда администрирования

Наиболее критичные ИС
Mission Critical (MC)



Основные ИС
Business Critical (BC)



Менее критичные ИС
Business Operational / Office Productivity (BO/OP)



1

Пользовательские данные в виде файлов

2

Асинхронная репликация данных с задержкой

3

Резервные копии

ДОВЕРЕННЫЙ ЦОД

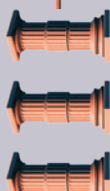
Команда администрирования

Центр мониторинга и реагирования

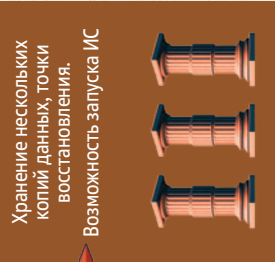
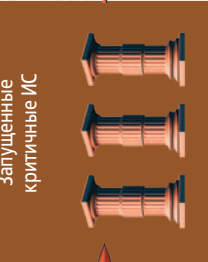
Система удаленного доступа

Карантинная зона

Прием данных из ЦОД
Анализ поступивших данных
Передача проверенных данных в ДК

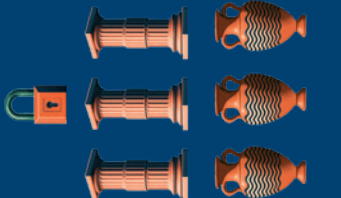


«ЦИТАДЕЛЬ»
Киберустойчивый ЦОД



«БУНКЕР»
Изолированная зона для СРК

Хранение нескольких версий РК
Автоматизация проверок РК
Создание доверенных резервных копий без возможности перезаписи (WORM)



НАДЕЖНОЕ ХРАНИЛИЩЕ

Сейф — изолированное хранилище РК



Хранение проверенных доверенных РК без возможности перезаписи (WORM)



Air gap

Готовимся к тому, что в час X мы будем переключать пользователей для работы в «Цитадели»

1

Использование единой схемы передачи данных

2

Запушенные ИС в «Цитадели». Минимизация времени переключения пользователей (RTO от 4–6 часов). RPO от 2–8 часов

3

Односторонняя асинхронная репликация данных. Больше время на включение ИС и переключение пользователей (RTO от 6–12 часов). RPO 4–12 часов

3

Хранение проверенных РК. Возможность восстановить ИС в принципе. RPO от 12 до 24 часов

информационных систем. Благодаря этому для переключения не приходится заново разворачивать всю инфраструктуру: значительная часть сервисов уже готова к работе.

Контур «Цитадели» не имеет открытого доступа в интернет и проектируется таким образом, что для злоумышленников он невидим. Доведенный ЦОД можно построить хоть за Уралом: для него неактуально минимальное время задержки, поскольку архитектура предполагает не-синхронную репликацию данных. В связи с этим часть из них может быть утрачена, но такой вариант все же лучше, чем потерять все данные.

Архитектура «Цитадели» строится в соответствии с несколькими ключевыми принципами.

Первый — полная изоляция и самостоятельность. Как и «Бункер», «Цитадель» не является продолжением продуктивной инфраструктуры. Это максимально изолированная от внешнего мира инфраструктура. Она имеет собственные служебные сервисы, сервисы мониторинга, резервного копирования, управления доступом, виртуальные рабочие места для администраторов и пользователей, а также службу каталога. То есть это отдельная экосистема, способная функционировать независимо от основной площадки, что мы и видим на схеме: практически все инфраструктурные сервисы продублированы внутри защищенного контура. В идеале для обслуживания контура нужно иметь выделенную команду, а доступ обеспечивать не через интернет или корпоративную сеть (*КСПД*), а с отдельных АРМ из офисов заказчика по отдельным сетевым линкам.

Второй — карантинная зона и доставка данных. Как и в «Бункере», здесь используется блочная асинхронная репликация на уровне СХД по Fiber Channel или iSCSI. При этом, если необходим iSCSI, предполагается подключать дисковые массивы напрямую порт в порт — чтобы исключить передачу данных через общую корпоративную сеть. Информация передается в формате файлов — никакой классической репликации по сети на уровне прикладных систем. Каждую ИС и бизнес-процесс предварительно обследуют, изучая весь жизненный цикл данных (*Data Life Cycle*) и проверяя всю последовательность этапов их обработки — от генерации до удаления или архивирования (*тип данных, места их расположения и пр.*). Необходимо четко понимать, какие данные и как часто необходимо переносить

в «Цитадель» для обеспечения нужного уровня RPO. Мы исходим из того, что поступающие извне данные по умолчанию нельзя считать безопасными, поэтому все файлы ИС, журналы транзакций, WAL-файлы СУБД (*журналы предзаписи*) и другая информация проходят многоступенчатую проверку до попадания в изолированный контур. В архитектуре для этого предусмотрена отдельная карантинная зона с антивирусной проверкой, песочницами,honeypots (*серверы-ловушки*) и другими средствами анализа. Только после прохождения всех проверок данные могут использоваться внутри «Цитадели».

Третий — работающие критичные ИС. В «Цитадели» развернуты и функционируют экземпляры наиболее критичных информационных систем. Часть из них могут находиться в состоянии максимальной готовности к запуску. Во время полного отключения основной инфраструктуры и проведения там расследования инцидента, в «Цитадели» полным ходом выполняется детальный план по переключению (*DRP*) и идет подготовка к переключению продуктивной нагрузки (*включение ИС, корректировка настроек сети и информационной безопасности, сбрасывание паролей и т. д.*). И как только коллеги из ИБ дают разрешение, мы уже готовы подключать пользователей.

Четвертый — своя система информационной безопасности. В «Цитадели» развернут собственный набор защитных средств. Минимально это:

- Next Generation Firewall (*NGFW*) — умный фильтр трафика, который блокирует атаки на уровне приложений;
- Web Application Firewall (*WAF*) — межсетевой экран для веб-приложений, который пропускает только легитимный пользовательский трафик;
- Security Information and Event Management (*SIEM*) — анализатор логов и событий, который бьет тревогу при аномалиях;
- Endpoint Detection and Response (*EDR*) — антивирус, который отслеживает подозрительные процессы и позволяет изолировать зараженную машину от сети;
- средства контроля привилегированного доступа, мониторинга и реагирования.

ДЛЯ САМЫХ КРИТИЧНЫХ СИСТЕМ МОЖНО ОРГАНИЗОВАТЬ ЗАЩИТУ НА УРОВНЕ «ЦИТАДЕЛИ», А ДЛЯ ОСТАЛЬНЫХ ИС ДОСТАТОЧНО ИМЕТЬ ПРОВЕРЕННЫЕ РЕЗЕРВНЫЕ КОПИИ В «БУНКЕРЕ»

Благодаря тому, что при штатной работе системы у нас нет продуктивной нагрузки, можно повысить уровень обеспечения ИТ: включить проактивный контроль трафика (*NTA*), выполнить расширенный сбор и анализ событий, оценить активность, применить несколько разных анти-вирусных решений, ввести контроль целостности и задать максимально жесткие параметры харденинга и настроек ИБ.

Часть механизмов защиты постоянно работают внутри контура, часть — активируются непосредственно перед переключением пользователей на «Цитадель». Благодаря этому после запуска сервисов инфраструктура находится под контролем собственной системы безопасности и не зависит от состояния основной площадки.

На схеме «Цитадели» представлены несколько подсистем. Есть компоненты, обеспечивающие работу критичных информационных систем: доверенные резервные копии, служебные сервисы, контур восстановления, системы удаленного доступа пользователей и администраторов. Отдельно — работающие и готовые к запуску приложения. Кроме того, имеются собственные средства защиты и управления (*системы контроля доступа, мониторинга, анализа угроз, управления конфигурациями и уязвимостями*). Между внешней основной инфраструктурой и «Цитаделью» располагается карантинная зона, через которую проходят все поступающие данные. Такой подход позволяет одновременно обеспечить высокий уровень защищенности и сохранить готовность сервисов к запуску.

Таким образом, «Цитадель» позволяет существенно сократить время восстановления. Если при использовании «Бункера» необходимо сначала развернуть инфраструктуру из доверенных резервных копий, то здесь значительная часть работы уже выполнена заранее.

Целевое время восстановления (*Recovery Time Objective, RTO*) в такой архитектуре составляет четыре-шесть часов, но в любом случае оно должно быть скоординировано с временем проведения расследования в скомпрометированной основной инфраструктуре.

Поскольку в «Цитадели» нет боевой нагрузки (*пользовательской активности*), в этом ЦОД можно проводить проверки и тестовые восстановления, анализировать сетевой трафик и пр.

«Бункер» и «Цитадель» в архитектуре «Непрерывности 2.0» не конкурируют, а дополняют друг друга. Для самых критичных систем можно организовать защиту на уровне «Цитадели» (*в составе доверенного изолированного ЦОД*), а для остальных ИС достаточно иметь проверенные резервные копии в «Бункере».

Возможность восстановления гарантируется сохранностью данных, а наличие доверенного ЦОД позволяет вернуть системы к работе максимально быстро. Да, создание «Цитадели» требует значительных инвестиций. Однако даже несколько часов простоя могут обойтись многим компаниям существенно дороже, и для них такая защита — не роскошь, а необходимость. ●



АВТОР

Дмитрий
Герасимов,

управляющий
директор
по информационным
технологиям Lamoda

КАК НЕ РУХНУТЬ С ПИКА

СЕКРЕТЫ НЕПРЕРЫВНОЙ
РАБОТЫ МАРКЕТПЛЕЙСА
ПРИ СЕЗОННОМ ВСПЛЕСКЕ



Для электронной коммерции осень, и особенно ноябрь, — самое напряженное время. Активность покупателей вырастает кратно по сравнению с любым другим сезоном, проводятся масштабные распродажи, маркетинговые акции. Нагрузка на сервисы огромная. Как в этот период обеспечить непрерывность процессов и высокое качество обслуживания клиентов? Универсального рецепта не существует, но есть практический опыт, накопленный Lamoda.

День холостяка и «черная пятница»: главные вызовы года

Пики нагрузки традиционно приходятся на День холостяка, 11.11, и «черную пятницу» — в 2026 году это 27.11. Эти дни не похожи ни на что, с чем мы сталкиваемся в течение года. Меняются паттерны поведения пользователей, проводятся акции, а значит, меняется нагрузка на все основные сервисы маркетплейса — в течение суток она может вырасти в десять раз. А в последние минуты акций пики выстреливают как свечи. Обеспечить безукоризненное качество сервиса в таких условиях — основной фокус и большой челлендж для команды.

Год от года задача не становится проще: растут бизнес, аудитория, ассортимент. Соответственно, растет количество заказов. Вместе с этим увеличивается сложность функционала. Но и мы не стоим на месте: наращиваем арсенал решений для пикового сезона и с каждым годом приходим к этому периоду все более подготовленными.

Цена ошибки

Когда мы разрабатывали систему KPI доступности Lamoda, то ставили во главу угла влияние технических инцидентов на бизнес-цели компании. Требовать от всех сервисов доступности на уровне четырех девяток (99,99%) не всегда оправданно.

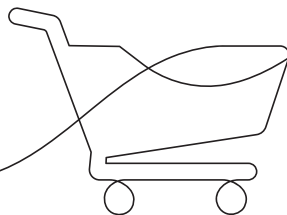
В силу асинхронности отдельных бизнес-сценариев, например в логистике или при подготовке контента, мы можем себе позволить

кратковременную недоступность — это не повлияет на качество обслуживания пользователя. Поэтому в наших KPI коммитимся на долю потерь NMV (*чистая стоимость проданных товаров*) и выручки по техническим причинам. Мы оцениваем влияние на бизнес каждого инцидента: сколько заказов не было создано или не доставлено клиенту в срок, сколько не показано коммерческой рекламы. И все эти импакты переводим в деньги. Так гораздо нагляднее и для ИТ, и для бизнеса.

Как все это выглядит в цифрах? Во время пиковых распродаж сезона 2025 года, в «черную пятницу» и День холостяка, нам удалось не допустить ни одного инцидента с потерей заказов, и за весь ноябрь потери составили менее 0,14% NMV. Команда тогда отработала на отлично. На второе полугодие 2026 года наш KPI меньше 0,3% от NMV потерь по техническим причинам. И в этом году нам удастся идти значительно ниже этой цифры.

Что критично для непрерывности

Для непрерывности важна не только работа ИТ-инфраструктуры, но и процессы самого сервиса. Нагрузка в сезон повышается по двум причинам: растет аудитория и увеличивается количество заказов. Плюс расширяется ассортимент, множатся промоакции, усиливается активность



партнеров — но это куда более предсказуемые факторы, не такие динамичные, как поведение пользователей. А значит, узкими местами, которые необходимо своевременно выявить и укрепить, сделав устойчивыми к скачкам нагрузки, становятся сервисы, задействованные в сценариях выбора товара, оформления заказа и на всех этапах доставки товара (*от склада до вручения клиенту*).

С помощью чего мы обеспечиваем непрерывность? Lamoda — большая платформа, поэтому назвать технологию или подход, которые не нашли отражения в нашей системе, будет сложно. У нас уже больше 600 микросервисов. Конечно, есть ряд требований к архитектуре, направленных на исключение типичных проблем: дублирования заказов, неактуальности информации по остаткам. При оформлении заказа одно из первых действий в системе — резервирование конкретного экземпляра товара на складе под конкретный заказ. Так мы исключаем ошибки в учете стоков. Если клиент приступил к оплате заказа, мы уверены, что этот товар есть в наличии именно для него.

Высокая устойчивость к сбоям — результат большой работы последних нескольких лет. Мы привели архитектуру сервиса и ИТ-инфраструктуру в соответствие с канонами построения облачных решений. Все критичные сервисы и базы данных размещены в трех зонах доступности, реализована репликация данных. Если происходит сбой в работе отдельных баз данных или сервисов либо выходит из строя зона доступности, нагрузка перераспределяется — и работоспособность восстанавливается автоматически.

Механизмы обратной связи ограничивают подключение новых пользователей, если сервис перестает справляться с нагрузкой при экстраординарном скачке активности. Это позволяет тем, кто уже начал работать с Lamoda, продолжать оформлять заказы. Когда часть пользователей завершат сессии, мы начнем постепенно впускать новых. Принцип такой: лучше обеспечить полноценный функционал тем, кто уже начал пользоваться сервисом и находится глубже в воронке, чем пытаться со снижением качества обрабатывать запросы всех желающих.

Это автоматический механизм. У нас за это отвечает Session Limiter, он постоянно мониторит состояние всех сервисов, участвующих в критических бизнес-сценариях.

Мир в режиме офлайн

С учетом периодически возникающих сложностей с мобильным интернетом мы приняли ряд мер для снижения рисков. В частности, обеспечили наиболее востребованные ПВЗ и магазины Lamoda Sport проводным интернетом и резервными каналами связи от разных провайдеров.

Наши курьеры теперь могут выдавать заказы в офлайн-режиме. Если мобильный интернет недоступен, курьер может вручить клиенту заказ и даже принять оплату. Для этого мы загружаем в специальное приложение курьера на сортировочном центре всю необходимую информацию по заказам и условиям оплаты. Клиент сможет оплатить покупку с помощью QR-кода, используя свой домашний интернет, а курьер уже без интернета сможет выдать заказ и провести эти операции.

А чтобы уменьшить влияние сбоев на стороне сервисов партнеров, мы используем принцип graceful degradation (*плавной деградации*). К примеру, если некоторые виды оплаты недоступны, мы предложим воспользоваться альтернативными методами или оформить заказ с постоплатой. При недоступности сервисов, реализующих некритичный для основного сценария функционал, мы продолжим работу без него — например, можем отключить показ рекламы, чтобы при этом предоставлять полноценную информацию о товаре, что для клиента гораздо важнее.

Там, где возможно, мы снижаем связанность сервисов, используя очереди сообщений. То есть сервисы не ждут мгновенного ответа друг от друга и не падают каскадом при временных сбоях, так как общаются через буфер (*очередь*). Такая возможность помогает переживать кратковременные сбои с меньшим влиянием на обработку пользовательских запросов и возвращаться к обработке заказов на том же этапе, на котором произошла ошибка.

Стресс-тест для системы

Ключевой метод подготовки сервиса к росту нагрузки — нагрузочное тестирование. Этот процесс у нас автоматизирован, и он не останавливается в течение всего года.

Мы регулярно получаем прогнозы бизнеса по ключевым для нас драйверам роста (*объему дневной аудитории, заказам, ассортименту*).

и на основе дневных прогнозов и исторической информации оцениваем потенциальные пики нагрузки. Тесты ежедневно валидируют готовность продакшена к пиковой нагрузке, которая ожидается в течение ближайшего месяца. Если выявлена деградация или необходимо масштабирование, команда оперативно вносит необходимые изменения.

Особенность нагрузочных «стрельб» для подготовки к распродаже — в том, что мы воспроизводим специфичный для нее профиль нагрузки. Как это делается? Во время реальных распродаж мы записываем всю последовательность обращений пользователей к нашему сервису, затем обезличиваем эти данные и воспроизводим в качестве теста, полностью имитируя нагрузку, характерную для тех или иных распродаж.

Кроме того, по расписанию тестируем DR-планы — сценарии восстановления при сбоях отдельных реплик и сервисов, переключения на резервные каналы связи с дата-центрами и логистическими объектами. У нас есть отработанный процесс управления инцидентами, он адаптирован для управления ситуациями разного масштаба. Для определенных сценариев есть протоколы реагирования как технических, так и операционных команд. Вторые должны скорректировать свои бизнес-процессы для митигации последствий технического сбоя. А при масштабных сбоях, которые влияют на большое количество пользователей, мы подключаем PR-службу, чтобы наладить коммуникацию.

DR-планы в классическом их понимании мы сформировали для нескольких критичных для бизнеса кейсов и при помощи автоматических тестов периодически валидируем готовность ряда систем к таким сценариям. Составлять исчерпывающие DR-планы на все случаи жизни пока считаем избыточным шагом.

Выпускайте канареек

Важное правило для ИТ-команды — не создавать дополнительных рисков, разворачивая новые функции или внося изменения в системы во время распродаж. Впрочем, фриззы на поставку релизов (*то есть периоды, когда запрещено выкатывать новые версии в «боевую» среду*) у нас крайне ограничены по времени, и мы стараемся дифференцировать их по сервисам

и сценариям. К примеру, в B2C- и в B2B-направлениях фриз длится, как правило, сутки-двое до акции плюс сам день акции, не дольше.

Для логистических компонентов более важен день акций и пара дней после: у них нагрузка в виде доставки рекордных объемов заказов, которые удалось оформить во время акции. При этом доставка в срок — не менее важная цель, поэтому мы очень внимательно относимся к стабильности логистики в этот период.

В остальные дни все команды разработки поставляют изменения в обычном режиме. Тем не менее мы постоянно контролируем активность пользователей, чтобы в случае ее всплеска приостановить поставку рискованных изменений.

Кроме того, мы постоянно развиваем инструменты по контролю качества и снижению рисков при выкатке релизов. Это известные на рынке подходы:

- **канарейки** — стратегия, при которой новая версия приложения сначала тестируется на небольшой части пользователей;
- **feature toggle** — переключатели функций приложения на лету, без развертывания нового кода;
- **АВ-эксперименты** — метод сравнения версий одного и того же компонента;
- **политики** — наборы правил и условий, которые автоматически проверяются перед тем, как разрешить или запретить какое-либо действие;
- **гейты** — контрольные точки в процессе поставки ПО, на которых автоматически или вручную принимается решение: пропустить релиз дальше или остановить;
- **автоматические и перформанс-«стрельбы»** — тестирование новой версии приложения, когда мы стреляем запросами-патронами в сервис и смотрим, как он реагирует на эту нагрузку.

Все эти подходы постоянно совершенствуем, чтобы снизить риски и иметь возможность поставлять релизы в том числе и во время высокого сезона.

Подготовка маркетплейса к пику сезона

- 1 **Проводите регулярные нагрузочные тесты именно на проде** — они дают гораздо больше гарантий готовности, чем любые проверки в тестовых средах. Важно, чтобы профиль нагрузки был не смоделирован вручную, а снят во время реальных распродаж. Да, продакшен-тестирование дорого и сопряжено с рисками, однако именно оно позволяет выявить проблемы в менее критичный момент и предотвратить катастрофические инциденты в пиковые нагрузки. А заодно исключает целый класс ошибок, связанных с неадекватной имитацией прода в тестовых окружениях.
- 2 **Применяйте механизмы graceful degradation как можно шире** — они делают сервис эластичным к нагрузке, а дежурным дают дополнительное время для принятия мер. Однако помните, что это не панацея: включение таких механизмов, к сожалению, снижает эффективность работы продукта.
- 3 **Устанавливайте ограничители внешней нагрузки** — допустите сценарий, при котором ваша распродажа превзойдет самые смелые прогнозы аналитиков. В этом случае избыточный трафик создаст
- 4 **Проверьте эффективность антиробот-системы заранее** — высокий сезон несет рост не только полезной активности пользователей, но и паразитной нагрузки. Ее создают парсеры цен, стоков, перекупщики, вылавливающие лучшие предложения, и киберхулиганы, стремящиеся обрушить сервис в момент максимального внимания аудитории. Убедитесь, что ваш антиробот действительно качественно чистит трафик и вы не просто так оплачиваете счета за этот сервис.
- 5 **Вводите фриз (заморозку) релизов новых функций за 24 часа до старта распродажи**. Я понимаю желание в последний момент выкатить «ту самую» фичу, тем более если ведущий разработчик готов поклясться, что с ней все будет хорошо. Но лучше возьмите паузу для наблюдения за сервисом и избегайте ненужных сюрпризов. Масштабные архитектурные изменения следует замораживать еще раньше, чтобы оставить время на стабилизацию и перебалансировку.
- 6 **Будьте в постоянном синке с планами бизнеса** — следите, чтобы календари акций и рассылки promo не накладывались друг на друга без необходимости. И лучше, если соответствующие ограничения в сервисах будут заданы технически.
- 7 **Поставьте дежурить сильнейших специалистов в дни распродаж**. Ноябрь — не лучшее время для отпусков. За ключевыми запусками и завершениями акций стоит следить как минимум основным дежурным неотрывно. В эти критические моменты мы держим ключевых специалистов в режиме реального времени в общей конференции и отслеживаем каждый этап процесса. 📍

СТРАТЕГИЯ ПРЕДВИДЕНИЯ

РОЛЬ ПРЕДИКТИВНОГО ИИ
В БЕСПЕРЕБОЙНОЙ РАБОТЕ
ПРЕДПРИЯТИЙ



Если час простоя критической ИТ-инфраструктуры обходится в миллионы рублей, а сбой в цепочке поставок парализует работу всей компании на недели, традиционные подходы к обеспечению непрерывности бизнеса перестают быть достаточными. Реактивные стратегии (когда на проблему реагируют уже после ее возникновения) уступают место проактивным (основанным на способности предвидеть сбой). Использовать новый подход позволяет предиктивный искусственный интеллект. Разберем, как именно работает эта технология, в каких сценариях она приносит максимальную пользу и с какими вызовами сталкиваются компании при ее внедрении.



ЭКСПЕРТ

Станислав Гордеев,

начальник отдела промышленных информационных технологий ООО «Объединенная сервисная компания» (оказывает сервисные услуги ММК)

Предиктивный ИИ — не черный ящик, предсказывающий будущее по наитию. Это совокупность методов машинного обучения, которые анализируют исторические данные, выявляют скрытые закономерности и на их основе прогнозируют будущие события.

В основе большинства промышленных предиктивных систем лежит анализ временных рядов. Датчики на оборудовании непрерывно передают показатели: вибрацию, температуру, давление, ток, акустические сигнатуры. Эти данные формируют последовательность значений, меняющихся во времени. Задача модели машинного обучения — уловить в этой последовательности паттерны, предшествующие сбою.



ЭКСПЕРТ

Никита Гусев,

руководитель направления ЕРМ компании «Инфосистемы Джет»

Эволюция методов прогнозирования временных рядов привела к появлению нейросетевых архитектур. Среди них — LSTM (*Long Short-Term Memory*), рекуррентные сети, способные «запоминать» долгосрочные зависимости в данных. Это критически важно для прогнозирования отказов, причины которых формируются неделями и месяцами.

Кроме того, сейчас часто применяют объединение больших языковых моделей (*LLM*) с анализом временных рядов. Например, фреймворк Time-LLM демонстрирует, как адаптировать предобученные языковые модели для решения четырех задач в единой архитектуре: прогнозирование, классификация, обнаружение аномалий и восстановление пропусков.

Ключевое отличие предиктивного ИИ от традиционной аналитики заключается в том,

что он не просто отвечает на вопрос «Что произошло?», а может рассчитать, «что произойдет» и «когда это произойдет». Именно это «когда» превращает его из инструмента отчетности в инструмент управления непрерывностью.

Вместе с тем для управления рисками важно не только строить прогнозы, но и проигрывать сценарии «что, если». В этом помогают цифровые двойники — виртуальные копии объектов, которые в реальном времени оценивают показания датчиков и демонстрируют, как поведет себя система при том или ином развитии событий.

Где предиктивный ИИ работает сегодня

Рассмотрим основные сценарии применения предиктивного ИИ на предприятиях в контексте обеспечения непрерывности бизнеса.

1 Предиктивное обслуживание оборудования

Планово-предупредительный ремонт по графику зачастую проводится либо слишком рано (*лишняя трата ресурсов*), либо слишком поздно (*допуск аварии*). ИИ анализирует состояние оборудования в реальном времени и рекомендует обслуживание ровно тогда, когда оно действительно нужно.

Никита Гусев

«Есть две идеологии: ремонт по регламенту (советская школа) и ремонт по состоянию (западная). Мы их не противопоставляем: регламентное обслуживание остается обязательной базой, а для ремонта по состоянию используются модели, которые работают с системами управления производством (MES), собирающими показания с датчиков. Если накоплен исторический набор данных о поведении агрегатов в разных режимах, то, обучив на этих данных ИИ, можно с точностью более 80% предсказать, что у конкретного агрегата в течение двух недель выйдет из строя определенный элемент. Это уже работает на практике».

В промышленности такой подход демонстрирует впечатляющие результаты: согласно отчету McKinsey «The future of maintenance», благодаря внедрению предиктивного ИИ простои

сокращаются на 35–45%, а затраты на обслуживание — на 25–30%. При этом более 95% компаний, внедривших предиктивное обслуживание, сообщают об окупаемости инвестиций, причем 27% достигают этого менее чем за год.

Дополненные ИИ-модулями системы могут предсказывать отказы оборудования не только на производственной линии, но и в ИТ-инфраструктуре. Например, в декабре 2025 года ГК «Датарк» совместно с научной командой УрФУ представила модули предиктивной аналитики для системы мониторинга ЦОД Datcheck. По словам разработчиков, они позволяют прогнозировать потенциальные сбои и аварии в дата-центрах за 6–10 суток до их возникновения.

2 Прогнозирование спроса и управление цепочками поставок

Сбои в цепочках поставок — один из главных источников риска нарушения непрерывности бизнеса. По прогнозу Gartner «Predicts 2024: Supply Chain Technology», к 2030 году 70% крупных организаций перейдут на прогнозирование спроса на основе ИИ.

В отличие от традиционных статистических движков, ИИ способен динамически выявлять сложные паттерны во временных рядах, а также учиться на различных наборах данных, что критически важно для прогнозирования спроса на новые продукты или для проведения промоакций.

Никита Гусев

«В одном из проектов мы разработали ИИ-ассистента для формирования логистических планов промышленной компании. Он анализирует как внутренние данные заказчика, так и внешние факторы (политическую обстановку, доступность маршрутов) и подсвечивает потенциальные угрозы, предлагая резервные каналы сбыта продукции по зарубежным контрактам».

3 Производственное и бизнес-планирование

Предиктивная аналитика проникает и в сферу операционного планирования. Например, для одной крупной медико-косметической компании специалисты компании «Инфосистемы Джет» применяют ИИ при планировании сменно-суточных заданий.

Никита Гусев

«Есть спецификация на изделие, параметры установок, ограничения в виде заcontractованных объемов и обязательных позиций. Наш алгоритм распределяет ресурсы так, чтобы максимизировать количество произведенных единиц продукции и прибыль, соблюдая эти ограничения».

Однако эксперт отмечает, что такая оптимизация работает только при синхронизации ИИ с поступлением информации о планах продаж и складских запасах.

Благодаря предиктивному ИИ, компания «Инфосистемы Джет» реализует проекты, в которых эффективность планирования возрастает на 7–8%, что для крупных предприятий, уже выжавших все резервы, становится значительным результатом. В абсолютных значениях это десятки и сотни миллионов рублей. Кроме того, это и экономия человеческих ресурсов, поскольку трудозатраты снижаются кратно.

4 Прогнозирование кибербезопасности

Предиктивные ИИ-системы применяются и в сфере кибербезопасности. В августе 2025 года группа компаний IBS разработала программный комплекс «Модель прогноза состояния информационной безопасности» (ПК МПСИБ), позволяющий спрогнозировать характер и динамику кибератак на три года вперед. На основе

фактических данных о кибератаках и инцидентах за прошлые периоды система оценивает состояние защищенности ИТ-инфраструктуры, выявляет наиболее уязвимые места и помогает планировать меры по минимизации рисков.

Российские кейсы: от металлургии до гидроэнергетики

Российские компании активно осваивают предиктивный ИИ, и накопленный опыт уже позволяет говорить о конкретных результатах.

ММК: практика предиктивной диагностики

Магнитогорский металлургический комбинат — один из лидеров по внедрению предиктивной аналитики в российской промышленности. За 2024–2025 годы здесь реализовано 19 проектов предиктивной диагностики оборудования.

Чтобы обеспечить непрерывность деятельности комбината, особенно важно отслеживать вибрацию и температуру в прокатном производстве ММК. Сейчас в листопрокатных цехах №№ 4, 5, 10, 11 и на агрегатах сортопрокатного цеха работают системы контроля, неоднократно

ПРЕДИКТИВНЫЕ МОДЕЛИ РАБОТАЮТ ПО ПРИНЦИПУ «МУСОР НА ВХОДЕ — МУСОР НА ВЫХОДЕ». ДЛЯ ОБУЧЕНИЯ ТРЕБУЮТСЯ БОЛЬШИЕ ОБЪЕМЫ РАЗМЕЧЕННЫХ ИСТОРИЧЕСКИХ ДАННЫХ

выявлявшего отклонения в работе электродвигателей, редукторов, подшипников, мультиклетей, которые могли привести к внеплановым простоям.

Станислав Гордеев

«Встроенные средства интеллектуального мониторинга и предиктивной аналитики обнаруживают дефекты на ранней стадии. Это могут быть недостаток смазки, дефект подшипника, некорректная работа оборудования после перевалки валков. Система выдает эксплуатационному персоналу рекомендации, которые помогают предотвратить аварию. Нередко проблему удается устранить во время плановой остановки простой и не дорогой операцией — например, добавив смазку. Своевременное выполнение таких рекомендаций предотвращает простои, сокращает число дорогостоящих аварийных ремонтов и снижает выпуск брака».

Отдельная группа проектов — цифровые двойники оборудования. В листопрокатном цехе № 10 внедрены две такие системы: одна прогнозирует утечки масла в общей гидросистеме, вторая контролирует состояние двигателей чистовой группы клеток по электрическим и механическим параметрам. Уникальность этих аппаратно-программных комплексов — в применяемых моделях прогнозирования отклонений. В первом случае удалось снизить потери смазочных материалов, во втором — сократить расходы на дорогостоящий аварийный ремонт силового оборудования.

Третья группа — системы контроля температуры холодильников, установленные на всех доменных печах. Они позволяют технологическому персоналу прогнозировать прогар холодильников и своевременно корректировать режим работы печи. Это помогает не допустить достижения точки невозврата, после которой требуется восстановительный ремонт продолжительностью более трех суток.

Все перечисленные системы, за исключением цифровых двойников, реализованы преимущественно на беспроводных технологиях компании «Предикта» — российского производителя решений в области интеллектуального мониторинга и предиктивной аналитики. Эти технологии упростили внедрение и эксплуатацию: датчики

можно быстро снимать и устанавливать, а при необходимости — переносить систему на другой агрегат при сравнительно небольших затратах на перепроектирование и пусконаладку.

В ММК отмечают, что на практике наибольший экономический эффект от применения предиктивной аналитики в технологическом обслуживании и ремонте оборудования (*TOuP*) принесло сокращение количества и длительности простоев, а также экономия на внеплановых ремонтах.

Станислав Гордеев

«Экономический эффект различается в зависимости от системы и определяется множеством факторов: количеством оборудования, конструктивными особенностями агрегата, нюансами инфраструктуры, сложностью моделей мониторинга и прогнозирования. В целом на текущий момент общий экономический эффект измеряется десятками миллионов рублей. Средний срок окупаемости проекта на базе ИИ и беспроводных технологий составляет от одного года до трех лет в зависимости от контролируемых параметров и географии размещения оборудования».

«РусГидро»: от диагностики трансформаторов до применения дронов с ИИ

Группа «РусГидро» развивает сразу несколько направлений предиктивной диагностики. Специалисты ДРСК (*входит в «РусГидро»*) в 2025 году успешно испытали собственную разработку — систему диагностики силовых трансформаторов (*ключевого оборудования для передачи электроэнергии*). Анализируя растворенные в трансформаторном масле газы и воду, она оценивает состояние внутренней изоляции трансформатора и прогнозирует допустимые нагрузки и остаточный ресурс оборудования, что позволяет предотвращать возникновение нештатных ситуаций. К тому же диагностику можно проводить прямо на месте эксплуатации — без демонтажа и отправки проб в лабораторию.

А в мае 2026 года «РусГидро» представила цифровой метод обследования плотин и дамб с использованием беспилотников и ИИ. В течение 30-минутного полета дрон делает тысячи снимков труднодоступных участков, что сильно ускоряет выявление повреждений, ведь, например,

высота плотины Саяно-Шушенской и Чиркейской ГЭС превышает 200 метров, а протяженность их сооружений исчисляется десятками километров. Снимки проходят фотограмметрическую обработку, и на выходе получается точная 3D-модель, где видны трещины, высолы и коррозия. Ключевая роль отведена ансамблю нейросетей, которые распознают дефекты на цифровом двойнике и классифицируют их по степени опасности.

В результате эффективность мониторинга выросла на 90%, время обработки часовой съемки сократилось почти в 4 раза — со 110 до 28 часов, а ручной труд снизился на 76%. Технология уже применяется на Саяно-Шушенской, Новосибирской и Усть-Среднеканской ГЭС. Проект полностью импортонезависим: используются собственное ПО и архитектура нейросетей. В планах компании — масштабирование метода на грунтовые плотины и развитие экологического мониторинга с применением БПЛА.

Подводные камни внедрения

Однако путь к таким результатам не всегда прост. По оценкам Gartner, в 2023–2024 годах примерно 60–70% инициатив по предиктивному обслуживанию не достигли поставленных целей и не перешли в стадию эксплуатации. Причина — не в технологии как таковой, а в системных ошибках на этапе внедрения. Рассмотрим основные из них.

1 Некачественные или неполные данные

Самая частая причина неудач. Предиктивные модели работают по принципу «мусор на входе — мусор на выходе». Для обучения требуются большие объемы размеченных исторических данных, причем они должны включать не только штатные режимы, но и предаварийные ситуации.

Никита Гусев

«В первую очередь необходимы зрелые бизнес-процессы и цифровая культура. У заказчика должна быть формализована методология: все прописано, нет сотрудников — хранителей сакральных знаний. Второе условие — наличие унифицированной нормативно-справочной информации (НСИ). Если в исходных данных есть несоответствия, нет единой версии правды, то искусственный интеллект не даст консистентной

картины. Итак, сначала методология, потом данные и только после этого — технологии».

Как поясняет эксперт, подготовка данных — это отдельный важный этап, потому что у заказчиков они часто неконсистентны. Один и тот же параметр — например, количество хлора — на разных участках может измеряться в разных единицах: килограммах, цистернах, бочках или литрах. Необходимо унифицировать все спецификации: для одних и тех же ресурсов должны использоваться единые единицы измерения. Это и есть нормализация НСИ. Решить такую задачу помогают системы Data Governance и озера данных: в них можно загружать сырые данные и обрабатывать их, в том числе с помощью ИИ, который выявляет идентичные номенклатуры, называемые по-разному.

В свою очередь, Станислав Гордеев отмечает, что качество данных для предиктивных моделей — понятие широкое: это не только форматы, источники и способы хранения, но и глубина архива, дискретность, ограничения инфраструктуры и требования информационной безопасности. Сочетание этих параметров далеко не всегда позволяет создать модель с требуемой точностью. Поэтому исходной точкой всегда служит конкретная задача. В одних случаях используют готовые рыночные модели, в других — модель разрабатывают самостоятельно или с привлечением стороннего подрядчика.

2 Соппротивление персонала и недоверие к ИИ

Технология сама по себе ничего не решает. Внедрение предиктивного ИИ требует перестройки рабочих процессов и, что еще сложнее, изменения менталитета сотрудников. Операторы, привыкшие полагаться на свой опыт и интуицию, часто не доверяют рекомендациям системы.

Никита Гусев

«Важна объяснимость результатов, которые выдает ИИ. Мы предлагаем инструменты визуализации — диаграммы Ганта, где видно, какие данные использовала модель, и можно “провалиться” к деталям. Также подготавливаем методики интерпретации результатов и чек-листы для операторов: пройтись по факторам, проконтролировать, что учтено, а что нет, и проверить человеческим глазом».

Эксперт отмечает: новый инструмент вызывает отторжение, люди держатся за привычное, поэтому необходимо проводить обучение, составлять инструкции, записывать видеоролики, формировать центр компетенций. Иначе продукт останется невостребованным.

Станислав Гордеев

«На начальном этапе внедрения на ММК наблюдались две крайности: одни сотрудники принципиально не доверяли системе и игнорировали предупреждения, другие, напротив, полагались на нее безоговорочно, считая, что она все сделает сама. Со временем стало ясно, что одной разъяснительной работы недостаточно. Необходимо formalизовать взаимодействие между различными службами компании при работе с системами интеллектуального мониторинга и предиктивной аналитики в ТОиР — не только в эксплуатации, но и в аналитике, применении метрик эффективности и использовании способов достижения экономического эффекта».

Так на ММК появился внутренний стандарт, описывающий соответствующие бизнес-процессы. Его задача — не только формализовать работу, но и помочь персоналу адаптироваться к новым технологическим реалиям.

3 Сложность интеграции с существующими системами

Предиктивный ИИ должен интегрироваться с уже работающими системами SCADA, ERP, MES и другими продуктами. Это требует не только технических усилий, но и согласования форматов данных, протоколов обмена и уровней доступа.

4 Неверный выбор технологического стека

Выбор ИИ-инструментов зависит от задач. Для производственного и логистического планирования это классическая задача коммивояжера (*поиск оптимального пути в графе*). Здесь эффективнее работает простая математическая оптимизация, а ИИ выступает как подсказчик и ускоритель вычислений. Для ассистентов менеджменту лучше подходят большие языковые модели: они выявляют коллизии, анализируют логику решений и помогают видеть последствия.

Никита Гусев

«В нашей библиотеке множество LLM. Мы адаптируем их под данные конкретного заказчика и внедряем в его контур. Это дает максимальную отдачу на вложенный рубль, экономит бюджет и гарантирует безопасность, так как модель работает без выхода в интернет».

В выборе платформы компания «Инфосистемы Джет» делает ставку на российские коммерческие решения — продукты «Яндекса», ВК, ГК «Цифра». Системы Open Source требуют больших затрат на доработку, тогда как готовые платформы дают быстрый результат.

Опоры предиктивной стратегии

Станислав Гордеев выделяет три главных фактора успеха при масштабном внедрении предиктивной диагностики. На первом месте — доверие персонала. На втором — готовность ИТ-инфраструктуры и унификация технологий, позволяющие внедрять решение без значительных капитальных затрат. На третьем — наличие в компании центров компетенций по IoT и предиктивной аналитике.

Станислав Гордеев

«Без собственных компетенций в области беспроводных технологий и инжиниринга данных компания вряд ли реализует успешный проект, даже при участии высококвалифицированных внешних исполнителей».

Технологии предиктивного ИИ дают способность прогнозировать будущее и управлять им, а не просто реагировать на наступающие события и сбои. Однако, как подчеркивает Никита Гусев, искусственный интеллект — не волшебная таблетка, а усилитель. Если изначальный показатель меньше единицы, ИИ даст худший результат; если все процессы отлажены — поможет.

Технология работает, но требует системного подхода — наличия зрелых данных, формализованных процессов и готовности персонала к изменениям. Именно эти составляющие превращают пилотный проект в промышленное решение, приносящее измеримый бизнес-эффект. 📍

ЭВОЛЮЦИЯ ТЕЛЕКОМ- МАГИСТРАЛИ

КАК И ЗАЧЕМ ОПЕРАТОРЫ ПЕРЕХОДЯТ
НА АРХИТЕКТУРУ TELCO CLOUD





ЭКСПЕРТ

**Дмитрий
Дементьев,**

архитектор МТС

От проприетарных «железок» и трехлетних внедрений — к виртуализированным решениям с доступностью 99,999% и готовностью к 5G. Разбираем, что такое телекоммуникационное облако (Telco Cloud), чем оно отличается от корпоративного и зачем нужно операторам связи.



ЭКСПЕРТ

**Денис
Непочатых,**

ведущий инженер
по решениям
для операторов
связи компании
«Инфосистемы Джет»

Еще 10–15 лет назад, чтобы предложить абонентам новую опцию, оператор объявлял тендер, а потом ждал полгода-год, пока выбранный поставщик привезет проприетарное «железо» и установит на него свой софт. Затем, после интеграции, настройки и тестирования (*а это еще примерно полгода*), услугу наконец выводили на рынок.

Денис Непочатых

«Иногда от старта конкурса до запуска услуги проходило несколько лет. Целая эпоха! За это время требования и реалии рынка существенно менялись, и внедряемое решение могло оказаться устаревшим».



ЭКСПЕРТ

**Александр
Гуляев,**

главный архитектор
по сетевым
технологиям компании
«Инфосистемы Джет»

При этом из-за жесткой привязки к вендорам у оператора со временем накапливался пестрый парк машин — от разных поставщиков. Возникали сложности в обслуживании: для каждого типа устройств требовались свои специалисты, обновления растягивались на месяцы, а запасные части приходилось держать на складах.

Вендоры поставляли монолитные вертикально интегрированные решения — софт и железо шли как единый «черный ящик». Заменить одну часть без другой было почти невозможно. Это и подтолкнуло операторов к переходу на стандартные серверы.

Параллельно с желанием сократить Time-to-Market и снизить зависимость от вендоров у телеком-операторов росла проблема недоутилизации ресурсов: мощности физических серверов не всегда использовались полностью. Однако запускать на одном сервере несколько решений было невозможно, потому что каждое устройство «затачивалось» под конкретную задачу (*коммутиция, маршрутизация, балансировка нагрузки*). В сезонные

РАНЬШЕ ВЕНДОРЫ ПОСТАВЛЯЛИ ОПЕРАТОРАМ СВЯЗИ МОНОЛИТНЫЕ ВЕРТИКАЛЬНО ИНТЕГРИРОВАННЫЕ РЕШЕНИЯ — СОФТ И ЖЕЛЕЗО ШЛИ КАК ЕДИНЫЙ «ЧЕРНЫЙ ЯЩИК»

пиковые нагрузки, наоборот, требовалось быстрое масштабирование, но сделать из одного сервера два по щелчку пальцев невозможно.

Так из корпоративного (*enterprise*) сегмента в телеком-индустрию переключался тренд на облака. В облачной инфраструктуре большой сервер стали делить на виртуальные машины (*VM*), а для управления ими создали системы виртуализации.

Александр Гуляев

«Облако — это способ потребления ресурсов и управления ими. Перевод сервисов в облако снижает зависимость от конкретных моделей и поставщиков серверов, ускоряет процессы запуска новых функций и обеспечивает эластичность использования ресурсов».

Таким образом родился прообраз Telco Cloud — облачной инфраструктуры, в которой на стандартных серверах размещаются виртуализированные сетевые функции (*Virtualized Network Function, VNF*), от пакетного ядра и биллинга до систем мониторинга. Это позволило быстро запускать услуги и снижать затраты за счет отказа от специализированного оборудования и унификации инфраструктуры.

Ключевую роль в унификации сыграл Европейский институт телекоммуникационных стандартов (*ETSI*), который в 2014 году выпустил единые стандарты виртуализации сетевых функций (*Network Functions Virtualization, NFV*). Речь

о фреймворке ETSI MANO (*Management and Orchestration*), ставшем архитектурным фундаментом телеком-облаков.

MANO включает три компонента: NFVO (*оркестратор, управляющий жизненным циклом функций*), VNFM (*менеджер конкретных виртуальных сетевых функций*) и VIM (*менеджер виртуальной инфраструктуры*). Именно эта тройка автоматизирует развертывание, обновление и масштабирование сетевых функций, а также распределение вычислительных, сетевых и дисковых ресурсов между ними. Благодаря единым стандартам крупные вендоры, такие как Nokia и Ericsson, создали каталоги виртуальных сетевых функций, и операторы получили возможность выбирать компоненты у разных поставщиков, будучи уверенными в их совместимости.

Эволюция Telco Cloud: от монолитных сервисов к контейнерам

Поначалу при переходе в облако традиционные телеком-функции — например, эволюционное пакетное ядро (*EPC, управляет сессиями и трафиком*), IP-мультимедийная подсистема (*IMS, отвечает за голосовые и мультимедийные сервисы*) и сеть радиодоступа (*RAN, базовые станции*) — просто виртуализировали, сохраняя их монолитную структуру. По сути, это были перенесенные в виртуальную машину копии проприетарного ПО — такие же ресурсоемкие и сложные

в обслуживании. Такой подход называли lift & shift («перенос как есть»).

Сегодня большинству участников рынка стало очевидно, что виртуализация — лишь промежуточный этап. Отрасль движется к контейнеризованным сетевым функциям (CNF), которые работают на микросервисах и автоматически управляются через Kubernetes (оркестратор контейнеров). Это подход cloud-native.

В связи с этим фреймворк ETSI MANO, изначально проектировавшийся для управления VNF на виртуальных машинах, сейчас эволюционирует, чтобы поддерживать контейнеры и Kubernetes как новый тип инфраструктуры с декларативным подходом. Теперь жизненным циклом сетевых функций (VNF/CNF) управляют оркестраторы: они самостоятельно разворачивают, масштабируют и сворачивают сервисы — участие человека минимально.

Денис Непочатых

«Во время массового мероприятия, например футбольного матча, система автоматически создает дополнительные ресурсы, чтобы обработать пиковый трафик, а после окончания — удаляет их. Болельщики не замечают нехватки пропускной способности, спокойно отправляют видео и постят сторис в соцсетях».

Оркестрация превращает набор серверов в гибкую, самонастраивающуюся платформу, готовую к требованиям 5G/6G и периферийных вычислений.

Чем Telco Cloud отличается от обычного облака

На первый взгляд, Telco Cloud просто еще одно облако. Но ключевое отличие — в том, как через него проходит трафик.

Денис Непочатых

«Корпоративное облако нагружено множеством операций: оно генерирует, обрабатывает и хранит терабайты информации. Например, когда клиент заходит на сайт маркетплейса, он прямо в облаке совершает покупку или получает информацию о трекинге своего заказа. А через Telco Cloud трафик

проходит транзитом, как по автомагистрали. Начальный и конечный пункты находятся за пределами платформы — внутри облака сама услуга не оказывается».

Для оператора ценность — в доставке этого трафика с заданными параметрами. Технологическая база у обоих типов облаков может быть одинаковой, но Telco Cloud проектируется как раз с учетом жестких требований к пропускной способности, задержкам, числу сессий и резервированию.

Александр Гуляев

«Хотя Telco Cloud — ниша телеком-операторов, его технологии могут использоваться также в корпоративных и исследовательских проектах. Мы обращаем пристальное внимание на выбор datapath и пропускную способность сетевого стека Telco Cloud. И когда в промышленности или науке возникнут требования и запросы, аналогичные операторским, решение уже будет готово, потому что в Telco Cloud решали похожие задачи».

Российские реализации: платформа 1Stack

Выбор технологий на каждом уровне зависит от стратегии оператора, бюджета и требований регулятора. Сейчас в России действует запрет на использование иностранного ПО для критической инфраструктуры, к которой относятся объекты связи. Поэтому на рынке появились отечественные решения. Один из ярких примеров — 1Stack от компании «Инфосистемы Джет».

Это облачная платформа виртуализации на базе OpenStack с открытым исходным кодом, предназначенная для управления виртуализированными ресурсами: процессорами, памятью, сетями и системами хранения. Продукт ориентирован на операторов связи и рассчитан на высокие нагрузки и масштабируемость.

Георезервирование для обеспечения «пяти девяток»

Для телеком-оператора непрерывность бизнеса — жесткое требование. Стандарт доступности 99,999% означает менее 5 минут простоя в год.

Ключевые компоненты Telco Cloud

Общую архитектуру Telco Cloud можно представить в виде трехуровневой конструкции.

01

ФИЗИЧЕСКИЙ СЛОЙ

Железо, на котором
все держится



Серверы (COTS x86)

Стандартные универсальные серверы, заменяющие проприетарные устройства



Системы хранения данных (СХД)

Программно-определяемые (например, **Ceph**) и аппаратные массивы



Сетевая фабрика

Высокоскоростные коммутаторы (400–800 Гбит/с) с поддержкой EVPN-VXLAN, которые создают единую программно-управляемую сеть; используются открытые сетевые ОС (например, **SONiC**) и white-box-оборудование

02

ПЛАТФОРМЕННЫЙ СЛОЙ

Делает железо
программируемым



Виртуальная инфраструктура

Платформа создания виртуальных машин и управления ими (обычно **OpenStack**), где работают VNF



Контейнерная инфраструктура

Кластеры Kubernetes для запуска легких CNF

03

УПРАВЛЯЮЩИЙ СЛОЙ

Мозг, автоматизирующий
процессы



Оркестрация (NFVO)

Управление жизненным циклом сетевых функций (VNF/CNF): развертывание, настройка, обновление, удаление



Автоматизация

Программное управление сетевой инфраструктурой и ресурсами, исключающее ручные операции



Мониторинг и OAM

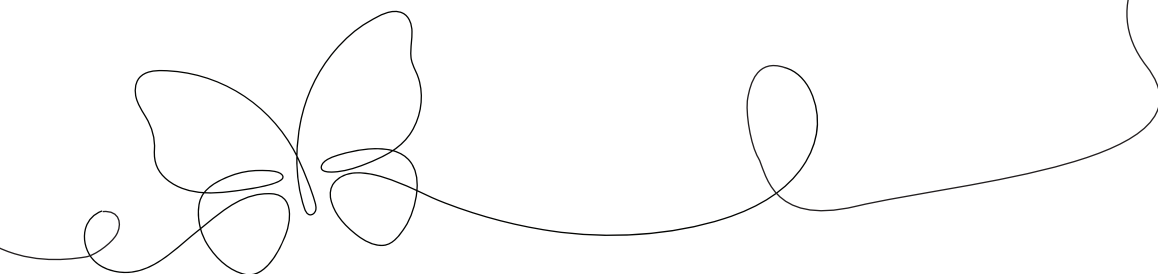
Сбор метрик производительности, анализ событий и аварий, распределенное резервное копирование, логирование и визуализация состояния системы

Такая трехуровневая архитектура обеспечивает доступность

99,999%

и минимальные задержки — то, что
отличает Telco Cloud от обычного облака

НА ПЕРВЫЙ ВЗГЛЯД, TELCO CLOUD ПРОСТО ЕЩЕ ОДНО ОБЛАКО. НО КЛЮЧЕВОЕ ОТЛИЧИЕ — В ТОМ, КАК ЧЕРЕЗ НЕГО ПРОХОДИТ ТРАФИК



И георезервирование становится ключевым инструментом его достижения.

Денис Непочатых

«Два независимых ЦОД, удаленных друг от друга, делят нагрузку пополам. При сбое одного трафик перетекает на другой — абоненты этого не замечают. Это как в космической технике: каждая важная подсистема резервируется (возможно, несколько раз), и при этом каждая из них полностью функциональна».

Резервирование пронизывает все уровни: сетевые узлы, серверы, коммутаторы, базовые станции. На каждом этапе заложены механизмы автоматического переключения — health-чеки, дублирование адресов, синхронизация сессий между ЦОД. Телеком-облако «Билайна», например, развернуто в ключевых центрах обработки данных оператора (Ярославль, Москва, Владивосток, Новосибирск, Екатеринбург), для части из них георезервирование уже внедрено, и до конца года планируется распространить его на все площадки.

Запуск Telco Cloud «Билайна», реализованный совместно с компанией «Инфосистемы Джет» в 2025 году, стал одним из первых крупных внедрений телекоммуникационного облака в России. Оператор связи продолжает унифицировать инфраструктуру, перенося на облачную платформу все больше функций (в виде VNF или CNF).

Стратегия и кадры

Для операторов связи Telco Cloud — это эволюционный шаг, хотя они понимают, что миграция в облако будет стоить сотни миллионов рублей и займет несколько лет. Вложения включают покупку серверов, софта, интеграцию, наем специалистов и последующую поддержку оборудования.

Операторы часто идут по двухэтапному пути: сначала полностью доверяют внедрение технологии интегратору, а по мере роста вложений начинают усиливать штат, чтобы самостоятельно развивать и поддерживать решение. При этом поддержка со стороны интегратора сохраняется, но уже на другом уровне.

Александр Гуляев

«Стоит учитывать, что переход на Telco Cloud требует новых компетенций. Раньше в телекоме работали

в основном сетевика, теперь нужны специалисты по виртуализации и контейнеризации, большая роль отводится инженерам DevOps и NetDevOps — тем, кто разбирается и в сетях, и в смежных областях».

5G и Network Slicing: когда одна сеть работает по-разному

Благодаря Telco Cloud стало возможным развитие технологий следующего поколения — в первую очередь 5G. Этот стандарт связи используется для критических сервисов: автопилотов, удаленной роботизированной хирургии, промышленного интернета вещей.

Ключевая инновация 5G — Network Slicing («нарезка сети»). Это когда на одной физической инфраструктуре выделяются логические пути, которые по-разному обрабатывают трафик.

Денис Непочатых

«На логических узлах нарезаются цепочки, обеспечивающие end-to-end-взаимодействие с определенным уровнем качества. Один срез дает высокую скорость передачи трафика, другой — нулевые потери, третий — возможность принимать данные от миллиона IoT-устройств».

То есть сеть перестраивается «на лету» под конкретную задачу без изменения физического оборудования.

Важно понимать: архитектура 5G Core (5GC) с самого начала проектировалась как cloud-native. Вместо монолитного EPS (как в 4G) в 5G используются микросервисы: AMF (управление доступом), SMF (управление сессиями), UPF (пересылка трафика) и другие. Они работают в контейнерах под управлением Kubernetes, общаются через API и могут масштабироваться независимо. Именно это дает возможность реализовать Network Slicing и обеспечивает эластичность, которой не было в предыдущих поколениях мобильной связи.

Эксперты подчеркивают, что 5G будет внедряться точно, а не массово, так как технология рассчитана в первую очередь на интерфейсы

machine2machine. Для обычных пользователей при стандартном объеме потребляемого трафика разница между 4G и 5G незаметна.

Дмитрий Дементьев

«На слайсинг идет колоссальный запрос от бизнеса. Однако сейчас внедрение 5G сдерживают две вещи. Первая — частоты, с которыми процесс более-менее налаживается: мы понимаем, что в этом году они будут розданы. Вторая — регуляторика. Как только мы получим четкие требования от Минцифры в отношении того, какие функции и особенности применения технологий должны быть в России, нам будет гораздо проще ее внедрять. Мы не хотим бежать впереди паровоза, чтобы потом не пришлось все переделывать».

Цифровое будущее уже строится

Вся философия 5G построена вокруг cloud-native-принципов, и реализовать их удалось только благодаря Telco Cloud. Та же архитектура ляжет в основу 6G и других технологий будущего.

Еще один драйвер развития Telco Cloud — искусственный интеллект, который потребует пересмотра самой модели потребления ресурсов.

Дмитрий Дементьев

«Буст развитию Telco Cloud, на мой взгляд, даст применение искусственного интеллекта. Раньше абоненты покупали минуты и SMS. Сейчас — гигабайты, объем трафика. Следующий шаг — токены. Продвинутые пользователи уже сейчас играют с локальными моделями, но ограничены производительностью личных устройств. Где взять токены для вычислительных ресурсов ИИ? Либо максимально близко к пользователю — это подход edge computing, либо в облаке сети оператора».

Показательно, что операторы связи уже начинают двигаться в этом направлении: «Билайн» включил ИИ-токены в свои тарифы подписки Bee. Это сигнал: телеком-облака становятся не просто магистралью для трафика, а платформой для новых цифровых сервисов. 📡



ВСЕ ЗА ОДНОГО

ПРОМЫШЛЕННЫЙ ПОДХОД
К ГЕОРАСПРЕДЕЛЕНИЮ ЦОД



ЭКСПЕРТ

Алексей Пигачев,

директор департамента
по ИТ группы компаний
«Талина»



ЭКСПЕРТ

Сергей Андронов,

директор центра сетевых
решений компании
«Инфосистемы Джет»



ЭКСПЕРТ

Всеволод Воробьев,

руководитель
направления ЦОД
центра сетевых решений
компании «Инфосистемы
Джет»

В 2023–2025 годах команда Jet CSIRT (центра кибербезопасности компании «Инфосистемы Джет») расследовала и ликвидировала последствия более 100 крупных киберинцидентов — каждый пятый случился на промышленных предприятиях. Однако угрозу заводам несут не только взломы: выход из строя оборудования, чрезвычайные ситуации, а теперь и атаки БПЛА могут прервать производство за считанные минуты. Единственный способ не допустить остановки — перестать полагаться на единственный ЦОД. Почему вместо неподъемного монолита надежнее подвижная инфраструктура из нескольких элементов? И в чем особенность геораспределенной защиты информационных ресурсов промышленных объектов?

Геораспределенные дата-центры — это проверенный способ обеспечить отказоустойчивость и катастрофоустойчивость информационных систем предприятия. Главная особенность этого подхода состоит в том, что ключевые компоненты ИТ-инфраструктуры (*серверы, базы данных, приложения, сервисы*) размещаются сразу в нескольких географически разнесенных дата-центрах и синхронизируются между собой. Если, например, отдельный сервер или целый ЦОД выходит из строя, его нагрузка перераспределяется на остальные узлы.

При этом у промышленных предприятий особый подход к геораспределению ЦОД. В отличие, скажем, от операторов связи, которым необходимо рассредоточить инфраструктуру по всей стране,

чтобы максимально приблизить обработку трафика к абонентам и обеспечить низкую задержку для голосовых и интернет-сервисов, промышленные компании чаще всего управляют несколькими крупными производственными объектами, расположенными за пределами крупных городов. Каждый объект связан с управляющим центром, однако имеет собственный уникальный ИТ-ландшафт, отвечающий его специфике.

Так, в управляющем центре могут размещаться серверы, отвечающие за бизнес-логику, базы данных для аналитики и принятия стратегических решений. В то же время все критические компоненты, обеспечивающие автоматизацию производства, должны располагаться на конкретном промышленном объекте: АСУ ТП, MES (*система управления производством*), средства защиты информации и другие системы.

Сергей Андронов

«Все, что критически важно для промышленного предприятия, является и критически уязвимым. Поэтому правильное решение — расположить ключевые сервисы максимально близко к производству и контролировать все изменения в режиме онлайн. А уже готовые выборки, накопленные на объекте за определенный промежуток времени, компания может анализировать централизованно».

Оптоволоконная сеть имеет ограничения в скорости передачи данных: преодолевать скорость света инженеры пока не научились. По словам эксперта, если для отказоустойчивой работы сервиса важна синхронная репликация данных с максимально низкой задержкой (*что актуально для любого производства*), то расстояние между ЦОД, где хранятся и обрабатываются эти данные, не должно превышать 15 км.

Таким образом, для предприятия логичным выглядит построение геораспределенной системы ЦОД непосредственно на каждом промышленном объекте или неподалеку от него.

Всеволод Воробьев

«Сейчас все бизнес-процессы функционируют при поддержке ИТ-систем. Значит, если в результате какого-то происшествия отключится единственный ЦОД, встанет все производство. Поэтому на территории предприятия нужно

создать несколько дата-центров, между которыми можно переключать нагрузку. Лучше всего локально распределить их в рамках обозримого участка, соблюдая необходимое расстояние для связности. Тогда выход из строя одного узла не повлияет кардинально на работу всего предприятия».

Эксперт уточняет, что для резервирования ресурсов можно использовать разные схемы взаимодействия ЦОД — как Active-Active (*когда все или несколько узлов одновременно обрабатывают запросы*), так и Active-Passive (*когда один узел активен, а другие находятся в режиме ожидания*). Главное — чтобы при необходимости переключение между ними происходило мгновенно.

Кто не спрятался...

Итак, для создания наиболее сбалансированной ИТ-архитектуры на промышленном объекте вместо строительства одного крупного ЦОД, который обслуживает все предприятие, стоит рассмотреть возведение нескольких небольших дата-центров. Но как защитить эти объекты от новых типов физических угроз — например, от атак БПЛА?

Сергей Андронов

«Есть крылатое выражение: ни одна крепость не падает без предательства. Каждый ЦОД тоже, по сути, является крепостью. Зачастую удары по нему происходят не потому, что его защита слабая, а потому что информацию о нем сложно долгое время хранить в тайне. Маскировка какое-то время спасает ситуацию, но если угроза физического воздействия существует, то рано или поздно предприятию придется задуматься о перемещении ЦОД».

Задача состоит в создании системы дата-центров, местоположение которых можно динамически менять. Лучше всего для этого подходят модульные ЦОД — готовые решения со всей необходимой начинкой: серверами, СХД, инженерными системами, сетевой и кабельной инфраструктурой. Они поставляются в виде отдельных блоков, и при необходимости их можно объединять как детали конструктора.

Всеволод Воробьев

«Модульные ЦОД отличаются минимальным сроком внедрения и возможностью гибкого масштабирования. Мобильный ЦОД в форм-факторе контейнера можно быстро отключить, перевезти в другое место и включить даже на минимально подготовленной площадке. Меняя таким образом конфигурацию системы дата-центров в пределах промышленной площадки, можно добиться высокой устойчивости и оптимального резервирования».

После перемещения такой контейнер можно очень быстро подключить к существующей инфраструктуре и ввести в эксплуатацию. По словам эксперта, для этого в месте установки достаточно провести минимальную строительную подготовку, подвести электричество, проложить подъездные пути и обеспечить каналы связи. Чтобы эффективно управлять ЦОД, необходимо предусмотреть систему автоматизации и диспетчеризации, которая позволит квалифицированным инженерам настраивать и контролировать инфраструктуру удаленно. Безусловно, эти операции повлекут издержки, тем не менее они не идут ни в какое сравнение с ущербом от полного разрушения узла в результате физической атаки.

Торг уместен?

Конечно, как и любой ИТ-проект, построение геораспределенной системы ЦОД на промышленном предприятии потребует ощутимых вложений. Однако их можно сильно сократить.

Во-первых, важно приоритизировать компоненты инфраструктуры. Это позволит спроектировать и построить дата-центр, который будет поддерживать работу лишь наиболее критичных для конкретного промышленного объекта приложений, сервисов и хранилищ данных.

Во-вторых, проект стоит разбить на несколько этапов — добавлять модули постепенно, по мере загрузки существующих. Вместе с тем каждый раз следует сохранять определенный запас вычислительных мощностей на случай внезапного роста нагрузки на ЦОД.

В-третьих, необходимо подготовить персонал предприятия к работе с геораспределенной

инфраструктурой: составить четкие инструкции и план аварийного восстановления, регулярно проводить тренинги. Чем быстрее команда сможет отреагировать на возникшую ситуацию (*например, переместить и переподключить мобильный ЦОД*), тем меньше будут издержки компании.

Не стоит опасаться того, что несколько распределенных ЦОД потребляют существенно больше электроэнергии, чем один централизованный. Чаще всего это не так, и на промышленном предприятии, оснащенном энергоемким оборудованием, разницы заметно не будет.

Таким образом, при правильном подходе локально распределенная система ЦОД в сравнении с монолитным дата-центром окажется для предприятия не только надежнее, но и выгоднее.

Фундамент для цифровизации

Летом 2025 года усилиями специалистов центра сетевых решений компании «Инфосистемы Джет» в Республике Мордовия на территории МПК «Атяшевский» (*входит в структуру группы компаний «Талина»*) были возведены два параллельно функционирующих модульных ЦОД. Они поддерживают работу WMS (*системы управления складом*), MES, систем учета и других критически важных программных комплексов предприятия.

Каждый ЦОД расположен на открытой площадке, имеет класс огнестойкости II, класс пылевлагозащиты IP66, рассчитан на девять шкафов 42U с максимальной общей мощностью более 100 кВт. Схема с двумя независимыми узлами обеспечивает отказоустойчивость ИТ-инфраструктуры комбината как в стандартных, так и в нештатных ситуациях.

Алексей Пигачев

«Опыт эксплуатации прежней серверной убедил нас: отказоустойчивость — это не опция, а обязательное условие для промышленного предприятия. Поэтому при проектировании новой архитектуры мы сделали ставку на резервирование всех критичных систем и надежную систему копирования данных. Сегодня два независимых ЦОД дают нам уверенность: производство не остановится даже при сбое одного из узлов».



ВРЕМЯ ЗАДУМАТЬСЯ О СОЗДАНИИ СИСТЕМЫ ДАТА-ЦЕНТРОВ, МЕСТОПОЛОЖЕНИЕ КОТОРЫХ МОЖНО ДИНАМИЧЕСКИ МЕНЯТЬ. ЛУЧШЕ ВСЕГО ДЛЯ ЭТОГО ПОДХОДЯТ МОДУЛЬНЫЕ ЦОД

ЦОД размещены таким образом, что при необходимости можно добавить в них новые секции или установить рядом дополнительное оборудование. Это дает предприятию большой задел для будущих проектов цифровизации.

Как отмечает Сергей Андронов, спрос на модульные ЦОД растет с каждым годом. С их помощью производства решают целый ряд задач — от обеспечения катастрофоустойчивости до более гибкого и эффективного распределения ресурсов.

Сергей Андронов

«На предприятиях, в том числе в металлургии и ТЭК, мы наблюдаем сейчас явную тенденцию к децентрализации ИТ-инфраструктуры и выстраиванию геораспределенной системы автономных ЦОД непосредственно на промышленных площадках. Такая схема дает максимальную гарантию того, что выход из строя одного дата-центра не приведет к остановке производства и другим негативным последствиям».

Эксперты компании «Инфосистемы Джет» подчеркивают, что в своих проектах собирают модульные ЦОД с использованием преимущественно отечественного оборудования: больше половины компонентов изготавливают российские заводы,

а остальное поставляется из дружественных стран, в основном из Китая. Это не только обеспечивает соответствие требованиям регуляторов к объектам КИИ (*к которым относятся многие производства*), но и позволяет предприятиям исключить зависимость от западных вендоров, быстрее разворачивать дата-центры и проводить их обслуживание: все комплектующие доступны, необходимые специалисты есть в любом городе.

Сегодня цифровизация промышленности идет крайне динамично. Процессы, которые раньше осуществлялись традиционным способом, активно автоматизируются — внедряются системы компьютерного зрения для контроля качества продукции, ИИ-алгоритмы, роботизированная сборка, интернет вещей. Это влечет масштабный рост данных — соответственно, появляется потребность в их надежном хранении и защите информационных систем. А постоянная готовность к отказам инфраструктурных компонентов и атакам стала для предприятий нормой жизни. В таких условиях выиграют компании, освоившие принципы антихрупкости: вместо опоры на надежный центр — децентрализация, вместо монолита — подвижная и адаптивная структура. Геораспределенные ЦОД — один из элементов такой парадигмы. Их взаимозаменяемость — фактор непрерывности бизнеса. ●

ЦИПР 2026

ПЕРЕДОВЫЕ ТЕХНОЛОГИИ

advanced technologies

// НИЖНИЙ НОВГОРОД

// NIZHNY NOVGOROD

ВСК
СТРАХОВОЙ ДОМ

СПАСИБО ЗА ВНИМАНИЕ



«ОСТАЛСЯ ТОЛЬКО СВЕТ»

НА ЦИПР-2026 ОБСУДИЛИ НЕПРЕРЫВНОСТЬ
БИЗНЕСА В ЭПОХУ КИБЕРТЕРРОРИЗМА



Еще несколько лет назад «обеспечить непрерывность бизнеса» означало реализовать набор технических и организационных мер, которые «должны сработать, если что-то случится». Резервные площадки, аварийные регламенты, планы восстановления, формальные ВСП — наличие всего этого свидетельствовало об инфраструктурной зрелости компании, но редко становилось предметом открытого управленческого разговора. На конференции «Цифровая индустрия промышленной России — 2026» (ЦИПР-2026) эту тему обсудили гораздо глубже. Сессия компании «Инфосистемы Джет» под названием «Непрерывность бизнеса в эпоху цифрового терроризма. Идеальный шторм» показала: сегодня остановка бизнеса все чаще связана не с техногенными авариями и природными катаклизмами, а с киберинцидентами, способными буквально за часы вывести из строя ключевые цифровые процессы. И компаниям теперь приходится жить в парадигме «когда это случится», а не «если...».

Фото: Станислав Карнаухов

С первых минут участники конференции обсуждали не только защиту периметра, но и саму возможность вести бизнес в ситуации, когда цифровая инфраструктура перестает быть надежной опорой компании. На этом фоне способность обеспечивать непрерывность бизнеса подтверждается не наличием набора документов, а реальным умением организации сохранять управляемость, быстро принимать решения и восстанавливаться в условиях кризиса.

Как отметил модератор дискуссии, генеральный директор компании «Инфосистемы Джет» Владимир Елисеев, за последние годы изменилась сама природа угроз.

Владимир Елисеев

«Именно в последние два года вероятность столкнуться с полной остановкой бизнеса в результате кибератаки драматически превысила вероятность получить ущерб вследствие любого другого инцидента. И при этом грубая оценка показывает, что в публичное поле попадают далеко не все такие случаи — лишь около 10%».

Эта мысль задала тон всей сессии: бизнес все чаще сталкивается не с гипотетическим риском, а с реальностью, в которой цифровой сбой способен стать причиной полномасштабного кризиса в компании.

Не киберзащита, а киберустойчивость

Одной из ключевых тем обсуждения стала смена самого подхода к обеспечению безопасности. Еще недавно корпоративная логика строилась вокруг идеи предотвращения инцидента: чем сильнее защита, тем меньше его вероятность. Но участники сессии говорили уже о другой модели — киберустойчивости, когда главный вопрос заключается не в том, удастся ли полностью исключить атаку, а в том, насколько быстро бизнес сможет пережить ее последствия. И чем

масштабнее цифровизация в компании, тем выше зависимость бизнеса от связности систем, технологий подрядчиков, резервных контуров и управленческой скорости. И тем шире поверхность атаки.

Георгий Старостин, директор по информационной безопасности компании «СОГАЗ»

«Построить инфраструктуру, в которой будет невозможна атака шифровальщика, — это практически невыполнимая задача. Скорость преобразований ИТ-ландшафта сегодня огромная.

Мы видим, что в компаниях он меняется на 30–40% в год. Появляются новые сервисы, меняются вендоры, расширяется цифровая среда. Защищать статичную инфраструктуру значительно проще, однако сейчас статичных инфраструктур практически нет».

Именно поэтому приоритеты компаний сместились от концепции «защитить всё» к модели постоянной готовности к атакам. В ходе дискуссии эксперты описали обеспечение непрерывности бизнеса как процесс, который начинается не после атаки, а задолго до нее — на уровне разработки архитектуры, резервирования, сценариев восстановления и культуры принятия решений.

Одной из тем обсуждения стал инцидент в ВСК, о котором рассказал член Совета директоров Страхового Дома ВСК Роман Фролов. Кейс оказался особенно ценным, так как речь шла не о теоретической модели восстановления после атаки, а о пережитом корпоративном кризисе.

Георгий Старостин отметил, что приоритеты компаний сместились от концепции «защитить всё» к модели постоянной готовности к атакам





Роман Фролов рассказал, как кибератака изменила отношение ВСК к рискам и инвестициям в безопасность

Киберинцидент в компании произошел 11 ноября 2025 года. Злоумышленники скомпрометировали ряд хостов, получили доступ к учетной записи администратора, внутри инфраструктуры были зафиксированы DDoS-атаки средней интенсивности. Позже форензика позволила восстановить полный вектор проникновения. Крайне важным оказалось то, насколько быстро технический инцидент перерос в глобальную бизнес-проблему: под ударом оказалась вся виртуальная инфраструктура компании (*серверы, виртуальные рабочие станции в обоих ЦОД*), а часть резервных копий была уничтожена. По сути, цифровая среда компании перестала быть рабочей. А ведь злоумышленники перед атакой находились в инфраструктуре меньше суток.

Роман Фролов

«Если говорить о критичных бизнес-процессах, то остановились все фронт-офисные инфраструктуры, в том числе система для продавцов. Пропала возможность онлайн-оформления договоров страхования, остановились партнерские API, системы скоринга и тарификации, перестал работать активный контакт-центр. То есть, по сути, из рабочих инструментов остался только свет, который можно было включить и выключить».

Атака помогла понять: существовавший план непрерывности бизнеса оказался лишь частично применим к реальности. По словам эксперта, в лучшем случае релевантными оказались лишь половина сценариев. Этот опыт стал точкой перехода от логики киберзащиты к логике

киберустойчивости. Вместе с тем случившееся заставило ВСК задуматься и о бюджете на информационную безопасность. До инцидента в компании обсуждали расходы порядка 10% от потенциального ущерба, но после атаки подход пересмотрели. Как отметил Роман Фролов, текущие затраты на ИБ составляют около 30–40% от возможных потерь, и теперь это воспринимается как инвестиция, а не избыточная нагрузка.

80/20: как бизнес сегодня смотрит на ИБ

Кроме того, в ходе дискуссии эксперты обсудили поиск оптимального баланса между расходами на предотвращение атак и затратами на восстановление после инцидентов. Здесь прозвучали важные цифры. Например, вице-президент по цифровизации и информационным технологиям компании «ТВЭЛ» Евгений Гаранин отметил, что в его практике основная часть бюджета ИБ уходит именно на недопущение проникновений в инфраструктуру.

Евгений Гаранин

«Прямые затраты на ИБ, которые направлены не только на сами проекты, но и на различные системы защиты, антивирусы, резервное копирование и все остальное, составляют более 80% от всего бюджета на информационную безопасность. И при этом у нас единственная крупная статья, на которую в принципе никто не смотрит при оптимизации бюджета, — это информационная безопасность».

Участники обсуждали не только защиту. Дмитрий Якоб, заместитель генерального директора по информационным технологиям ТМК, говорил о рискориентированном подходе: расходы должны соотноситься не с модой или отраслевыми бенчмарками, а с вероятностью и стоимостью потенциального ущерба.

В процессе обсуждения не обошли стороной и подрядчиков как потенциальную точку входа в инфраструктуру. По статистике, представленной Романом Фроловым, около 10% проникновений происходит именно через внешних подрядчиков. А Владимир Елисеев добавил: «Для крупных организаций такой вектор атаки остается одним из наиболее распространенных». Это в очередной раз доказывает, что непрерывность

Обеспечение непрерывности бизнеса начинается не после атаки, а задолго до нее — на уровне разработки архитектуры, резервирования, сценариев восстановления и культуры принятия решений

бизнеса зависит не только от внутренних защитных контуров, но и от зрелого управления внешней экосистемой — поставщиками, интеграторами, подрядчиками и доступами, через которые компания коммуницирует с внешней средой.

Почему наличие резервных копий — это не гарантия восстановления

Одно из самых оживленных обсуждений на сессии развернулось вокруг резервного копирования. Формально для большинства крупных компаний создание резервных копий давно стало базовой частью киберзащиты. Однако дискуссия показала: сам факт наличия бэкапов еще не означает, что бизнес действительно сможет восстановиться.

Георгий Старостин подчеркнул, что в случае масштабной атаки резервирование должно рассматриваться не как единый технический инструмент, а как многослойная система. По его словам, один из самых надежных контуров — физические изолированные копии с воздушным зазором: съемные кассеты, ленточные носители и другие варианты, которые не зависят от общей цифровой среды. Но такая изоляция имеет и обратную сторону — скорость восстановления. Перенос больших массивов данных с ленты может занимать от 72 до 720 часов в зависимости от объема, а значит, такие копии важны для сохранности, но не всегда подходят для быстрого возврата бизнеса в рабочий режим.

Именно поэтому на сессии эксперты отметили необходимость поддерживать несколько независимых уровней резервирования: горячих копий — для быстрого запуска критичных сервисов, холодных — для физической изоляции, а также разнесенных контуров хранения, которые не зависят от одной инфраструктурной цепочки отказа.

При этом, как подчеркнул Георгий Старостин, важны и сами процессы, а не только оборудование. По его статистике, даже там, где резервные копии существуют, примерно в 30% случаев восстановление из них в полном объеме невозможно из-за сбоев носителей, ошибок копирования или других технических причин. Поэтому компаниям необходимо не просто усиливать защиту, а всегда иметь план Б.

Дополнительные практические подробности этой темы раскрыл и кейс ВСК. Роман Фролов признался, что даже наличие ленточных копий не всегда означает возможность восстановления. В ходе инцидента часть резервных данных оказалась недоступной, а некоторые процессы резервирования пришлось пересматривать уже после атаки.

Учения вместо ВСР на бумаге: несколько суток без цифровых систем

Если кейс ВСК показал, как компания восстанавливается после удара, то ТМК продемонстрировала другой подход — сознательную проверку непрерывности бизнеса до наступления кризиса.

Как рассказал Дмитрий Якоб, в компании давно существовали и business continuity plan (BCP), и disaster recovery plan (DRP). Но насколько эти документы соответствуют реальности, если речь идет не о локальном сбое, а о потере критических цифровых контуров? Сначала компания проводила стандартные ИТ-проверки: восстановление систем из резервных копий, миграции между основным и резервным ЦОД, тестирование отдельных технических сценариев. Однако затем было принято решение поднять эти проверки на корпоративный уровень: сотрудникам предстояло столкнуться с имитацией кибератаки и прожить несколько суток без информационных систем.





Дмитрий Якоб поделился, как ТМК проверила готовность бизнеса к работе без критических цифровых систем

Подготовка заняла около полугода. В работу были вовлечены генеральный директор, заместители по ключевым функциям, владельцы бизнес-процессов, рабочие группы и отдельный штаб. В компании начали разбирать не только технические контуры, но и реальную жизнеспособность бизнеса: какие процессы завязаны на конкретные информационные системы, что произойдет, если эти системы перестанут функционировать, как подразделения будут работать без привычной цифровой среды.

Дмитрий Якоб

«Неделю мы жили полностью на резервных каналах связи и резервных мощностях, а затем несколько дней заняло обратное восстановление. И конечно, много чего обнаружилось».

Главный вывод ТМК заключался в том, что ВСП-планы на бумаге работают только до тех пор, пока компании не сталкиваются с реальностью. В процессе подготовки пришлось заново инвентаризировать зависимости между системами, актуализировать инструкции, проверять ручные сценарии и уточнять реальные маршруты эскалации.

ИТ, ИБ и бизнес: обеспечение непрерывности стало общей задачей

В рамках дискуссии эксперты также обсудили разрыв между ИТ, информационной безопасностью и бизнесом — исторически эти функции в крупных компаниях часто развивались в разных вертикалях. Департамент ИТ отвечал

за инфраструктуру и восстановление, подразделение ИБ — за защиту и регуляторику, а бизнес-юниты — за операционные процессы. Но в момент серьезного инцидента такая разобщенность быстро становится слабым местом.

Участники сессии отметили: универсальной модели управления не существует, однако необходимо установить тесные связи между перекрестными функциями актуальна для всех компаний. Где-то, как в «СОГАЗе», такую задачу решают в ходе совместной работы комиссий ИТ и ИБ. Где-то, как в ТМК, кибербезопасность интегрировали в ИТ-вертикаль, чтобы быстрее принимать решения и не терять время на долгие согласования.

Дмитрий Якоб

«Когда случаются какие-то инциденты, то превалируют технические меры защиты — нужно просто оперативно принимать решения, быстро действовать. Наш опыт показывает, что концентрация компетенций кибербезопасности в ИТ очень сильно упрощает жизнь и позволяет безотлагательно принимать решения и реализовывать их».

Главным выводом в этой части дискуссии стало то, что обеспечение непрерывности бизнеса больше не является задачей лишь одной функции. Требуется общая ответственность — ИТ, ИБ, руководства и владельцев бизнес-процессов.

Именно эта мысль в итоге стала ключевой для всей сессии на конференции ЦИПР-2026. Помимо проблемы непрерывности бизнеса, участники уделили внимание достижению зрелости компаний — способности не только предотвращать инциденты, но и признавать неизбежность риска, быстро адаптироваться и восстанавливаться под давлением. В эпоху, когда кибератака все чаще становится не техническим сбоем, а полноценным бизнес-кризисом, устойчивыми оказываются не те, кто рассчитывает на абсолютную защиту, а те, кто заранее выстраивает процессы, проверяет их в реальных сценариях и умеет возвращать бизнес к жизни быстрее, чем развивается сам кризис. ●



ОТРИЦАТЬ НЕЛЬЗЯ ПРИЗНАТЬ



КАК КОМПАНИИ
ГОВОРЯТ
О КИБЕРАТАКАХ



Кибератака запускает в компании сразу два кризиса — технический, когда нужно остановить атаку и восстановить системы, и коммуникационный, когда необходимо объяснить клиентам и партнерам, что произошло. При этом репутационные последствия часто зависят не столько от масштаба самого инцидента, сколько от выбранной стратегии поведения. Одни компании отрицают атаку или маскируют ее под технический сбой, другие — признают проблему лишь частично, третьи — открыто рассказывают о произошедшем и своих дальнейших действиях. Разбираемся, как работают стратегии отрицания, торга и принятия, к каким последствиям они приводят и какие действия в первые часы после киберинцидента помогают сохранить доверие рынка.

Отрицание, торг и принятие — это не всегда последовательные этапы, которые проходит организация. Скорее — три возможные стратегии, одну из которых бизнес должен выбрать в первые часы и дни после инцидента. Причем выбранная позиция повлияет не только на текущую репутацию, но и на число кризисов, которые компании придется пережить в дальнейшем.

Антон Мерцалов

«Если смотреть на крупные инциденты последних лет, то для репутации бизнеса



ЭКСПЕРТ

Антон Мерцалов,

старший менеджер практики кибербезопасности компании «Технологии Доверия»



ЭКСПЕРТ

Дарья Керценбаум,

директор по коммуникациям и PR компании Kept

обычно оказывается критичным не сам факт атаки, а то, как компания ведет себя после ее обнаружения. Отношение рынка к киберинцидентам заметно изменилось: клиенты, партнеры, работники и регуляторы понимают, что атаковать могут практически любую организацию. Однако ожидания в отношении реакции бизнеса теперь иные: клиенты и партнеры гораздо легче воспринимают сам факт инцидента, чем ощущение того, что компания пыталась скрыть проблему».

Отрицание: «У нас технические работы»

Первая реакция — попытаться сделать вид, что ничего серьезного не произошло. Компания молчит, называет недоступность сервисов техническим сбоем или плановыми работами, а иногда категорично заявляет, что данные клиентов не пострадали, хотя расследование еще продолжается.

Причины такой реакции понятны. Руководство боится паники, оттока клиентов, внимания

регуляторов и снижения выручки. Возникает надежда на то, что ИТ-команда быстро восстановит системы, а инцидент удастся оставить внутри компании. Но информационный вакуум редко сохраняется надолго. О взломе могут первыми рассказать злоумышленники, сотрудники, отраслевые каналы или СМИ. После этого бизнесу придется объяснять уже не только саму атаку, но и замалчивание последствий.

Дарья Керценбаум

«Попытка скрыть информацию однозначно наносит большой и долгосрочный ущерб. Кибератака сегодня — это технический вызов, которого практически невозможно избежать, но который компания способна преодолеть. Скрытие же — этический провал, ставящий под сомнение саму надежность компании как партнера. В модели “отрицание — торг — принятие” отрицание и попытка скрыть инцидент за “техническими работами” — самая разрушительная стратегия. Как только вскрывается правда, компания получает двойной удар: за техническую уязвимость и за попытку обмана».

Одним из самых известных примеров отрицания стала реакция компании Uber на утечку данных в 2016 году. Тогда злоумышленники использовали украденные учетные данные, чтобы проникнуть в закрытый репозиторий исходного кода Uber. Там они обнаружили ключ доступа к облачному хранилищу компании и с его помощью скопировали данные миллионов пользователей и водителей.

Вместо того чтобы сообщить об инциденте, Uber выплатила злоумышленникам 100 тыс. долл. в обмен на неразглашение информации и удаление похищенных данных. Компания не сообщила о взломе Федеральной торговой комиссии США, которая в тот момент уже расследовала другой инцидент, связанный с безопасностью данных Uber. Публично об атаке стало известно примерно через год, после



МЛН

ПОЛЬЗОВАТЕЛЕЙ И ВОДИТЕЛЕЙ UBER, ЧЬИ ДАННЫЕ СКОПИРОВАЛИ ЗЛОУМЫШЛЕННИКИ

смены руководства компании. В итоге инцидент превратился в историю не столько о недостаточной защите данных, сколько о намеренном сокрытии произошедшего.

Кейс Uber показывает главную опасность отрицания: компания получает не один кризис, а два. Сначала ей приходится отвечать за утечку данных, а затем — за решение скрыть ее от пользователей и регуляторов. При этом второй кризис нередко оказывается болезненнее первого, поскольку ставит под сомнение уже не качество технологий, а надежность самого бизнеса.

Торг: признать, но не до конца

Полное отрицание становится все менее жизнеспособной стратегией, поэтому компании чаще занимают промежуточную позицию — торг. Речь здесь идет не о переговорах с хакерами и выплате выкупа, а о попытке признать проблему лишь частично и выиграть время.

Компания уже признаёт, что столкнулась с проблемой, но старается максимально уменьшить ее масштаб: «зафиксирована подозрительная

активность», «затронута часть инфраструктуры», «основные системы работают штатно». Иногда такие формулировки продиктованы осторожностью: расследование действительно продолжается, а подтвержденных данных мало. Но торг начинается там, где осторожность превращается в намеренное преуменьшение последствий.

Бизнес пытается выиграть время: сначала сообщить минимум, затем дожидаться результатов расследования и только после этого раскрыть детали. Риск заключается в том, что новые факты могут противоречить первоначальной версии.

Антон Мерцалов

«Наиболее рискованными стратегиями остаются отрицание или попытка выиграть время за счет неполного раскрытия информации. Когда компания сначала заявляет об отсутствии серьезных последствий, затем признает часть инцидента, а позже вынуждена пересматривать собственную позицию, возникает уже не один кризис, а несколько последовательных кризисов доверия. Поэтому раннее признание факта атаки — без преждевременных выводов о ее масштабе — в большинстве случаев оказывается более устойчивой стратегией».

Вот почему в первые часы особенно опасны типовые формулировки. Если в дальнейшем заявление придется корректировать, аудитория запомнит не то, что расследование помогло установить новые обстоятельства, а то, что первоначальные слова оказались неверными. При этом контролируемое раскрытие информации о произошедшем само по себе не является торгом. Компания не обязана сразу публиковать технические подробности, возможные версии атаки или точное количество затронутых записей. Граница проходит между осторожностью и попытками создать заведомо более благополучную картину.

Корректная позиция звучит так: факт инцидента подтвержден, расследование продолжается, окончательный масштаб пока не установлен. Некорректная: серьезных последствий нет, — хотя компания еще не может этого знать.

Принятие: сначала факты — затем оценки

Стадия принятия начинается с признания реальной реальности: инцидент уже произошел, компания сама становится основным источником сведений, приводит подтвержденные факты, прямо обозначает границы известного и регулярно обновляет информацию.

При этом одного публичного признания недостаточно. Открытая коммуникация работает только в том случае, когда внутри организации уже создан кризисный штаб, определены ответственные и налажен постоянный обмен информацией между ИБ, ИТ, юристами, PR-службой и руководством.

Дарья Керценбаум

«Принятие требует внутренней компетенции. Заявить “мы атакованы, разбираемся” при видимом хаосе внутри

В модели «отрицание — торг — принятие» отрицание и попытка скрыть инцидент за «техническими работами» — самая разрушительная стратегия. Как только вскрывается правда, компания получает двойной удар: за техническую уязвимость и за попытку обмана



МЛН РУБ.

**ПОТЕРИ 12 STOREEZ
ИЗ-ЗА ПРОСТОЯ
(23 МЛН) И
НЕСОСТОЯВШИХСЯ
ПРОДАЖ (20 МЛН),
А ТАКЖЕ РАСХОДЫ
НА ПРИВЛЕЧЕНИЕ
ВНЕШНИХ
СПЕЦИАЛИСТОВ
И ЮРИДИЧЕСКОЕ
СОПРОВОЖДЕНИЕ
(5 МЛН)**

компании почти так же разрушительно, как и замалчивание. Компания должна быть первым и главным источником информации о кризисе для всех аудиторий. Для этого необходимо активировать кризисную группу, наладить постоянный сбор фактов и назначить одного спикера по теме. Первое сообщение должно содержать факт инцидента, информацию о принятых мерах и контакт для запросов, а дальше необходимо регулярно обновлять сведения».

Показательным примером такой стратегии стала реакция российского бренда одежды 12 Storeez на атаку, случившуюся летом 2025 года. В ночь с 8 на 9 июня хакеры получили доступ к корпоративной инфраструктуре. Они зашифровали и удалили часть данных, а также повредили около 30% резервных копий. В магазинах начались сбои в работе касс, возникли очереди, временно перестали работать сайт и мобильное приложение.

16 июня бренд публично сообщил, что подвергся самой масштабной хакерской атаке в своей истории. Компания не стала объяснять происходящее плановыми техническими работами: она рассказала о проблемах с внутренними системами из-за взлома, извинилась перед клиентами и продолжила делиться информацией о восстановлении сервисов. Позже представители бренда сообщили, что одной из причин успешного проникновения киберпреступников стало отсутствие многофакторной аутентификации для внешнего доступа. Злоумышленники потребовали 20 млн руб. в криптовалюте за ключи дешифрования и неразглашение информации, но бренд отказался платить выкуп.

Именно поэтому случай 12 Storeez можно отнести к полному принятию. Компания не ограничилась дежурными фразами, а объяснила, что именно произошло, почему защита не сработала, каких потерь это стоило и как проходило восстановление. Бренд открыто рассказал и о требовании выкупа, и о собственных недостатках, не пытаясь представить атаку исключительно как внешнее и совершенно непредотвратимое событие.

Такая коммуникация не уменьшает последствия атаки, но меняет отношение аудитории: клиенты видят организацию, которая способна признать проблему, отвечать за свои решения и делать выводы.

ПЕРВЫЕ СУТКИ КИБЕРИНЦИДЕНТА: ПЛАН ДЕЙСТВИЙ



ПЕРВЫЕ 1–2 ЧАСА

АКТИВИРОВАТЬ КРИЗИСНЫЙ ШТАБ

Подключить руководство компании, ИБ- и ИТ-службы, юридический блок, PR, а также подразделения, отвечающие за работу с клиентами и партнерами. При необходимости привлечь внешних специалистов по расследованию инцидентов и кризисным коммуникациям.

ОПРЕДЕЛИТЬ ПОРЯДОК ПРИНЯТИЯ РЕШЕНИЙ

Зафиксировать, кто собирает и проверяет информацию, кто согласовывает сообщения и кто имеет право выступать от имени компании.

СОЗДАТЬ ЕДИНЬЙ КОНТУР ОБМЕНА ИНФОРМАЦИЕЙ

Все участники кризисного штаба должны опираться на одну версию событий и использовать только подтвержденные данные.

НЕ ИСКАТЬ ВИНОВНЫХ И НЕ ОЦЕНИВАТЬ УЩЕРБ ПРЕЖДЕВРЕМЕННО

В первые часы информация почти всегда неполна, поэтому поспешные выводы могут привести к ошибочным заявлениям.

ПЕРВЫЕ 4–8 ЧАСОВ

ПОДГОТОВИТЬ ПЕРВОЕ ОФИЦИАЛЬНОЕ СООБЩЕНИЕ

В нем следует подтвердить факт инцидента, сообщить о начале расследования и о привлечении необходимых специалистов, а также пообещать обновлять информацию в дальнейшем.

ГОВОРИТЬ ТОЛЬКО О ПОДТВЕРЖДЕННЫХ ФАКТАХ

Не стоит давать окончательную оценку масштаба атаки, состояния систем или возможной утечки, пока расследование продолжается.

ПОДГОТОВИТЬ СООБЩЕНИЯ ДЛЯ РАЗНЫХ АУДИТОРИЙ

Сотрудникам, клиентам, партнерам, регуляторам и СМИ нужна разная степень детализации, но фактическая основа всех сообщений должна оставаться единой.

ПЕРВЫЕ 24 ЧАСА

ПЕРЕЙТИ К РЕГУЛЯРНЫМ ОБНОВЛЕНИЯМ

Даже если новых подтвержденных данных пока нет, важно сообщать, что расследование продолжается и ситуация находится под контролем.

НЕ ДОПУСКАТЬ ИНФОРМАЦИОННОГО ВАКУУМА

При длительном молчании пространство быстро заполняется слухами, предположениями и версиями внешних источников.

СОХРАНЯТЬ ПОСЛЕДОВАТЕЛЬНОСТЬ СООБЩЕНИЙ

Новые заявления не должны противоречить предыдущим. Если информация уточняется, необходимо прямо объяснить, что именно изменилось.

СЛЕДОВАТЬ ГЛАВНОМУ ПРИНЦИПУ ОТКРЫТОЙ КОММУНИКАЦИИ

Говорить раньше внешних источников, но приводить только проверенные факты. Такой подход дает компании больше шансов сохранить доверие клиентов, партнеров и рынка.

РЕШАЕТ РЕАКЦИЯ

После кибератаки компания отвечает не только за то, насколько быстро восстановит системы, но и за то, как будет говорить о произошедшем. Отрицание почти всегда усиливает кризис, торг лишь откладывает неизбежное и неприятные вопросы, а принятие дает шанс сохранить контроль над повесткой и доверие аудитории.

В первые часы важно подтвердить факт инцидента, не делать преждевременных выводов и последовательно сообщать только проверенную информацию. А после завершения расследования — рассказать о причинах, последствиях и мерах, которые помогут избежать повторения атаки. Сам факт киберинцидента рынок все чаще воспринимает как риск, от которого не застрахована ни одна компания. Гораздо строже оценивается то, что происходит после: пытается ли бизнес скрыть проблему или способен признать ее, взять ответственность и сделать выводы. 🌐



«МЫ В СВОЕЙ ОТКРЫТОЙ ПОЗИЦИИ ВИДИМ ВКЛАД В ОБЩУЮ КИБЕРБЕЗОПАСНОСТЬ»

РОМАН ФРОЛОВ,
член Совета директоров Страхового Дома ВСК

Фото: Карэн Эгнатосян

Киберустойчивость начинается с неприятного признания: идеальной защиты не существует. В ноябре 2025 года Страховой Дом ВСК столкнулся с масштабной кибератакой, которая нарушила работу ключевых систем и потребовала длительного восстановления. Этот опыт заставил компанию пересмотреть не только технические подходы, но и логику управления кризисом. В интервью JetInfo член Совета директоров ВСК Роман Фролов рассказал, как компания восстанавливалась после атаки, как повели себя конкуренты, к чему привела открытая коммуникация и почему киберустойчивость давно перестала быть задачей только ИБ.

— Роман, до инцидента 2025 года что для вас лично означала непрерывность бизнеса? И насколько это представление изменилось после того, как компании пришлось пройти через разрушительную кибератаку? Был ли у вас этап отрицания происходящего?

— Я бы не сказал, что у нас был этап отрицания. Скорее, сначала было непонимание масштаба происходящего. До этого мы сталкивались либо с локальными техническими сбоями, либо с киберинцидентами меньшего масштаба. Например, могло пропасть электричество, но серверная продолжала работать на резервных источниках. Иногда возникали более длительные простои на стороне внешних сервисов, от которых

зависели отдельные процессы — например, получение данных при страховании ОСАГО.

То, что произошло 11 ноября, в первые минуты тоже воспринималось как временная остановка: казалось, что еще немного — и все заработает. Но с каждой минутой становилось понятнее, что в ближайшее время ничего не восстановится. Примерно через час после инцидента собралось правление — и были приняты первые организационные решения. Полного понимания масштаба катастрофы в тот момент, конечно, еще не было.

Раньше казалось, что на непрерывность бизнеса в первую очередь влияют внешние факторы: регуляторная среда, макроэкономическая обстановка, технологические тренды, которым должна следовать любая финансовая компания. Но наш опыт показал, что устойчивость бизнеса не меньше зависит от внутренних факторов — инфраструктуры, уровня защиты и готовности компании быстро восстановиться.

— Если устойчивость бизнеса во многом определяется внутренней готовностью к восстановлению, то кто должен быть в центре этого процесса? Это зона ответственности службы ИБ?

— Важно понимать: ИБ-специалисты не могут решить такую ситуацию в одиночку. Они могут защищать внешний и внутренний периметр, локализовывать отдельные угрозы, но восстановление работы компании после масштабной атаки — это вопрос не только информационной безопасности.

Речь идет об организации работы всей команды, принятии управленческих решений, расстановке приоритетов. Ключевая роль здесь принадлежит прежде всего первому и второму уровням управления. Именно топ-менеджмент напрямую влияет на то, как быстро компания сможет сориентироваться, перестроить работу и начать восстановление.

— В момент инцидента какие решения остаются на уровне первого лица компании, а какие должны уходить в работу функциональных и технических команд?

— В такой ситуации нельзя ждать, пока «технические специалисты разберутся»: фокус всего топ-менеджмента должен быть немедленно переключен на восстановление. Первое решение — собрать



Во время инцидента ВСК продолжала урегулировать убытки в Москве и регионах, выполняя обязательства перед клиентами и партнерами

кризисный штаб под руководством генерального директора и сразу разложить работу по функциональным группам. У каждого направления должна быть понятная зона ответственности: кто отвечает за инфраструктуру, кто — за ИБ, кто — за коммуникации с сотрудниками, регуляторами, правоохранительными органами, клиентами и партнерами.

Нужна регулярная сверка — например, совещания штаба каждые два часа, где быстро фиксируется, что уже сделано, что заблокировано, какие решения нужно принимать немедленно и какие ресурсы требуются командам.

Очень помогает визуальное управление — условная канбан-доска, на которой весь процесс

восстановления виден как на ладони. Роль первого лица в такой системе — принимать стратегические решения: утверждать план восстановления, выделять ресурсы, обеспечивать взаимодействие с регуляторами и участвовать в публичной коммуникации. Операционное управление при этом должно оставаться за топ-менеджерами второго уровня.

Отдельно стоит упомянуть, что важно заранее составить перечень партнеров, которые в момент аварии максимально оперативно помогут организовать процесс восстановления. И конечно, к такой ситуации нельзя готовиться только на бумаге. Лучший способ проверить реальную готовность команды — киберучения. Например, моделирование масштабного сбоя, что, несмотря на стоимость, является бесценной инвестицией в устойчивость.

— На ЦИПР-2026 вы отмечали, что восстановление заняло месяц.

— Сроки зависели от конкретных систем. Если говорить о продающем контуре, то его мы восстанавливали примерно три недели. Но важно понимать: продающий контур не существует сам по себе. За фронт-офисными решениями стоят базы данных, учетные системы, печатные формы, системы принятия решений и тарификации, API-интеграции с партнерами и другие внутренние сервисы. Если этот фундамент нестабилен, нет смысла запускать пользовательские приложения — они просто не смогут корректно работать.

Инфраструктуру мы восстановили раньше, но для бизнеса ключевым показателем стал именно запуск продаж. Нам помогло то, что продающий контур в основном построен на микросервисной архитектуре: у нас не было одной большой монолитной системы, восстановление которой могло бы занять неопределенно долгое время. При этом ряд критичных процессов мы не останавливали ни на минуту. Например, урегулирование убытков продолжало работать и в Москве, и в регионах,



потому что для нас было принципиально важно выполнять обязательства перед клиентами и партнерами.

— А как это работало на практике?

— Мы продолжали принимать заявления на урегулирование, хотя какое-то время не могли полноценно сопоставлять их с данными в системах и проверять, действительно ли полис был оформлен у нас. Конечно, мы понимали, что теоретически это создает риск фрода: человек мог прийти с недействительным или поддельным полисом, а в моменте у нас не было технической возможности быстро это проверить. Но мы осознанно приняли на себя этот риск, потому что остановка урегулирования была бы для клиентов очень болезненной. Позже, когда мы ретроспективно проанализировали все выплаты и обращения за этот период, оказалось, что фактического мошенничества не было.

Помимо этого, поняв, что у нас не работает контакт-центр по ДМС, мы в течение нескольких часов переключили обслуживание на подрядчика с сохранением прежних номеров. Это позволило продолжить работу с клиентами. Инцидент инцидентом, но людям может понадобиться скорая помощь, консультация или другая срочная поддержка.

— В вашей истории восстановление затянулось во многом потому, что злоумышленники полностью уничтожили резервные копии в одном из ЦОД. По вашим оценкам, почему им удалось это сделать? В архитектуре хранения бэкапов была уязвимость?

— Слабая точка в таких историях редко бывает одна. Обычно это цепочка обстоятельств, которая срабатывает как эффект домино. В нашем случае дополнительным фактором стало то, что мы как раз находились в процессе переезда из одного ЦОД в другой. Переезд шел по графику, но технически еще не был завершен, поэтому между двумя площадками сохранялись каналы связи. В результате бэкапы в первом ЦОД были повреждены. Если бы они уже успели полностью переехать во второй ЦОД, где резервные копии не пострадали, восстановление прошло бы значительно быстрее. Поэтому проблема не в том, что сама идея резервного копирования не работает. Она работает, но только если бэкапы действительно изолированы от продуктивной среды.

ВСК регулярно проводит внешние и внутренние пентесты, проверяя уязвимости, скорость реакции SOC и процессы эскалации

— Роман, а что происходит с командой, когда неделями приходится работать в таком напряженном режиме?

— Вообще, в таких условиях очень быстро становится видно, кто чего стоит. Команда ВСК показала себя очень слаженной и надежной. Никого не приходилось заставлять выходить на работу не по графику: все понимали, что в любой момент может потребоваться их ресурс. После случившегося мы вместе с генеральным директором и правлением решили отдельно отметить людей, которые особенно активно участвовали в восстановлении, и создали номинацию «Герои ВСК» — коллеги получили и денежные премии, и публичное признание. Для нас было важно, чтобы люди почувствовали: их вклад увидели и оценили.

Что касается топ-менеджмента, мы не писали код и не могли заменить ИТ-специалистов, но своим примером показывали командам второго и третьего уровней, как нужно относиться к компании и к делу в кризисной ситуации. Тогда многие из нас впервые глубоко погрузились в темы, которые раньше казались набором непонятных аббревиатур. К слову, у меня, как и у многих топ-менеджеров и членов правления, первый выходной после атаки был только 31 декабря. Хотя продающий контур мы запустили примерно через три недели после инцидента, нам еще предстояло восстановить страховой учет, контур безопасности, отдельные внутренние процессы.

— Помимо огромной нагрузки, в такие моменты в коллективе возникает много тревоги и слухов. Что помогало удерживать нормальную атмосферу внутри компании?

— Да, мы понимали, что в регионах слухов может быть даже больше, чем в Москве, поэтому старались регулярно информировать сотрудников о происходящем. Несмотря на то, что многие системы не работали, мы смогли собрать большую видеоконференцию с региональными точками продаж и провести ежемесячное подведение итогов — как делали это всегда. Очень показательная история — выплата аванса. Инцидент произошел 11-го числа, а 15-го коллектив должен был получить деньги. Внутренние системы учета рабочего времени не работали, но банк-клиент был доступен. Мы приняли решение повторить октябрьский платеж, вручную исключили тех, кто к этому моменту уволился, и выплатили аванс в срок. На первый взгляд, это операционная

деталь, но для атмосферы в коллективе она имела огромное значение: сотрудники чувствовали стабильность.

— А как выстраивались внешние коммуникации?

— Мы сразу проинформировали регулятора, налоговую службу, правоохранительные органы, подали необходимые заявления и начали выстраивать коммуникацию с клиентами и партнерами. Наша позиция была простой: лучше рассказать самим, чем ждать, пока за тебя это сделает кто-то другой. Мы не стали объяснять происходящее «техническими работами» или просить подождать пару дней — почти сразу на сайте разместили баннер с сообщением о том, что произошел киберинцидент. При этом подчеркнули главное: компания продолжает выполнять свои обязательства.

Открытая позиция помогла и во взаимодействии с рынком. У нас возникли сложности с продажей ОСАГО, а это обязательный вид страхования, который должен быть доступен по всей территории России. Коллеги по страховому рынку, в том числе конкуренты, повели себя как партнеры: помогли с запасами полисов, чтобы мы могли обеспечить ими филиалы и продолжить работу. Недобросовестной конкуренции в этот момент не было, и это действительно дорогого стоит.

То же самое касается партнеров по восстановлению. Многие подключались очень быстро, еще до оформления контрактов и согласования бюджетов, потому что понимали: в такой ситуации нельзя терять время на бюрократию.

— Ваша открытая позиция впечатляет. Далеко не все компании рассказывают о кибератаках публично...

— Мы в своей открытой позиции видим в том числе вклад в общую безопасность. Сегодня кибератаки — не исключение, а реальность, с которой может столкнуться любая организация. По данным исследования компании «Инфосистемы Джет», в 2024 году в России было более 31 тыс. кибератак на различные предприятия, в 2025-м — уже 105 тыс., а за первое полугодие этого года — примерно столько же, сколько за весь прошлый год. На фоне таких цифр какой смысл делать вид, что проблема вас не касается?

Наш опыт может помочь другим компаниям лучше подготовиться и быстрее сориентироваться



Компания открыто рассказывает об инциденте и восстановлении на отраслевых площадках и референс-визитах, вовлекая в разговор не только ИБ-специалистов, но и руководителей бизнеса

в кризисе. Поэтому мы продолжаем открыто говорить о том, что произошло: выступаем на отраслевых площадках, рассказываем о восстановлении, приглашаем партнеров на референс-визиты в наш офис. Причем зовем не только специалистов по ИБ, но и собственников, генеральных директоров, топ-менеджеров. Потому что киберустойчивость не должна оставаться темой только безопасников. Когда первые лица слышат от первых лиц, как атака влияет на бизнес, продажи, клиентов, сотрудников и партнеров, отношение к этой теме меняется молниеносно.

— После произошедшего вы честно признавали, что существовавший в компании план непрерывности бизнеса оказался не до конца применимым к реальности. Как считаете — почему?

— Не могу сказать, что наш ВСП оказался формальным или плохим: это был нормальный, рабочий документ. Но такие планы часто пишутся по учебникам и методологиям. А когда все происходит в реальности, выясняется, что между методологией и практикой может быть очень большая дистанция.

Можно подробно описать, что делать при отказе конкретной системы, сбое отдельного сервиса или потере части инфраструктуры. Но когда одновременно реализуется много рисков, да еще с катастрофическими последствиями, привычного сценария недостаточно. Большинство компаний в ВСП чаще прорабатывают наиболее вероятные события, а не самые масштабные. У нас тоже были хорошо описаны и детально разобраны сценарии по отдельным системам, но мы не предполагали, что повреждение окажется комплексным.

Поэтому я бы сказал так: наш ВСП был полезен, но не рассчитан на кризис такого масштаба. После получения подобного опыта становится понятно, что план непрерывности бизнеса должен не просто описывать вероятные сбои, а проверять готовность компании к действительно катастрофическим сценариям. Причем



Для самых активных участников восстановления в ВСК создали номинацию «Герои ВСК»

не на бумаге, а на практике: через тестирование планов аварийного восстановления (*DRP*), восстановление из резервных копий, моделирование масштабных отказов.

— Свой ВСП, очевидно, вы переработали?

— Да, и продолжаем перерабатывать дальше. Он должен постоянно обновляться с учетом новых рисков. Сейчас мы оцениваем сценарии с точки зрения не только вероятности, но и возможных катастрофических последствий. Это большая системная работа: ею занимается отдельное подразделение.

СТОПРОЦЕНТНОЙ ЗАЩИТЫ НЕ СУЩЕСТВУЕТ. ЕСЛИ ЗЛОУМЫШЛЕННИКИ ЦЕЛЕНАПРАВЛЕННО ХОТЯТ АТАКОВАТЬ КОМПАНИЮ, ОНИ БУДУТ ИСКАТЬ РАЗНЫЕ ПУТИ

— А как после атаки изменился подход к проверке защищенности? Вы стали чаще проводить разного рода учения?

— Безусловно, средства информационной защиты у нас были и до атаки: работал центр ИБ (SOC), использовались разные инструменты мониторинга и защиты. Возможно, какие-то проверки, например пентесты, проводились не так часто, как это необходимо в сегодняшних условиях, но защита была. При этом важно понимать: стопроцентной защиты не существует. Если злоумышленники целенаправленно хотят атаковать компанию, они будут искать разные пути: через подрядчика, напрямую, через уязвимости в инфраструктуре или сотрудников. Даже двухфакторная аутентификация сама по себе не является гарантией.

Сейчас мы регулярно проводим пентесты и делаем это в разных форматах. Есть внешние подрядчики, которые пытаются найти уязвимости со стороны, а есть внутренние проверки — своего рода мини-провокации, которые позволяют понять, как реально работает защита сейчас: насколько быстро реагирует SOC, видит ли он подозрительную активность, как отрабатывает процессы эскалации.

— Если говорить о последствиях масштабных кибератак для бизнеса, что в итоге обходится дороже всего: техническое восстановление, простой, репутационные риски, потеря клиентов?

— Если говорить о прямых потерях, то дороже всего, конечно, обходится простой. Для компании с сотнями миллионов рублей ежедневного оборота каждый день остановки — это очень большие деньги. Расходы на техническое восстановление тоже существенные, но на фоне стоимости простоя они уже не выглядят главным источником потерь.

Мы теперь с полной осознанностью, как страховщики, прошедшие через кибератаку, предлагаем нашим партнерам услугу киберстрахования. Это сервисно-страховой продукт: с одной стороны, компенсация расходов, с другой — практическая помощь в восстановлении. Потому что, когда все уже случилось, главный вопрос не только в том, сколько вам возместят, но и в том, кто может снова запустить бизнес.

— Что вы посоветуете компаниям, которые пока не проходили через такой кризис?

— В первую очередь помнить: вопрос уже не в том, случится атака или нет, а в том, когда она произойдет. А значит, следует заботиться не только о кибербезопасности, но и о киберустойчивости. Заранее, еще до наступления кризиса, продумывать, как будете восстанавливать инфраструктуру, процессы, какие ресурсы для этого понадобятся. Оценивать все действия компании не только через призму того, насколько хорошо закрыт периметр, но и задавая вопрос: как быстро бизнес сможет подняться из руин? 🌐



ЦИФРОВОЙ РУБЕЖ ДОВЕРИЯ

КАК КИБЕРРИСКИ ВЛИЯЮТ
НА ИНВЕСТИЦИОННЫЙ
ЛАНДШАФТ



АВТОР

Олег Абелев,

кандидат экономических наук, декан
факультета международных финансов
Всероссийской академии внешней торговли
(ВАВТ), начальник аналитического отдела
инвестиционной компании «Риком-Траст»,
доцент кафедры финансов и валютно-
кредитных отношений ВАВТ, доцент Высшей
школы бизнеса НИУ ВШЭ

Еще несколько десятилетий назад отношения между эмитентом и инвестором определялись фактом физического обладания ценными бумагами и строились на личных встречах для совершения сделки. Сегодня же взаимодействие между участниками финансового рынка опосредовано сложной многоуровневой цифровой инфраструктурой. В этой парадигме информация уже не просто сопроводительный элемент сделки — она стала самым активом. А уязвимость цифрового контура компании тождественна уязвимости ее рыночной стоимости.

Цифровизация не только многократно повысила эффективность и скорость операций, но и породила уникальную зависимость: доверие, которое всегда являлось краеугольным камнем инвестиционного процесса, вышло за рамки отношений контрагентов — теперь оно неразрывно связано с состоянием кода, протоколов передачи данных и архитектурой информационной безопасности.

Именно по этой причине кибербезопасность из узкоспециализированной технической функции ИТ-департаментов превратилась в фундаментальный фактор, определяющий не только капитализацию компаний, но и саму способность рынка выполнять функцию справедливого ценообразования. Вопрос защиты данных уверенно трансформировался в вопрос защиты корпоративного суверенитета и капитала участников рынка, что создало новую систему координат.

Киберинциденты и феномен «цифрового гудвилла»

Исторически фондовый рынок реагирует на негативные новости с временным лагом, требующимся для осмысления информации. Кибератака ломает эту модель. Инцидент, будь то проникновение в инфраструктуру шифровальщика, парализующего операционную деятельность, или кража чувствительных данных клиентов, вызывает мгновенную и часто иррациональную реакцию алгоритмических трейдеров. Однако за волатильностью первого дня следует более глубокая переоценка.

Для инвестора утеря данных — это не просто репутационный удар. Это прямые финансовые последствия, которые мгновенно отражаются на стоимости акций: регуляторные штрафы, достигающие 4% годовой выручки в рамках Общего регламента по защите данных граждан Европейского союза (*GDPR*), затраты на восстановление систем, судебные издержки из-за коллективных исков акционеров и отток клиентов. В российской юрисдикции с 2024 года также введены существенные оборотные штрафы для юридических лиц за утечки персональных данных — до 3% совокупной годовой выручки. А экспертно-аналитический центр InfoWatch и компания «Циркон» по итогам совместного исследования в 2024 году оценили средний ущерб российских организаций от одной утечки информации в 11,5 млн руб.

При этом возникает феномен «цифрового гудвилла»: практически любой нематериальный актив, который отражает доверие к бренду публичного эмитента, при кибератаке получает четкое стоимостное выражение через падение котировок.

Получается, что отныне инвестор (розничный или институциональный) больше не может полагаться исключительно на бухгалтерский баланс, поскольку вынужден оценивать архитектуру сетевой безопасности эмитента при финансовом анализе.

Раскрытие информации: отчет как карта слабых мест

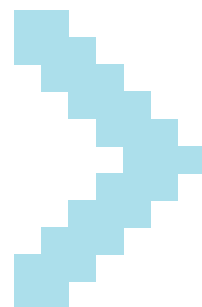
Традиционная модель взаимодействия контрагентов на инвестиционном рынке подразумевает, что эмитент раскрывает существенные факты, касающиеся финансовых результатов компании. В различных юрисдикциях требования регуляторов по вопросу киберинцидентов сегодня сильно различаются: от отсутствия в правовом поле до обязательств публичных компаний сообщать о киберинцидентах, которые могут оказать значительное влияние на бизнес.

Правила, принятые в США в июле 2023 года, требуют от эмитентов разглашения информации о существенном инциденте в течение четырех рабочих дней после его обнаружения, а также периодического описания процессов управления киберрисками в годовых отчетах. Схожий подход развивается и в России: в соответствии с Положением Банка России № 757-П некредитные финансовые организации обязаны уведомлять регулятора о выявленных инцидентах информационной безопасности, а публичные акционерные общества должны раскрывать в ленте новостей существенные факты, способные повлиять на стоимость их ценных бумаг. Это породило сложную дилемму.

С одной стороны, инвестор на рынках всегда и везде требует прозрачности, поэтому раскрытие информации о методах управления киберрисками становится конкурентным преимуществом. Те эмитенты, которые демонстрируют зрелость в этом вопросе и имеют соответствующие рычаги реагирования (*наличие в совете директоров эксперта по кибербезопасности, проведение регулярных стресс-тестов и т. д.*), воспринимаются рынком как более устойчивые.

С другой стороны, излишняя детализация отчетов о попытках взлома может подсказать потенциальным злоумышленникам и киберпреступникам векторы атак. Возникает парадокс «защищенной транспарентности»: коммуникация с инвестором находится на грани между успокоением рынка и предоставлением киберпреступнику конфиденциальных данных. Балансировать на этой грани помогают отраслевые стандарты, такие как NIST Cybersecurity Framework (*рекомендации Национального института стандартов и технологий США*). В российском корпоративном секторе все чаще делают ставку на национальный стандарт ГОСТ Р 57580.1-2017. Он устанавливает уровни защиты для финансовых операций и используется в диалоге с инвесторами как маркер надежности.

ИНВЕСТОР НА РЫНКАХ
ВСЕГДА И ВЕЗДЕ ТРЕБУЕТ
ПРОЗРАЧНОСТИ, ПОЭТОМУ
РАСКРЫТИЕ ИНФОРМАЦИИ
О МЕТОДАХ УПРАВЛЕНИЯ
КИБЕРРИСКАМИ СТАНОВИТСЯ
КОНКУРЕНТНЫМ
ПРЕИМУЩЕСТВОМ



По сути, взаимодействие эмитента с инвестором в текущих условиях смещается от попыток дать количественные гарантии защищенности компании, что в киберсфере практически невозможно, к качественным сигналам через демонстрацию устойчивости инфраструктуры бизнеса.

Кибербезопасность как нефинансовый критерий в ESG-повестке

Наиболее значимый сдвиг в мышлении инвесторов, особенно институциональных, заключается в интеграции кибербезопасности в компоненты «G» (*Governance — управление*) и «S» (*Social — социум*) повестки устойчивого развития. Если управление рисками не способно защитить персональные данные клиентов, то на сегодняшний день большинством рейтинговых агентств это однозначно интерпретируется как грубый провал социальной ответственности.

Рейтинговые агентства, такие как MSCI и Sustainalytics, включают метрики защиты от киберрисков в свои методологии ESG-оценок, где низкий балл автоматически вычеркивает эмитента из портфелей ответственного инвестирования, объем которых исчисляется триллионами долларов США.

Ключевой перелом в трактовке фактора киберрисков в ESG-повестке уже произошел. Раньше эмитент сам выбирал степень публичности в вопросах своего технического оснащения и уровня защиты информации. Сегодня институциональный инвестор формирует запрос к эмитенту, используя целый спектр инструментов: от рассылки детальных анкет, требующих раскрытия архитектуры защиты информации, до подробной истории реагирования эмитента на инциденты с информацией и политики обновления программного обеспечения. Неспособность эмитента предоставить инвестору удовлетворительные ответы на вышеупомянутые вопросы ведет к голосованию представителей инвесторов (*особенно институциональных*) против менеджмента на собраниях акционеров или к прямому выходу из капитала. Таким образом, фактор кибербезопасности становится мощным инструментом

давления и прямого влияния инвестора на операционную стратегию эмитента.

Новый вид асимметрии и «токсичные» активы

Помимо прямого воздействия на стоимость компании, фактор кибербезопасности создает целый ряд скрытых угроз, которые способны исказить сам процесс инвестиционного анализа. Прежде всего стоит сказать об асимметрии информации: лишь ограниченный круг лиц в момент кибератаки может оценить реальный масштаб ущерба, тогда как рынок часто питается слухами. Хрестоматийным стал случай с Yahoo!, когда задержка в раскрытии масштабов утечки данных (*запро- нувшей все 3 млрд учетных записей*) повлияла на оценку компании в процессе сделки с Verizon, что в итоге снизило цену покупки на 350 млн долл. Этот кейс подробно анализировался российскими деловыми изданиями как наглядный пример того, как утаенный киберинцидент способен изменить экономику сделки.

Кроме того, в практике взаимодействия инвесторов и эмитентов на почве отношения к вопросам кибербезопасности встречается феномен «наследования рисков» в сделках слияний и поглощений. Если покупатель, приобретающий долю в компании, не проверил ее цифровой периметр, он сильно рискует получить «токсичный» актив, стоимость которого может лавинообразно измениться не в лучшую сторону из-за закладок в коде или «дремлющих» вредоносных программ, попавших в ИТ-ландшафт еще до сделки.

Случаи, подобные поглощению гостиничной сетью Marriott сети Starwood, когда утечка данных миллионов гостей была обнаружена через несколько лет после покупки, стали предупреждением рынку о том, что будущая сделка без учета киберрисков недопустима, а процедура Due Diligence (*комплексная проверка бизнеса*) должна быть обязательной.

Выводы в эпоху цифровой ответственности

Влияние фактора кибербезопасности на взаимодействие эмитента и инвестора можно охарактеризовать как переход от эпизодической благодетельности в вопросах ИТ-рисков к новой зоне ответственности для инвестора и эмитента.

ДОВЕРИЕ К БРЕНДУ БОЛЬШЕ НЕ ЯВЛЯЕТСЯ ЧЕМ-ТО НЕЗЫБЛЕНЫМ, ТЕПЕРЬ ОНО ЕЖЕДНЕВНО ПОДТВЕРЖДАЕТСЯ НУЛЕВЫМ УРОВНЕМ УТЕЧКИ ИНФОРМАЦИИ

Стоит признать тот факт, что кибербезопасность давно перестала быть статьей расходов сугубо на защиту информационного периметра эмитента и превратилась в ключевой индикатор качества корпоративного управления.

Выделим основные последствия данной трансформации для рынка:

- 1 **Происходит глубокая перестройка коммуникации**
Диалог эмитента и инвестора становится непрерывным и превентивным: теперь вместо отчета раз в квартал эмитент вынужден постоянно информировать широкую общественность об информационной безопасности компании, чтобы не возникло цифрового вакуума при потенциальных киберинцидентах. Доверие к бренду больше не является чем-то незыблемым, теперь оно ежедневно подтверждается нулевым уровнем утечки информации.
- 2 **Рынок пришел к пониманию того, что абсолютной защиты не существует**
Сегодня главным критерием для инвестиционного сообщества становится не наличие максимальной ИБ-защиты у эмитента, а уровень адаптивности компании к меняющейся среде и скорость восстановления доступа к информации и базам данных. Эмитенты, которые способны менее чем за сутки восстановить операции после атаки, возвращают доверие рынка гораздо быстрее, чем те, кто безуспешно и целенаправленно пытается строить иллюзию идеальной защиты. Эта концепция нашла отражение в растущем внимании регуляторов и советов директоров

к планированию непрерывности бизнеса, что подчеркивается, например, в рекомендациях Национального института стандартов и технологий США (NIST) и заложено в ГОСТ Р 57580.1-2017 для российских компаний.

- 3 **У эмитентов меняется философия управления рисками**
Ответственность за кибербезопасность переместилась из серверной в зал заседаний совета директоров и закрепились в обновленных регуляторных требованиях, которые возлагают персональные риски на топ-менеджмент. В России принцип личной ответственности руководителей за убытки, причиненные их неразумными действиями, установлен статьей 53.1 Гражданского кодекса РФ, а нарушение требований безопасности критической информационной инфраструктуры (*Федеральный закон № 187-ФЗ*) влечет уже не только административную, но и уголовную ответственность.

Таким образом, кибербезопасность для публичного эмитента становится фактором, синтезирующим значимость репутации, финансовой и операционной деятельности в единый конгломерат. А инвестор сегодня — это не просто покупатель доли в бизнесе, а в некотором роде «сканер» цифрового суверенитета эмитента. Главный парадокс заключается в том, что глубина погружения участников рынка в среду информационной безопасности прямо коррелирует с уязвимостью эмитентов на рынке, поскольку ключевой ценностью для инвестора сегодня становится именно способность эмитента сохранить целостность данных и непрерывность процессов. ●

У НЕРВНЫЙ СРЫВ ПРОИЗВОДСТВА

С ЧЕГО НАЧИНАЕТСЯ
КИБЕРУСТОЙЧИВОСТЬ АСУ ТП

**ЭКСПЕРТ****Константин
Ильютченко,**

практикующий эксперт
в области защиты
информации на ОКИИ
и АСУ ТП с опытом
работы более 8 лет на
предприятиях ракетно-
космической, химической
и горнодобывающей
промышленности

**ЭКСПЕРТ****Антон
Елизаров,**

начальник отдела защиты
АСУ ТП и КИИ компании
«Инфосистемы Джет»

**ЭКСПЕРТ****Александр
Карпенко,**

руководитель направления
защиты АСУ ТП компании
«Инфосистемы Джет»

Автоматизированная система управления технологическим процессом (АСУ ТП) — это мозг и нервы производства: она принимает сигналы от его сегментов и передает команды в режиме реального времени. Без нее современный завод слеп, глух, парализован и в то же время опасен. В чем особенность киберфизических атак? Что делает АСУ ТП отказоустойчивой и почему это не вечно? Как укрепить защиту и подготовиться к взлому, чтобы избежать остановки выпуска продукции?

Нефтехимический завод, электростанция, водоканал и котельная, пищевое производство — на каждом промышленном и энергетическом предприятии работает АСУ ТП. Автоматизация используется в выпуске большинства видов продукции. Именно АСУ ТП управляет оборудованием без постоянного участия человека.

Как работает АСУ ТП:

- 1 Собирает данные с датчиков (*температура, давление, расход, уровень*).
- 2 Передает их на контроллеры (*специальные промышленные компьютеры*).
- 3 Контроллеры по заложенной программе автоматически меняют параметры (*открывают/закрывают клапаны, увеличивают/уменьшают частоту вращения насосов, включают/выключают нагрев*).
- 4 Оператор видит всю картину на экране SCADA (*системы диспетчерского управления и сбора данных*) и может вмешаться, если нужно.

Антон Елизаров

«Системы АСУ ТП работают в режиме реального времени. Технологический процесс идет постоянно, за исключением плановых окон для ремонта либо модернизации. Именно АСУ ТП является основной системой создания энергии, сырья и другой продукции, поэтому важнейшими показателями для этих систем являются отказоустойчивость и надежность».

В случае взлома АСУ ТП злоумышленник может полностью остановить процессы переработки (*например, сырья*) или выпуска продукции либо внести изменения в управляющую программу, чтобы вызвать непреднамеренный износ компонентов в долгосрочной перспективе. То есть атака может быть отложенной.

Предприятию приходится вкладывать огромные средства в восстановление систем и расследование инцидента: по оценкам BI.ZONE, эти расходы увеличивают итоговые потери в среднем в 1,2–1,8 раза по сравнению с прямыми потерями от простоя.

Нарушение технологического процесса зачастую обрывает и цепочку поставок. Так, другие заводы не смогут выпустить свою продукцию, если не получат сырье (*его запасов не всегда хватает*). То есть финансовые потери из-за простоев несут все участники этой цепочки.

Однако убытки — не самое страшное из последствий. Для объектов повышенной опасности сохранение непрерывного производства критично. Если сбой АСУ ТП произойдет, например, на химическом заводе, давление в реакторе может превысить норму, клапан не откроется и произойдет авария. Именно поэтому отказоустойчивость для АСУ ТП — вопрос не только экономии на простоях, но и промышленной безопасности.

Самый опасный враг

Промышленность сейчас находится в фокусе внимания злоумышленников — число кибератак на нее растет. Впрочем, проникновение киберпреступников именно в технологический сегмент

осложнено тем, что исторически на предприятиях его изолировали, то есть не соединяли с корпоративными системами и интернетом.

Антон Елизаров

«В технологическом сегменте большинство киберинцидентов до сих пор случаются по вине персонала. Например, вирус-шифровальщик может попасть в АСУ ТП, если сотрудник принесет на предприятие зараженную флешку и воткнет ее в рабочую станцию или, например, решит подзарядить свой телефон от USB-порта рабочей станции или сервера АСУ ТП».

Внутренними нарушителями становятся инженеры, операторы и даже руководители производств. И основной риск связан именно с неосведомленностью в части угроз ИБ. Молодые специалисты приходят на завод иногда и вовсе без базовых знаний в области информационной безопасности, потому что в вузах этот курс зачастую отсутствует.

Константин Ильютченко

«Приведу пример из собственной практики. Именно из-за недостаточной осведомленности в части информационной безопасности молодой инженер крупной компании, где я раньше работал, осужден на три года условно по ст. 274.1 УК РФ (уголовная ответственность за неправомерное воздействие на критическую информационную инфраструктуру). По незнанию он подключил составную часть значимого объекта КИИ к сети Интернет, как говорится, “из лучших побуждений”».

Эксперт напоминает, что внутренний нарушитель может навредить не только неосознанно, но и умышленно. И в этом случае он гораздо опаснее киберпреступника со стороны, потому что знает технологию производства и слабые места в АСУ ТП. Для предотвращения таких ситуаций Константин Ильютченко рекомендует не забывать о первоочередных и простых мерах ИБ, таких как регулярная смена паролей и разграничение уровня привилегий для эксплуатирующего персонала. И конечно, стоит проводить дополнительные инструктажи и регулярные аудиты.

Константин Ильютченко

«Во время категорирования, например, я всегда стараюсь провести анализ

киберрисков при воздействии на составные части критически важных объектов, то есть поэтапно моделирую компьютерную атаку извне, а также со стороны внутреннего нарушителя».

«Пропиленные» дыры и киберкинетические атаки

Воздушный зазор (*физическая изоляция*) между технологическим и корпоративным сегментами по-прежнему существует на ряде предприятий. Однако в эру работы с данными АСУ ТП все чаще подключают к корпоративным системам, таким как MES и ERP, которые анализируют информацию о технологическом процессе.

В этом случае, чтобы снизить риск целенаправленных атак на производственную линию через корпоративный сегмент, выстраиваются демилитаризованные зоны (*ДМЗ*). Это отдельный сегмент сети, который служит буфером между технологической и корпоративной сетями.

Сейчас в нашей стране любая организация, имеющая критически важный объект в эксплуатации, применяет меры безопасности, перечисленные в Приказе № 239 ФСТЭК России. Помимо защиты периметра, реализует ДМЗ. Грамотно построенная ДМЗ необходима для больших производств, ведь именно благодаря ей обеспечивается безопасная передача данных и сокрытие архитектуры технологического сегмента. В случае целенаправленной атаки на субъект КИИ это позволит замедлить продвижение злоумышленника, своевременно обнаружить его и не допустить ущерба производству. Однако в реальности это работает не всегда.

Александр Карпенко

«Граница между корпоративным и технологическим сегментами почти никогда не бывает четкой — при проведении аудита в ней можно найти десятки “пропиленных” дыр и зон ответственности. Системы на предприятиях внедряются десятилетиями — о части оборудования просто забывают, и она не попадает в вотчину ни специалистов по АСУ ТП, ни безопасников. Это одна из больших проблем. А еще есть подрядчики, которые “ходят” через корпоративку в технологический сегмент».

Эксперты напоминают, что есть и такие предприятия, где АСУ ТП и корпоративные системы в принципе «живут» в одной локальной сети.

Может возникнуть **каскадный эффект** — когда воздействие на одну систему затрагивает другую. В качестве аналогии Александр Карпенко приводит системные заболевания: сначала поражается один орган, за ним второй — и организм разваливается. По мнению эксперта, проблема в том, что на промышленных предприятиях этот эффект плохо прогнозируется и относится к категории риск-менеджмента.

Каскадный эффект порождается зачастую атаками нового типа — **киберкинетическими (или киберфизическими)**. Это когда атакуют ИТ-инфраструктуру, но воздействие переходит на реальный мир — останавливается выпуск продукции. Бывает и обратное: физическое воздействие (*например, атака дронов*) выводит из строя серверную и контроллерную инфраструктуру.

Отечественные стандарты

Сегодня многие предприятия в рамках импортозамещения переходят на отечественные решения в технологическом секторе. Этот процесс подкреплен нормативными актами: Приказ ФСТЭК № 239 обязал значимые объекты критической информационной инфраструктуры внедрять сертифицированные средства защиты информации, а Указы Президента № 166 и № 250 (*касаются мер по обеспечению технологической независимости и ИБ в ТЭК*) дали импульс разработке новых СЗИ и модернизации АСУ ТП. Как подчеркивает Константин Илютченко, в итоге системы вышли на принципиально иной уровень автоматизации и зрелости в области информационной безопасности.

Однако замена решений привычных западных брендов (*Siemens, Cisco и др.*) на российские либо поставляемые из дружественных стран аналогично сопряжена с дополнительными трудозатратами.

В частности, с необходимостью тестировать совместимость новых АСУ ТП с СЗИ и прочими компонентами инфраструктуры.

Константин Илютченко

«Раньше все было отработано, международный опыт изучен и понятен, однако сегодня ситуация кардинально изменилась: мы имеем дело с отечественным сетевым оборудованием, передовыми системами автоматизации и современными средствами защиты информации — и вынуждены проверять на практике, насколько эффективны эти решения и как они могут взаимодействовать друг с другом».

Кроме того, при импортозамещении АСУ ТП некоторые вендоры концентрируются в первую очередь на переносе технологического процесса, отодвигая вопросы безопасности на второй план. Эксперты из компании «Инфосистемы Джет» советуют внедрять уже защищенную систему на отечественном оборудовании.

Антон Елизаров

«В рамках модернизации или при строительстве новых АСУ ТП оптимальнее преднастроить, протестировать работу СЗИ и прикладного ПО на этапе заводских испытаний. Это позволяет отладить систему до того, как она будет внедрена на площадке. В итоге мы получаем готовую киберустойчивую АСУ ТП при вводе в эксплуатацию».

Ассистент, а не капитан

Развитие АСУ ТП стимулируется и искусственным интеллектом. Он берет на себя анализ гигантских массивов данных с производственных линий, выявляет скрытые закономерности и доводит технологические процессы до идеала.

Константин Илютченко

«Сейчас это распространенная практика: ИИ собирает данные, анализирует их и предоставляет оператору или инженеру конкретные рекомендации — например, скорректировать уставки или повысить мощность того или иного компрессора. Такие задачи внедряются в том числе на действующих производствах в рамках развития АСУ ТП».



Каскадный эффект — когда воздействие на одну систему затрагивает другую — на промышленных предприятиях плохо прогнозируется и относится к категории риск-менеджмента

Как правило, данные из технологического сегмента автоматически передаются на сервер в сегменте АСУ ТП, где развернута подсистема на основе ИИ. Там ИИ-ассистент проводит детальный анализ и формирует рекомендации. Решение о внесении изменений принимает технологический персонал.

Кроме того, ИИ активно применяется для видеоаналитики: контроля промышленной и пожарной безопасности, мониторинга охраны труда, выявления брака продукции на конвейере по заданным датасетам.

Антон Елизаров

«Искусственный интеллект помогает в работе с большими данными, в применении машинного зрения и оптимизации технологических процессов. Это позволяет быстрее вносить изменения в технологический процесс, снижая расходы и увеличивая производительность. Однако принятие решений остается за человеком, к управлению в промышленности ИИ пока не допускают».

Внедрение ИИ — позитивный тренд, но в то же время он порождает новые угрозы безопасности АСУ ТП, связанные с подменой обучающих выборок, искажением телеметрии, уязвимостями самих моделей и компрометацией каналов передачи данных. В ответ на это повышаются и требования к ИБ.

Изношенный фундамент

Промышленность сегодня живет в парадоксальной ситуации: все обсуждают искусственный

интеллект и озера данных (*Data Lake*), а на деле многие предприятия надстраивают новые цифровые этажи на изношенном фундаменте, заложенном еще в прошлом веке. Если корпоративный ИТ-сектор уже полностью виртуализирован, то технологический сегмент развивается гораздо медленнее: все по-прежнему замыкается на отдельных рабочих станциях и устаревших серверах, отмечают эксперты. Это напрямую сказывается на отказоустойчивости систем.

Особенно остро проблема стоит на производствах, где АСУ ТП введены в эксплуатацию десятилетия назад. В отличие от современных объектов, там зачастую используют оборудование, к которому невозможно применить никакие сертифицированные средства защиты информации. Отсутствие элементарного апгрейда оборудования сводит на нет любую программную защиту, напоминает Константин Илютченко. И единственный выход — внедрять компенсирующие меры, то есть механические средства защиты.

Кроме того, на старых предприятиях нередко отсутствует единая схема сети и нет понимания компонентного состава, так как системы внедрялись разными интеграторами в разное время. Эта «каша» создает дополнительные риски.

Антон Елизаров

«Часто при проведении аудитов мы видим, что на критических машинах жесткие диски уже отмирают, а заказчик этого не осознает. Если диск умрет, а бэкапов нет, восстановить систему будет очень сложно, а для некоторых — просто невозможно. Как итог, выход из строя компонентов АСУ ТП может привести к простоям».

Основные причины успешности атак на промышленность



всего технологического процесса. Незнание внутренней инфраструктуры АСУ ТП — боль, которая не утихает до сих пор. Мы помогаем заказчикам понять, что у них есть, и привести системы к современному виду».

Отсутствие резервного копирования — еще одна хроническая проблема промышленности. Даже если на предприятии есть специалисты, умеющие эксплуатировать АСУ ТП, то инженеров, способных восстановить ее с нуля, может и не быть. Необходимо регулярно делать бэкапы и тестировать восстановление, но это правило порой игнорируется.

Александр Карпенко

«К традиционным проблемам киберустойчивости АСУ ТП можно отнести отсутствие сегментации и мониторинга, дефолтные настройки и, отдельно, проблемы с бэкапами: нет

регламентов, бэкапов, которые помогут при полном разрушении инфраструктуры, и зачастую даже защиты самой системы резервного копирования».

Эксперт убежден: сейчас самое время вкладываться в резервирование. И начинать следует с аудита и элементарного обновления техники.

Киберустойчивость вместо стены

Концепция киберустойчивости принципиально меняет подход к безопасности: акцент смещается с вопроса «Может ли такое произойти с нами?» на вопрос «Что мы будем делать, если это случится?».

Александр Карпенко

«Будут взломаны все — и надо к этому готовиться, а не просто строить защитную стену от злоумышленников».

На случай сбоев АСУ ТП оснащены специальными противоаварийными системами, а также механизмами дублирования различных компонентов: контроллеров, рабочих станций, серверов, сетевого оборудования и пр.

Константин Ильютенко

«Если сравнивать ИТ и АСУ ТП, то на любом критичном производстве изначально проектируются и внедряются системы противоаварийной защиты, такие как пружинные предохранительные клапаны, разрывные мембраны и другие средства механической защиты. Если рассматривать их в рамках ИБ, то это, по сути, компенсирующие меры, которые в случае успешной кибератаки и, например, подмены параметров системы помогут предотвратить огромный ущерб производству».

Однако аварийная остановка не победа, ведь на деле это прямые убытки. Настоящий успех — это функционирование производства хотя бы с ограниченной мощностью. И разумеется, механической защиты здесь недостаточно.

Для построения киберустойчивых АСУ ТП эксперты рекомендуют применять комплексный подход:

- 1 **Сегментировать сеть** — разделить технологический уровень от корпоративного сегмента с помощью дополнительных средств защиты и организовать «воздушные зазоры» или ДМЗ (*физические или логические разрывы между средами*), чтобы локализовать возможную атаку и не дать ей распространиться на производственный контур.
- 2 **Переводить АСУ ТП на виртуализированные платформы** — это позволяет в случае атаки или сбоя оперативно перенести технологический процесс с основного ЦОД на резервный без длительной остановки производства, а также упрощает восстановление систем после инцидентов.
- 3 **Использовать endpoint-решения (средства защиты конечных устройств)** с широким функционалом — антивирус, контроль целостности, ограничение подключения внешних носителей,

встроенный межсетевой экран. Это своего рода «комбонабор», закрывающий основные векторы атак на уровне рабочих станций и серверов.

- 4 **Внедрять резервное копирование с регулярным тестированием восстановления** — наличие актуальных бэкапов и отработанного DR-плана критически важно для АСУ ТП и минимизирует простой при любом сбое.

Константин Ильютенко

«Если кибератака все же произойдет и приведет к шифрованию ИТ-инфраструктуры предприятия, а также к повреждению основных резервных копий АСУ ТП в промышленном сегменте, то на этот случай я всегда требую у персонала, непосредственно отвечающего за функционирование АСУ ТП, предусматривать хранение резервных копий локально, на защищенных внешних жестких дисках».

Построение киберустойчивой АСУ ТП специалисты компании «Инфосистемы Джет» рекомендуют начинать именно с диагностики: проанализировать текущее состояние инфраструктуры и ИБ технологического сегмента, проследить информационные потоки между сегментами сети и приложениями, провести аудит подрядчиков, сделать пентест для выявления уязвимостей. Не менее полезным будет стресс-тест восстановления — например, можно отключить сервер базы данных и посмотреть, как отработают технологические процессы. После этого следует организовать процессы мониторинга и реагирования (SOC) и внедрить базовые меры ИБ. В финале — проверить защищенность в формате «красной команды», устранить выявленные недостатки, разработать DRP и BCP. И продолжить развивать ИТ-инфраструктуру, внедряя сетевую сегментацию, СРК и пр.

Как отмечает Александр Карпенко, заказчики иногда возражают: «Если дрон прилетит, ваша ИБ не поможет». Но это заблуждение. Даже при физической атаке основные сценарии восстановления остаются релевантными, а наличие резервных копий и отработанных планов позволяет минимизировать последствия. ●



АВТОР

Роман
Шапиро,

руководитель дирекции
информационной
безопасности
«Почты России»



Всё

по-настоящему





КАК «ПОЧТА РОССИИ» РЕШИЛАСЬ
НА МЕСЯЦ НЕПРЕРЫВНОГО
ПРОТИВОСТОЯНИЯ УГРОЗАМ ИБ

Вместо недели пентеста — 30 дней атак 24/7 без каких-либо запретов для «красной команды». «Почта России» совместно с компанией «Инфосистемы Джет» провела киберучения федерального масштаба. Разбираем итоги: где пряталась главная уязвимость, на чем сломался SOC и почему оплату заслужили лишь 10 из 27 подсистем защиты, внедренных за год в ходе проекта по усилению киберустойчивой инфраструктуры.

Признаюсь, я не очень люблю пентест в классическом исполнении. Для меня его результат — скорее диагностика. Это снимок состояния «здесь и сейчас» — и не более того. Поможет ли он найти типовые уязвимости, проверить соответствие требованиям регулятора, оценить отдельные сегменты инфраструктуры? Да, но только в конкретный момент. Реальную устойчивость к целевой атаке классический пентест не покажет: ведь он не имитирует поведение настоящих злоумышленников.

APT-группировки месяцами изучают компанию, ее инфраструктуру, собирают досье на работников, используют социальную инженерию, чтобы спланировать проникновение и остаться незамеченными. Тогда как при тестировании в классическом понимании центр мониторинга ИБ (*Security Operation Center, SOC*) оповещается, а пентестер не скрывается, хотя и не «шумит», чтобы проверить, включится ли защита, — как правило, он фиксирует уязвимость и идет дальше. Нам же хотелось увидеть другое: как отреагирует наш SOC, когда «красная команда» прорвется внутрь, и сможем ли мы гонять атакующих по инфраструктуре?

Кроме того, по завершении первой фазы трехлетнего проекта построения киберустойчивой инфраструктуры «Почты России» нам было важно оценить эффективность внедренных подсистем безопасности, удостовериться в том, что в защите нет брешей и все собрано правильно. А при отрицательном

результате — перекроить бюджет так, чтобы деньги действительно шли на развитие ИБ. Есть ли смысл следовать выбранной стратегии, если все динамично меняется? Или покупать «бала-лайку», сертифицированную как средство защиты информации, просто потому, что так записано в плане?

Именно поэтому мы отказались от классического пентеста и решили играть по-настоящему.

Атака без ограничений

По-настоящему — это когда вместо недельного тестирования вас ждет месяц непрерывных атак 24/7. Вместо классического пентеста «по плану» — имитация действий реальной APT-группы. Когда сценарии держатся в секрете, а центр мониторинга не знает, в какой момент начнет действовать «красная команда» (*Red Team*). Причем у атакующей стороны нет ограничений — вплоть до физического проникновения в офис, кражи жестких дисков и АРМ. Разрешены любые рассылки на корпоративные устройства, звонки, манипуляции с персоналом. Что угодно, лишь бы достичь цели, — ровно так и работают настоящие преступники.

И Red Team из компании «Инфосистемы Джет» этим пользовалась. Например, проводила фишинг под видом антифишинга: после блокировки первичной фишинговой рассылки атакующие отправили поддельное письмо от имени ИТ-руководства с «памяткой по противодействию фишингу», а во вложении сидел вредоносный код. Файл открыли более 15 сотрудников.

А в какой-то момент один из «красных» просто пришел в отделение «Почты России»,

вытащил жесткий диск из ПК, предназначенного для общего пользования, и спокойно ушел с ним. И после того, как проанализировал содержимое и поставил «закладку», так же спокойно вернул на место.

Кроме того, «красная команда» выбирала для атак самые уязвимые временные окна: например, атаковала вечером в пятницу, когда все уже мысленно на даче. В то же время атаки реальных киберпреступников никто не отменял. SOC не знал, кто именно атакует, — и не мог позволить себе расслабиться. Стало очевидно: человеческая усталость — критический фактор. За ночь набиралось по несколько тысяч событий, и команда защиты не раз оказывалась на пределе.

Оплата реализованных сценариев

Я не люблю расставаться с деньгами просто так. Мне нравится платить за конкретный, измеримый результат. Обычно при проведении тестирований на проникновение подрядчик получает деньги за отчет и затраченное время. Мы предложили другую схему: базовая оплата за трудочасы + премия за каждый осуществленный сценарий. Это радикально изменило мотивацию всех участников. Red Team действовала более дерзко и решительно: она рисковала гонораром. Blue Team понимала: пропустит атаку — потеряет премию. Вендоры, чьи средства защиты были задействованы, тоже несли финансовую ответственность.

В такой модели у всех вовлеченных сторон — и «красной», и «синей команды» — были свои цели и задачи. Мы оборонялись не только силами SOC. Все вендоры, которые год строили с нами систему ИБ и внедряли свои СЗИ, встали плечом к плечу. В итоге 12 пентестеров бились против 20+ вендоров (включая SOC'и «Лаборатории Касперского» и Positive Technologies) и целого департамента ИБ.

Архитектурная дыра

Самый болезненный удар пришелся в точку, где его точно не ждали. Red Team хватило трех дней, чтобы найти и проэксплуатировать уязвимость. Причем дыра оказалась не в ИБ-системе, а в самой логике ИТ-архитектуры.



50+

отработанных техник атак реальных злоумышленников



4000+

событий, из них около 1400 были квалифицированы как действия «красной команды», а порядка 100 инцидентов признаны критическими



37

сценариев недопустимых событий



10 из 37

сценариев реализованы, а кроме того, в ходе учений обнаружены 4 новых



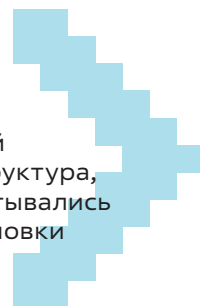
12

пентестеров против **20+ вендоров** и штатного SOC



38 тысяч

отделений по всей России — инфраструктура, на которой отрабатывались сценарии без остановки бизнес-процессов



В ХОДЕ КИБЕРУЧЕНИЙ ПРОВЕРИЛИ НЕ ОТДЕЛЬНЫЕ УЗЛЫ, А ВСЮ СВЯЗКУ «ЛЮДИ — ПРОЦЕССЫ — ТЕХНОЛОГИИ» В УСЛОВИЯХ РЕАЛЬНОГО ДАВЛЕНИЯ

Не вдаваясь в подробности, суть проблемы можно изложить так: совмещение внешней и внутренней инфраструктуры в рамках одного ИТ-решения может привести к катастрофе. Как безопасник, я был горд: брешь нашли не в защите. Но как руководитель — пришел в ужас, прикинув, сколько сил и денег уйдет на перестройку инфраструктуры.

Еще одним неприятным результатом стало то, что из 27 систем защиты, внедренных в рамках проекта за год, оплату по итогам учений зачислили только 10. Остальные либо не справились с атакой, либо не обновились до начала тестирования, либо не зафиксировали действий атакующих. Претендовать на получение оплаты они смогут только по итогам следующей верификации, если она будет успешной.

Измеримые итоги киберучений

Работать вживую было и сложно, и страшно — ведь наша компания обслуживает каждого гражданина России. Соответственно, нарушение ее работы может привести к коллапсу в масштабах всей страны. Тем не менее проверка принесла пользу не только нам, но и всему рынку. Вендоры, чьи продукты дали сбой, доводили их до ума прямо по ходу учений. В результате они доработали свои СЗИ. Это поможет и другим компаниям.

Мы не просто оценили скорость работы SOC и нашли слепые зоны: мы выполнили комплексную проверку сети, веба, Wi-Fi, конвейера безопасной разработки, технологических сегментов, а также протестировали физическую безопасность

и устойчивость сотрудников к социальной инженерии. Причем проверили не отдельные узлы, а всю связку «люди — процессы — технологии» в условиях реального давления.

По результатам киберучений «Почта России»:

- пересмотрела общий список недопустимых событий и добавила в него 4 новых сценария, выявленных «красной командой»;
- актуализировала правила мониторинга в SIEM/SOC;
- обновила политики реагирования и процедуры блокировки;
- скорректировала инвестиционные планы: проекты по развитию ИБ были пересмотрены с учетом реальных, а не гипотетических векторов.

Основной урок учений: нельзя бездумно докупать средства защиты и надеяться на чудо. Главный итог — не список уязвимостей и не экономия на неэффективных СЗИ, а рабочий механизм пересмотра стратегии ИБ на основе реальных данных. Это суперэффективный способ планировать финансирование на ближайшее будущее. Вам не придется выбивать бюджет: достаточно показать, что через конкретную дыру компанию взломали трижды.

В ходе проекта мы сформировали комплекс по-настоящему работающих подсистем обеспечения ИБ и готовы к их дальнейшему тиражированию на всю инфраструктуру «Почты России».

Что делать завтра: 5 советов



Проводите харденинг

Харденинг работает лучше, чем многие средства защиты информации. Никакой сертификат не заменит базовой гигиены: закрытых портов, отключенных лишних служб и минимальных привилегий.

Наладьте взаимодействие ИБ с ИТ и разработкой

Если подразделения не умеют работать слаженно, нормального MTTR (среднего времени на восстановление системы после сбоя) не добиться. А разработчикам пора воспринимать требования ИБ не как помеху, а как часть процесса.



Не будьте обособленной кучкой могучих богатырей

За периметром должны следить не только безопасники, но и ИТ, и DevOps. Любой сотрудник — ваш союзник. Коллега, вовремя сообщивший о подозрительном звонке, может помочь расследовать серьезный инцидент. Вовлекайте персонал в программу информирования и фиксации инцидентов.

Учитывайте усталость команды

Тысячи алертов за ночь, атаки в пятницу вечером, ложные срабатывания — люди выгорают быстрее, чем ломается защита. Закладывайте сменный график и автоматизируйте фильтрацию событий.



Ищите теньевые ИТ сами

Иначе это сделают за вас. Нелегитимные сервисы, используемые сотрудниками, забытые тестовые контуры, «удобные» обходные пути — все эти уязвимости должны выявляться в порядке регулярной практики, а не становиться сюрпризом в разгар атаки. ☹



АВТОР

Роман
Лебедь,

руководитель центра
защиты приложений
в «Т-Банке»

ИСКУССТВЕННЫЙ ИНТЕЛЛЕКТ АТАКУЕТ!

КАК «Т-БАНК» ПОСТАВИЛ НА НЕПРЕРЫВНЫЙ ПОТОК
ПРОВЕРКУ СВОЕЙ КИБЕРУСТОЙЧИВОСТИ



Мир информационной безопасности изменился под воздействием искусственного интеллекта. Пример последних месяцев — выпуск сильной модели Claude Mythos, способной в составе агента выявлять и эксплуатировать уязвимости значительно быстрее человека. А значит, сегодняшние киберугрозы в сравнении с угрозами 5-летней давности — совершенно новая история, требующая адаптации защиты. Так почему бы не превратить ИИ в белого хакера, который будет гораздо эффективнее багхантеров, пентестеров и статических анализаторов кода, вместе взятых?

Если говорить об инструментах защиты, используемых в «Т-Банке», то одним из основных является классический пентест, выполняемый несколько раз в год и охватывающий определенный набор систем. И раньше выходило так, что существенные изменения инфраструктуры случались чаще проверок ее безопасности.

Кроме того, тренд на технические уязвимости в нашей инфраструктуре падает, а на ошибки логического характера — растет. Например, такие как неправомерное получение скидки, обход ограничений на перевод средств, получение доступа к данным другого клиента.

Проблема в том, что такие ошибки не выявляются традиционными автоматизированными

средствами. Поэтому, чтобы оставаться на фронтире разработки, сокращать окно между появлением уязвимости и ее обнаружением, учитывать бизнес-контекст для поиска уязвимостей логического характера, мы начали разработку атакующего ИИ.

Так появилась наша Nulla — группа интеллектуальных агентов, которые автономно анализируют устойчивость инфраструктуры на всех этапах: от разработки до использования человеком. Для нас это дополнительный инструмент защиты, помогающий справляться с современными вызовами и проверять самих себя после каждого значимого изменения. Уже в этом году мы первыми среди российских компаний проверили собственную устойчивость к внешним враждебным кибератакам с помощью искусственного интеллекта — протестировали около 1300 сервисов и платформ, входящих в экосистему. В их числе: «Т-Бизнес», «Т-Путешествия», «Т-Авто» и другие.

Nulla — быстрая и умная. Она не работает по заранее заданным шаблонам, а анализирует выявленные недостатки в совокупности и комбинирует их. То есть система, как профессиональный хакер, способна воспроизводить сложные, многоэтапные сценарии и выявлять уязвимости в условиях, имитирующих реальные атаки. И все это за 45 минут в сравнении с «человеческими» 2–3 днями.

Преодолимые трудности и сочетание компетенций

Разработка Nulla началась в прошлом году, но мы уже довольны результатом. Конечно, не обошлось без трудностей:



Баланс между глубиной проверки и безопасностью процесса

Самым сложным было внедрить Nulla в промышленную среду. Одно дело — показать хорошие результаты в лаборатории, и совсем другое — ежедневно проверять тысячи сервисов крупной компании. Действия атакующего ИИ должны максимально соответствовать поведению реального злоумышленника, но при этом не влиять на стабильность сервисов и не создавать рисков для клиентов. Поэтому нам пришлось выстроить отдельные механизмы контроля, ограничений и безопасного выполнения сценариев.

300 МЛН РУБ. — ТАКОЙ ЭКОНОМИЧЕСКИЙ ЭФФЕКТ ИСПОЛЬЗОВАНИЯ NULLA ДЛЯ ПРЕДОТВРАЩЕНИЯ ИНЦИДЕНТОВ ДО КОНЦА ЭТОГО ГОДА ПРОГНОЗИРУЮТ В «Т-БАНКЕ»



Интеграция с существующими процессами управления уязвимостями

Работа традиционных сканеров полностью детерминирована: после исправления достаточно повторно выполнить ту же проверку. ИИ-агенты устроены иначе: они каждый раз самостоятельно выбирают стратегию исследования и могут прийти к одному и тому же результату разными путями. Поэтому для подтверждения устранения уязвимостей нам пришлось построить отдельный процесс верификации, который обеспечивает воспроизводимость результатов и органично встраивается в существующие процессы AppSec (безопасности приложений).

Если говорить о секрете успеха, то прежде всего это команда. Такие системы невозможно создать усилиями только ИИ-инженеров или специалистов по информационной безопасности. У нас бок о бок работают эксперты по кибербезопасности, ИИ-инженеры, разработчики и специалисты по данным. Исследователи изучают новые техники атак, способы эксплуатации и нестандартные сценарии.

Именно сочетание этих компетенций позволяет быстро проверять гипотезы, создавать надежные решения и сокращать время от появления новой идеи до ее внедрения в продукт.

Экономический эффект от атакующих ИИ-агентов

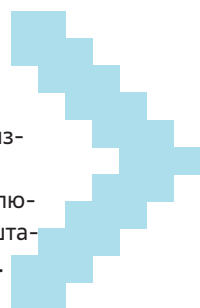
Прогнозируемый экономический эффект использования Nulla для предотвращения инцидентов

до конца этого года мы оцениваем в 300 млн руб. Это объем потенциальных выплат по программе багбаунти в случае обнаружения этих уязвимостей внешними белыми хакерами. Однако отмечу, что сумма относительная, так как точно просчитать возможную атаку и убыток от нее — невозможно.

Кроме того, с Nulla мы можем управлять покрытием, частотой и глубиной сканирования и тем самым определять бюджет на проверку. Финансово такой подход кратно выгоднее в сравнении с ручной работой.

Помимо экономической эффективности, Nulla выигрывает в продуктивности: за квартал она находит больше подтвержденных уязвимостей, чем багхантеры, пентестеры и статические анализаторы, вместе взятые. Она ставит анализ безопасности на непрерывный поток, проверяя изменения в инфраструктуре и приложениях по мере их появления. В рамках масштабной экосистемы с сотнями сервисов и высоким уровнем ответственности перед клиентами это просто необходимо.

Ключевым эффектом для нас стало то, что теперь мы можем предоставлять одинаковый уровень сервиса по всем бизнес-линиям и продуктам, не занимаясь приоритизацией и не привлекая новых людей, как это было раньше, когда мы масштабировали знания за счет роста команды.



Да, Nulla обходится дешевле, чем содержание команды топ-пентестеров, которые к тому же физически не смогли бы выполнить тот же объем работы за то же время. Но даже с ней мы не отказываемся от ручного пентеста. У нас гибридная модель проверки собственной устойчивости: действует программа багбаунти, а еще в июне мы запустили открытые кибериспытания, в рамках которых любой багхантер сможет протестировать стабильность инфраструктуры «Т-Банка».

Зачем? Отвечать на атаки ИИ исключительно стандартными инструментами теперь небезопасно, но отрицать экспертизу команды, внешнюю экспертизу и мировой опыт мы не хотим. Кроме того, результаты пентестов, ручных аудитов, кибериспытаний и багбаунти используются для совершенствования качества работы Nulla.

Что важно учитывать: опора на доказательства, а не впечатления

Сможет ли компания обнаружить уязвимость, прежде чем она станет причиной простоя или компрометации? Именно этот вопрос все чаще становится ключевым для бизнеса. Мы ожидаем, что в ближайшее время скорость выявления и отработки уязвимости будет исчисляться часами, а значит, ручного пентеста раз в квартал и багбаунти будет недостаточно. Ответить на современные вызовы смогут те, кто вовремя автоматизирует поиск уязвимостей и поставит этот процесс на поток.

На что я обратил бы внимание специалистов, нацеленных внедрить атакующего ИИ-агента:



Ограничение функционала. Не пытайтесь сразу построить универсальный ИИ-пентестер. Намного эффективнее начать с 1–3

понятных задач, решение которых сразу принесет практическую пользу команде безопасности. По мере накопления данных, опыта и доверия к системе можно будет расширять ее возможности и сценарии применения.



Контекст. Чтобы ИИ действительно понимал инфраструктуру, необходимо объединить информацию об активах, владельцах сервисов, контейнерных образах, артефактах сборки, сетевой архитектуре, API, зависимостях между системами и публикациях во внешние контуры. Только имея такую целостную картину, агент способен строить реалистичные сценарии атак и оценивать их влияние.



Объективная оценка качества ИИ-агента. Ориентируйтесь на бенчмарки и измеряйте качество, используя объективные метрики: количество подтвержденных находок, уровень ложных срабатываний, успешность выполнения сценариев и стабильность результатов. Развитие ИИ не должно опираться на впечатления.



Подтверждаемые результаты. Если система генерирует большое количество неподтвержденных находок, команды быстро перестают ей доверять. Поэтому мы стараемся автоматически подтверждать возможность ее эксплуатации и предоставлять воспроизводимые доказательства. Это значительно снижает уровень шума и ускоряет устранение действительно значимых рисков.

Самый важный вывод касается роли людей. Не рассматривайте ИИ как замену специалистов по информационной безопасности. Сегодня мы сосредоточены на исследовании новых классов уязвимостей, способов эксплуатации и сложных атакующих сценариев. После проверки эта экспертиза переносится в Nulla и автоматически применяется при анализе всей инфраструктуры компании.

Таким образом, нашим главным активом остаются профессиональные знания. Благодаря ИИ-модели они постепенно становятся частью системы и начинают работать на тысячи сервисов, повышая общий уровень защищенности всей организации. 🌐

ВРЕМЯ ПЕРЕСМОТРЕТЬ ИТ-ЛАНДШАФТ

дата: __/__/__

Проверьте, нет ли у ваших ИС знакомых симптомов:

	да	нет
Платите за системы с дублирующей функциональностью	☐	☐
Критичные ИС зависят от одного специалиста	☐	☐
Не знаете реальную стоимость владения ИС	☐	☐
Не проверяли, укладывается ли восстановление в заявленный RTO	☐	☐



Нашли хотя бы один?

Пора на чек-ап информационных систем.
Покажем, что оставить, что модернизировать,
что заменить и от чего отказаться.

Результат — карта состояния ИС
и дорожная карта изменений.

infrastructure@jet.su

+7 495 411-76-01

КАК БЫСТРЕЕ ВЫЙТИ ИЗ ЛАБИРИНТА

ВЕРНЫЕ ШАГИ И ТИПИЧНЫЕ
ОШИБКИ В ПЕРВЫЕ 48 ЧАСОВ
ПОСЛЕ КИБЕРАТАКИ



ЭКСПЕРТ

**Ринат
Сагиров,**

директор центра
мониторинга
и реагирования компании
«Инфосистемы Джет»



ЭКСПЕРТ

**Александр
Сулима,**

руководитель
направления Wintel
компании
«Инфосистемы Джет»



Две недели — столько в среднем требуется компаниям, чтобы вернуть ИТ-системы в рабочее состояние после крупной кибератаки. После инцидента бизнес оказывается в лабиринте восстановления: еще неясно, какие системы скомпрометированы, каким данным можно доверять и с чего начинать возвращение к работе. Насколько долгим окажется путь к выходу, во многом зависит от действий команды в первые 24–48 часов. Именно в это время принимаются решения, которые могут сократить простой или, наоборот, растянуть его на недели и даже месяцы. В материале разбираемся, как выстроить восстановление в первые часы после атаки — от локализации и расследования до безопасного запуска систем. А также — какие ошибки чаще всего усложняют этот процесс и увеличивают сроки возвращения бизнеса к работе.

Две недели — ориентир для возвращения в работу критичных систем, а не для полного завершения восстановления. Расследование инцидента, поиск причины компрометации, проверка инфраструктуры и устранение последствий могут занимать месяцы. Во многом это связано с характером современных атак. По данным отчета Jet CSIRT (*центра кибербезопасности компании «Инфосистемы Джет»*) «Популярные тактики и техники нарушения киберустойчивости российских компаний», в 76% крупных инцидентов злоумышленники прибегали к шифрованию или разрушению инфраструктуры. В таких случаях недостаточно просто запустить сервисы — необходимо заново выстроить безопасную среду, устранить оставленные атакующими механизмы доступа и убедиться, что инфраструктуре снова можно доверять.

Первые 24–48 часов: как начинается восстановление

Первые часы после атаки задают траекторию всего восстановления. Команде приходится одновременно останавливать распространение инцидента, сохранять цифровые следы, оценивать масштаб компрометации и определять, какие системы можно возвращать в работу. Ошибка на любом из этих этапов может стоить нескольких дополнительных дней или недель простоя. Разберем их по порядку.

Локализация атаки

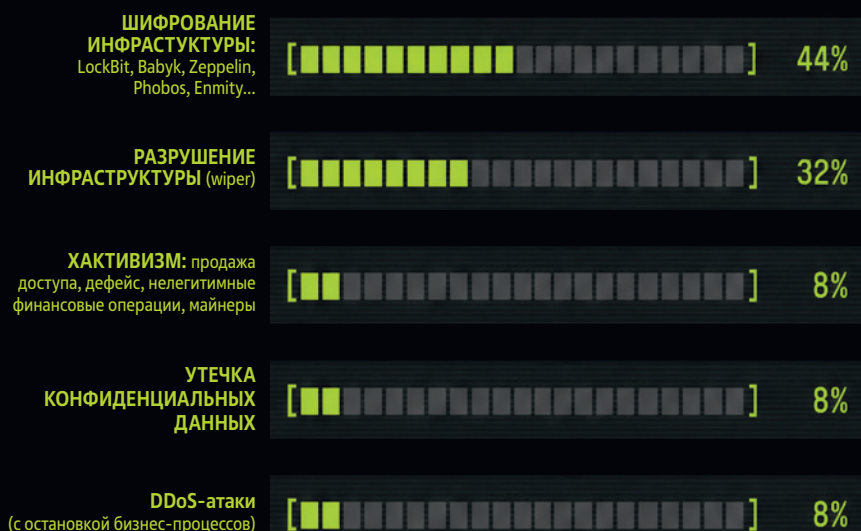
Первый шаг — остановить распространение кибератаки. Для этого нужно понять, насколько глубоко злоумышленники успели проникнуть в инфраструктуру, какие системы уже скомпрометированы и сохраняется ли риск дальнейшего развития атаки. На практике локализация включает сразу несколько параллельных действий:

- проверку и изоляцию резервных копий;
- ограничение внешних подключений;
- смену привилегированных учетных записей;
- перевод удаленного доступа на защищенные каналы;
- актуализацию сведений о критически важных системах.

✗ Ошибка: выключать или перезагружать зараженные системы

В оперативной памяти, журналах событий и активных процессах могут содержаться артефакты, необходимые для восстановления картины атаки и оценки масштаба компрометации. При выключении или перезагрузке часть этих данных можно безвозвратно потерять, поэтому

АКТУАЛЬНЫЙ ЛАНДШАФТ КИБЕРУГРОЗ



[ВАЖНО]

76%

АТАК СЕГОДНЯ —
шифрование и разрушение
инфраструктуры

ТАЙМЛАЙН ВОССТАНОВЛЕНИЯ ПОСЛЕ ЧС

01. ВОССТАНОВЛЕНИЕ КЛЮЧЕВОЙ
ИНФРАСТРУКТУРЫ

X часов

- > Ключевая инфраструктура восстановлена
- > Старт восстановления критичных ИС

02. ВОССТАНОВЛЕНИЕ ДАННЫХ
КРИТИЧНЫХ ИС

Y часов

- > Восстановлены данные критичных систем
- > X ТБ — данные из текущей СРК (при использовании СХД РК All-flash)
- > Передача данных осуществляется по сети SAN. Каналы передачи не являются узким местом
- > Выполняется восстановление критичных ИС из последней доверенной резервной копии
- > Запуск критичных ИС

03. ПРОВЕРКА КРИТИЧНЫХ ИС



Z часов

- > Восстановлена работа ключевых систем
- > Проверка восстановления данных администратором ИС
- > Предоставление доступа пользователям к ИС



Время целевого восстановления критичных систем для последней незашифрованной РК критичных ИС
(RTO): X + Y + Z часов

Предельная потеря данных в случае восстановления на последнюю доверенную РК: **(RPO) — R часов**



[ВАЖНО]

Целевые параметры RTO/RPO достигаются только при наличии DR-планов, восстанавливаемых ИС и обученной команды, которая выполняет периодические восстановления данных ИС



такие действия допустимы только в случае крайней необходимости.

Сначала понять — потом восстанавливать

Прежде чем запускать процесс восстановления, необходимо получить ответы на несколько ключевых вопросов. Каким образом злоумышленники получили первоначальный доступ? Какие системы были скомпрометированы? Как происходило распространение вредоносного кода внутри инфраструктуры? Сохранились ли механизмы удаленного доступа? Произошла ли утечка данных?

✗ Ошибка: начинать восстановление до того, как понятен сценарий атаки

Вместе с резервными копиями в инфраструктуру могут вернуться и злоумышленники. В результате восстановленные системы рискуют оказаться повторно зараженными.

Ринат Сагиров

«Расследование может продолжаться и после запуска критичных сервисов, однако еще до начала восстановления команде особенно важно понять, как распространяется вредоносное ПО и какие методы злоумышленники использовали для закрепления в инфраструктуре. Пока эти вопросы остаются без ответа, восстанавливаемая система подвержена высокому риску повторного заражения».

Платить или не платить

Один из самых сложных вопросов, который может возникнуть в первые часы после кибератаки: соглашаться ли на требования злоумышленников? При этом выплата выкупа сама по себе не гарантирует возвращения данных и тем более не означает завершения восстановления.

Ключевые риски, которые необходимо учитывать:

- нет гарантий, что после получения выкупа злоумышленники предоставят инструмент для расшифровки;

- полученный инструмент может работать некорректно или восстановить данные лишь частично;
- даже после расшифровки инфраструктура остается скомпрометированной;
- выплата выкупа стимулирует злоумышленников к проведению новых атак.

✗ Ошибка: сосредоточиться на поиске виновных вместо определения сценария атаки

Однозначно установить, кто именно стоял за инцидентом, удастся далеко не всегда. Для восстановления гораздо важнее понять, как развивалась атака: каким был первоначальный доступ, как злоумышленники перемещались внутри сети, повышали привилегии, закреплялись в инфраструктуре и переходили к шифрованию или уничтожению систем. Такая картина позволяет закрыть использованные пути доступа и снизить риск повторной компрометации.

Популярные техники атак

Список наиболее распространенных техник атак команда Jet CSIRT сформировала на основе анализа реальных инцидентов в российских организациях. Для их описания эксперты использовали MITRE ATT&CK (*Adversarial Tactics, Techniques, and Common Knowledge*) — открытую базу знаний о том, как злоумышленники действуют на разных этапах атаки.

Скорость восстановления зависит не только от действий специалистов после обнаружения атаки и определения ее сценария. Не менее важно, насколько готова к инциденту компания: назначены ли ответственные, понятен ли порядок принятия решений и существует ли проверенный план восстановления.

Именно эта организационная основа превращает реагирование из набора несогласованных действий в управляемый процесс. Ключевые элементы — кризисный штаб, заранее распределенные роли и актуальный DRP.

Кто управляет восстановлением

Восстановление невозможно вести силами одной ИТ-команды. Параллельно с техническими

ТАКТИКИ И ТЕХНИКИ КИБЕРАТАКИ



Получение
доступа в
инфраструктуру

T1190 Эксплуатация уязвимостей публично доступного сервиса

T1133 Внешние службы удаленного доступа

T1078 Существующие учетные данные

T1566 Фишинг

T1199 Доверительные отношения



Выполнение
команд и кода

T1059 Интерпретаторы командной строки и сценариев

T1072 Средства развертывания ПО



Закрепление

T1543 Создание или изменение службы

T1098 Манипуляции с учетными записями

T1112 Изменения в реестре

T1053 Создание, изменение задач

T1505 Компонент серверного ПО (веб-шелл)

T1197 Задания BITS



Повышение
привилегий

T1134 Манипулирование токенами доступа

T1068 Эксплуатация уязвимостей для повышения привилегий

T1078 Существующие учетные данные



Доступ
к учетным
данным

T1003 Дамп учетных данных

T1110 Подбор учетных данных

T1555 Использование данных из хранилищ паролей

T1558 Кража тикетов Kerberos

T1552 Небезопасное хранение паролей

T1219 ПО для удаленного доступа

T1572 Туннелирование протокола

T1090 Прокси



Деструктивные
воздействия

T1486 Шифрование данных

T1485 Уничтожение данных

Холодный → горячий (эскалация угрозы)





КОМАНДА РАССЛЕДОВАНИЯ ИНЦИДЕНТА, КОТОРАЯ ОТВЕЧАЕТ ЗА:

- ☑ Организацию процессов сбора цифровых артефактов, необходимых для определения границ инцидента и вектора атаки
- ☑ Определение используемых техник атак, инструментов и индикаторов компрометации
- ☑ Координацию локализации инцидента
- ☑ Формирование рекомендаций по восстановлению ИТ-инфраструктуры



КОМАНДА ИЗ ИБ-ПОДРАЗДЕЛЕНИЯ, КОТОРАЯ ОТВЕЧАЕТ ЗА:

- ☑ Сбор необходимых цифровых артефактов
- ☑ Внесение индикаторов компрометации в СЗИ и средства мониторинга
- ☑ Использование индикаторов компрометации для поиска скомпрометированных узлов инфраструктуры
- ☑ Разработку и реализацию плана восстановления с учетом требований ИБ
- ☑ Восстановление подсистем обеспечения ИБ
- ☑ Разработку мер по усилению защиты инфраструктуры после инцидента



КОМАНДА ИЗ ИТ-ПОДРАЗДЕЛЕНИЯ, КОТОРАЯ ОТВЕЧАЕТ ЗА:

- ☑ Актуализацию данных о текущем состоянии инфраструктуры
- ☑ Сбор необходимых цифровых артефактов
- ☑ Определение приоритетов запуска систем
- ☑ Подготовку детального технического плана восстановления
- ☑ Восстановление ИТ-инфраструктуры с учетом требований ИБ

работами необходимо решать, какие сервисы временно отключить, какие — восстановить в первую очередь, как выстраивать коммуникацию с клиентами и партнерами и как минимизировать юридические риски.

Поэтому управлять восстановлением должна не только ИТ-служба, но и единый кризисный штаб. Как правило, в него входят руководители ИТ-и ИБ-подразделений, представители бизнеса, юридической службы и отдела внешних коммуникаций.

Александр Сулима

«В первые 48 часов важно определить и утвердить сценарий восстановления: оценить масштаб работ, установить их последовательность и оперативно привлечь необходимых специалистов. У нас были кейсы, когда топ-

менеджеры со стороны заказчика с первых минут взлома находились на площадке вместе со своей ИТ-командой и нашими инженерами, участвовали в выборе тактики восстановления и расстановке приоритетов. Благодаря этому запустить часть критичных бизнес-процессов в чистых контурах удавалось уже в первые три дня. Главный совет — иметь под рукой контакты компаний, которые смогут установить причины инцидента, предложить оптимальный сценарий и провести восстановление в сроки, необходимые бизнесу».

При этом кризисный штаб не выполняет технические задачи самостоятельно. Для реагирования формируются отдельные команды, каждая из которых отвечает за свою часть процесса.

✗ **Ошибка:** действовать разрозненно

Если подразделения принимают решения независимо друг от друга, их действия могут помешать расследованию. Например, одна команда может перезапустить систему, пока другая еще собирает цифровые следы для расследования. В результате важные данные теряются, картина атаки становится менее ясной, а сроки восстановления увеличиваются.

Ринат Сагиров

«Роли и полномочия участников восстановления важно заранее закрепить в DRP — плане аварийного восстановления ИТ-инфраструктуры. В нем должно быть четко прописано, какие системы являются критичными, в какой последовательности их запускать, какой простой и какой объем потери данных допустимы, кто отвечает за каждый этап и какие ресурсы потребуются. Но сам по себе документ еще не означает, что компания готова к инциденту. DRP должен регулярно обновляться и проходить практические проверки».

Инфраструктура, которой снова можно доверять

После кибератаки просто вернуть системы в работу недостаточно. Инфраструктуру необходимо восстановить так, чтобы закрыть использованные злоумышленниками уязвимости и каналы доступа и снизить риск повторной компрометации.

Для этого необходимо:

- проверить все хосты средствами защиты с актуальными индикаторами компрометации;
- переустановить операционные системы на подозрительных хостах;
- полностью сменить доменные и локальные пароли, включая сервисные и технологические учетные записи;
- ограничить удаленный доступ и разрешать его только с двухфакторной аутентификацией;
- сегментировать сеть;

- обновить программное обеспечение до актуальных версий;
- отключить устаревшие протоколы;
- обновить и дополнить индикаторы компрометации в системах мониторинга.

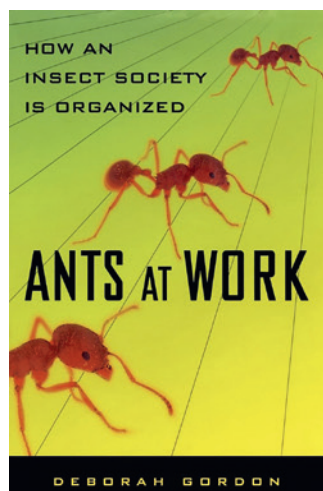
Такие меры позволяют вернуть инфраструктуре не только работоспособность, но и доверие. Полноценное восстановление после кибератаки завершается тогда, когда компания поняла, как произошла компрометация, устранила ее причины и закрыла использованные злоумышленниками пути доступа. В этих шагах и заключается главная задача восстановления в первые 48 часов после киберинцидента.

Александр Сулима

«В нашей практике был случай, когда топ-менеджер со стороны заказчика решил не тратить время на выяснение причин взлома и точки проникновения, а также пренебрег сменой паролей на оборудовании. Вместо этого приложение сразу опубликовали во внешнем контуре. Злоумышленники заметили его и уже в первые 30 минут повторно проникли в инфраструктуру и зашифровали данные. После этого компания вернулась к правильному сценарию восстановления — с соблюдением всех требований информационной безопасности».

Первые 48 часов даже при слаженной работе могут не дать команде исчерпывающую картину атаки — на полноценное расследование потребуются недели или месяцы. Но именно в этот период во многом определяется общая продолжительность восстановления. За это время необходимо прежде всего остановить распространение инцидента, сохранить данные для расследования и выстроить единый порядок принятия решений.

Правильная последовательность действий помогает избежать повторного заражения, потери цифровых следов и необходимости заново выполнять уже проделанную работу, а значит, сокращает простой и ускоряет возвращение систем в рабочий контур. Если же в первые часы допущены ошибки, каждый следующий шаг принимается на основе неполной информации и в итоге может еще сильнее затянуть восстановление. ●



ДЕБОРА ГОРДОН

«МУРАВЬИ ЗА РАБОТОЙ: КАК ОБЩЕСТВО ВЫЖИВАЕТ БЕЗ НАЧАЛЬНИКА», 1999

Муравьи существуют на Земле более ста миллионов лет и за это время распространились практически на всех континентах. Их колонии обходятся без единого центра управления, но при этом способны эффективно распределять ресурсы, реагировать на угрозы и восстанавливаться после потерь. Автор показывает, как сложное поведение возникает из множества простых взаимодействий между отдельными участниками системы. Это исследование коллективного интеллекта и самоорганизации.



ДЖОН М. БАРРИ

«ИСПАНКА. ИСТОРИЯ САМОЙ СМЕРТОНОСНОЙ ПАНДЕМИИ», 2004

Пандемия испанского гриппа стала одним из крупнейших кризисов XX века. Джон Барри рассказывает о распространении вируса и о том, как государственные институты (правительство, армия, здравоохранение, пресса) ломаются под давлением неизвестной угрозы. Автор показывает: скорость распространения болезни определяется не биологией, а решениями о закрытии городов, цензуре и «сохранении лица». Любые планы отлично работают, когда понятна причина сбоя. А что, если угроза неизвестна?



РИЧАРД ДОКИНЗ

«ЭГОИСТИЧНЫЙ ГЕН», 1976

Что именно сохраняется в живой природе на протяжении миллионов лет? Ричард Докинз предлагает смотреть на эволюцию как на историю непрерывного воспроизводства информации, закодированной в генах. Организмы рождаются и исчезают, а генетические стратегии продолжают существовать, передаваясь через поколения. Книга стала одной из самых влиятельных работ по эволюционной биологии и помогает увидеть непрерывность как способность системы сохранять ключевую информацию даже в условиях постоянных изменений.

6 КНИГ О ТОМ, КАК ВЫЖИВАЮТ СЛОЖНЫЕ СИСТЕМЫ





ПЕТЕР ВОЛЬЛЕБЕН

«ТАЙНАЯ ЖИЗНЬ ДЕРЕВЬЕВ. ЧТО ОНИ ЧУВСТВУЮТ, КАК ОНИ ОБЩАЮТСЯ — ОТКРЫТИЕ СОКРОВЕННОГО МИРА», 2015

Лес в книге немецкого лесничего Петера Вольлебена — не набор отдельных растений, а сложная взаимосвязанная экосистема. Деревья обмениваются питательными веществами, предупреждают друг друга об угрозах и поддерживают ослабленных соседей через подземные грибные сети. Непрерывность жизни здесь возникает благодаря кооперации и долгосрочным связям, которые позволяют экосистеме сохранять устойчивость на протяжении столетий. Автор также объясняет, почему дрожит осина, как вода преодолевает силу гравитации, чтобы подняться к верхушкам деревьев, и показывает, насколько деревья уязвимы — даже небольшая царапина на коре может стать смертельной.



ДЖАРЕД ДАЙМОНД

«КОЛЛАПС. ПОЧЕМУ ОДНИ ОБЩЕСТВА ПРИХОДЯТ К ПРОЦВЕТАНИЮ, А ДРУГИЕ — К ГИБЕЛИ», 2005

Историк и географ Джаред Даймонд исследует судьбы обществ, столкнувшихся с экологическими, экономическими и социальными кризисами. Каждый случай рассматривается сразу через несколько факторов, что позволяет увидеть, насколько сложными бывают причины упадка. На примере обитателей острова Пасхи, викингов Гренландии и других культур автор показывает, как способность адаптироваться к изменениям влияет на будущее целых цивилизаций. Книга рассматривает устойчивость как совокупность решений, принимаемых на протяжении многих лет.



ДЭВИД БЕЙКЕР

«КРАТЧАЙШАЯ ИСТОРИЯ ВСЕЛЕННОЙ. ОТ БОЛЬШОГО ВЗРЫВА ДО НАШИХ ДНЕЙ», 2022

История Вселенной в книге предстает как непрерывная цепь преобразований, растянувшаяся почти на 14 миллиардов лет. Из элементарных частиц возникают атомы, из атомов — звезды и планеты, а затем — жизнь, человеческие общества и технологии. Каждое новое состояние мира становится продолжением предыдущего, сохраняя накопленную информацию и создавая основу для дальнейшего развития. Непрерывность здесь проявляется как способность сложных систем меняться, не теряя связи со своим прошлым. 🌌

ТОР* «ЭПИК» — единая платформа для инженерных изысканий

*ТОР — типовое отраслевое решение

«ЭПИК» объединяет данные, процессы и программные инструменты инженерных изысканий в единой информационной среде.

Единая платформа инженерных изысканий:

- объединяет данные разных этапов изысканий;
- интегрирует существующие отраслевые и корпоративные системы через API;
- сохраняет накопленные наработки и собственные инструменты компании;
- автоматизирует процессы поэтапно.

Модульная архитектура «ЭПИК» адаптируется под ИТ-ландшафт и процессы конкретного предприятия, позволяя постепенно перейти от набора разрозненных инструментов к сквозному цифровому процессу.



**Инфосистемы
Джет**

Подробнее о платформе «ЭПИК» —
на сайте «Инфосистемы Джет».



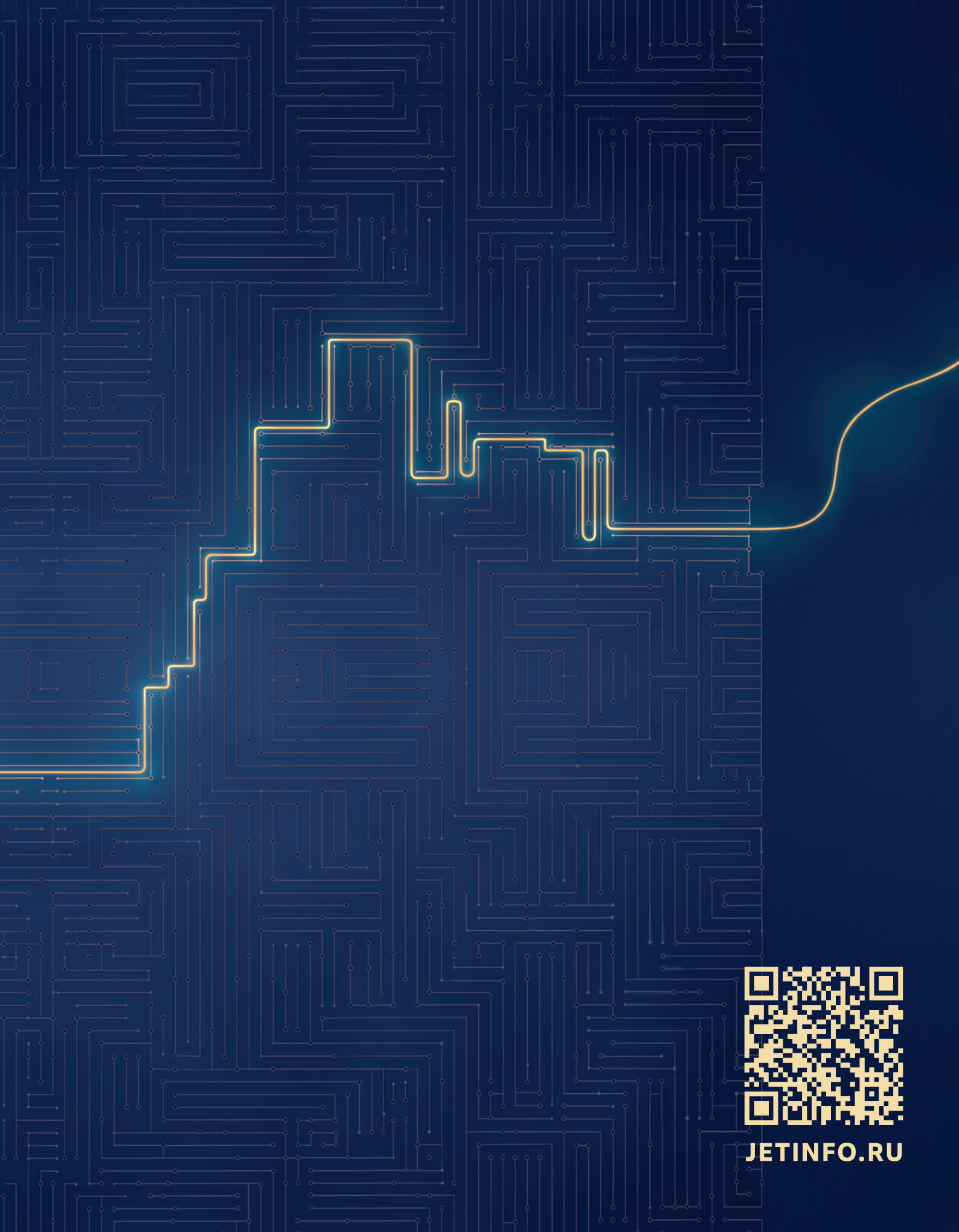
тел: +7 495 411-76-01



e-mail: marketingpo@jet.su







JETINFO.RU