JET SECURITY TEAM

ИССЛЕДОВАНИЕ

ВОССТАНОВЛЕНИЕ КАК СТРАТЕГИЧЕСКИЙ АСПЕКТ КИБЕРУСТОЙЧИВОСТИ БИЗНЕСА

Инфосистемы Джет
JET.SU

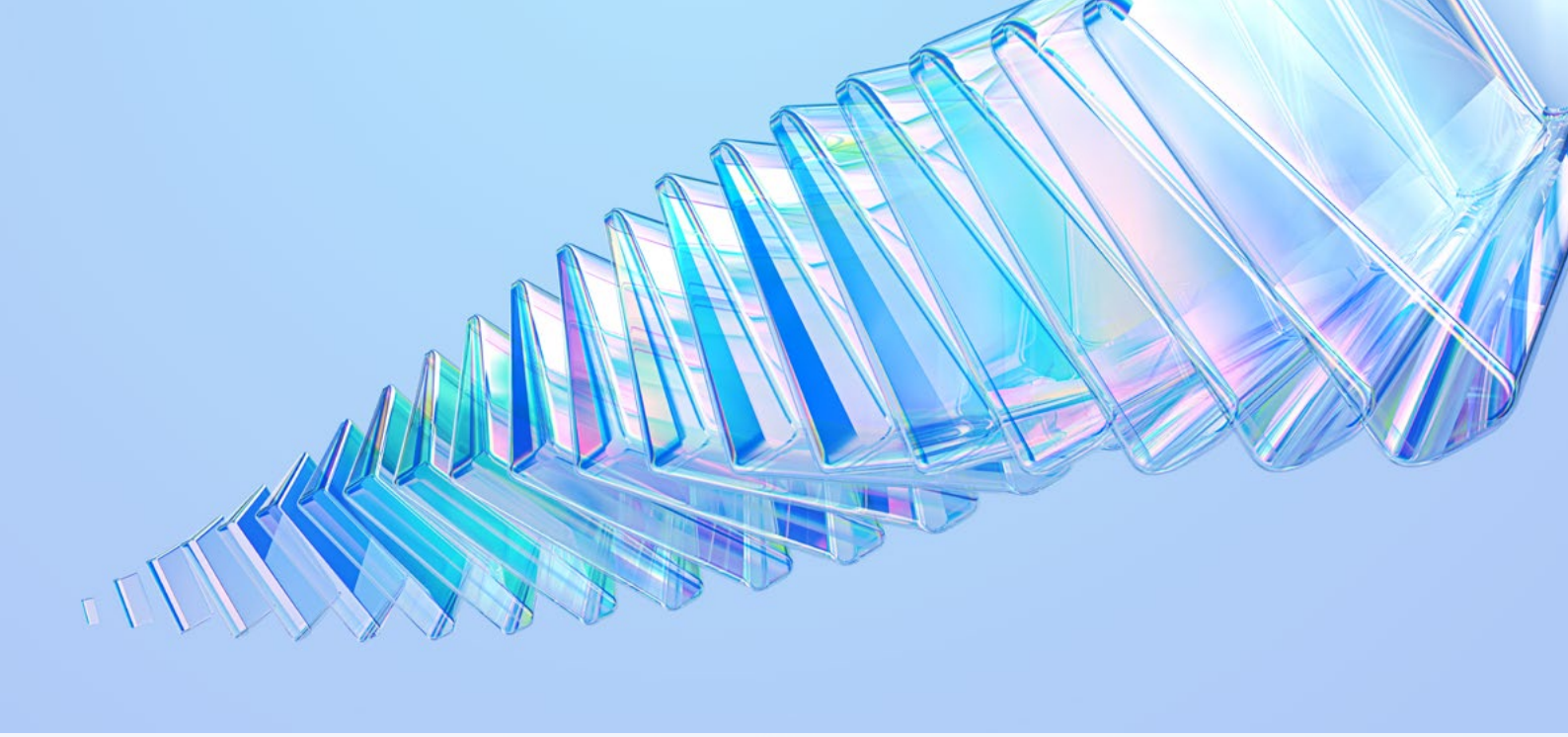
АВТОРЫ

АЛЕКСАНДР МОРКОВЧИН

Руководитель группы аналитики и исследований департамента консалтинга, «Инфосистемы Джет»

АСКАР МУСАЕВ

Эксперт по непрерывности бизнеса, «Инфосистемы Джет»



КЛЮЧЕВЫЕ ВЫВОДЫ

Инциденты ИБ и масштабные ИТ-сбои — главные риски прерывания бизнеса. Классические риски, такие как природные и техногенные катастрофы, пандемии, отошли на второй план.

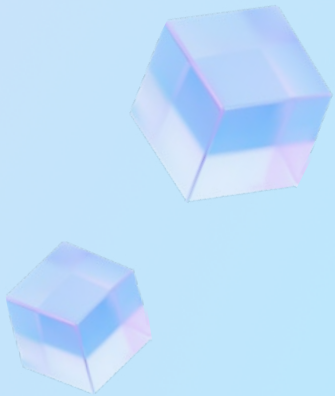
37% компаний полагаются на резервное копирование как на гарантию восстановления ИТ-систем в случае сбоев, однако каждая пятая компания не принимает никаких мер по дополнительной защите резервных копий.

Более чем в половине компаний основным владельцем процесса обеспечения непрерывности бизнеса является департамент ИТ. Это приводит к смещению приоритетов с восстановления бизнеса на восстановление ИТ-ландшафта.

70% компаний проводят тестирования планов аварийного восстановления, но только малая часть из них использует метод симуляции аварии в инфраструктуре.

Кризис-менеджмент в большинстве компаний — скорее, реактивный процесс. Реагирование на масштабный инцидент происходит ситуационно, при этом 40% компаний готовы публично рассказывать об инциденте.

BIA, оценка рисков и тестирования планов восстановления деятельности — приоритетные направления развития системы управления непрерывностью бизнеса для большинства компаний.



Только 20% компаний имеют согласованную с бизнесом последовательность восстановления ИТ-систем в случае инцидента.

ВВЕДЕНИЕ

Система управления непрерывностью бизнеса, как и любые системы управления, развивается с учетом вызовов, меняющих мир. За последние десятилетия компаниям из разных отраслей так или иначе пришлось реагировать и восстанавливаться после реализации различных рисков, влияющих на устойчивость бизнеса. И если с классическими угрозами непрерывности, такими как чрезвычайные ситуации, пандемии или техногенные аварии, многие компании уже научились справляться, то инциденты ИБ, например, атаки с использованием вирусов-шифровальщиков, через призму управления непрерывностью бизнеса рассматривались крайне редко до появления направления киберустойчивости.

Чтобы «План Б» был встроен в ИТ-архитектуру, а хаотичные последствия кибератак превратились в управляемый процесс восстановления, необходимо не только обнаружение и предотвращение инцидента, но и реагирование с последующим восстановлением бизнеса, если киберинцидент реализовался (рис. 1). Для этого подходит практика управле-

Киберустойчивость — способность организации непрерывно предоставлять свои услуги и выпускать продукты, несмотря на любые неблагоприятные киберинциденты, путём активной подготовки к ним, планирования защитных мер, обнаружения и реагирования на киберинциденты, а также восстановления организации после кибератак.

Адаптация к меняющимся угрозам, эффективное обучение персонала и обеспечение тестирований планов реагирования и восстановления помогают построить антихрупкую архитектуру ИТ — новую норму зрелости бизнеса, способную выживать и становиться сильнее после ударов.

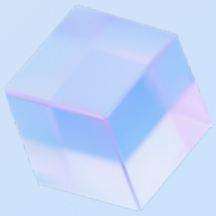
ния непрерывностью бизнеса.

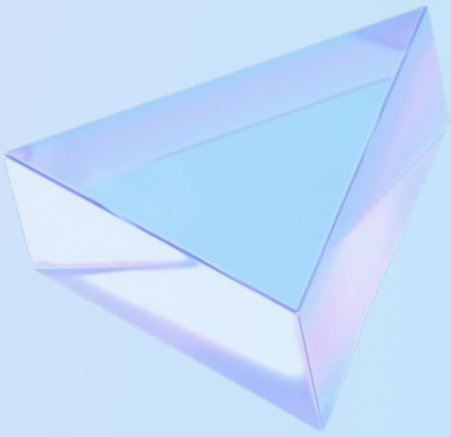
На российском рынке практически не встречается синергия систем управления информационной безопасностью и непрерывностью бизнеса. Для финансового сектора как самой зарегулированной отрасли характерно относить практики непрерывности бизнеса к управлению операционными рисками, в остальных же секторах такие практики чаще всего управляются ИТ.

Таким образом возникает пробел в реализации киберустойчивости организации, заключающийся в отсутствии процесса сквозного реагирования: когда обнаружение, предотвращение и защита от киберинцидента управляются ИБ, а при наступлении значительного негативного влияния, например длительного простоя в случае реализации такого инцидента, хаотично вовлекаются ИТ и бизнес для реактивного управления кризисом и восстановления деятельности компании.

Целью настоящего исследования является оценка текущего состояние практик киберустойчивости, связанных с реагированием и восстановлением после инцидента.

Мы исследовали практики управления непрерывностью бизнеса как одну из важнейших функций киберустойчивости, а также проанализировали, как с помощью этих практик обеспечивается устойчивость компаний при реализации киберинцидентов. Отчет составлен на основе опыта компании «Инфосистемы Джет», полученного в ходе проектов по непрерывности бизнеса и экспертного консалтинга, а также результатов опроса крупных компаний.





РАЗВИТИЕ ТРЕНДА НА КИБЕРУСТОЙЧИВОСТЬ

С середины 2010-х мы наблюдаем усиление тренда на интеграцию кибербезопасности и непрерывности бизнеса в единый подход киберустойчивости, признающий неизбежность инцидентов и фокусирующийся на способности организаций эффективно противостоять угрозам и быстро восстанавливаться. Ранее киберугрозы не рассматривались как основной риск нарушения устойчивости компаний, однако фокус смещается, и сегодня, по данным Business Continuity Institute, главными рисками непрерывного функционирования организаций по всему миру являются кибератаки[1].

Наш опыт и опрос компаний рынка показывают, что классические риски непрерывности бизнеса отходят на второй план, а главной угрозой прерывания бизнеса для компаний становятся кибератаки.

Какие наиболее вероятные угрозы прерывания деятельности вы видите для своей организации?

[1] По данным BCI Horizon Scan Report 2024 https://www.thebci.org/resource/bci-horizon-scan-report-2024.html

Немаловажным фактором интереса к киберустойчивости являются и громкие инциденты, вызванные атаками с использованием вирусов-шифровальщиков, с которыми российские компании массово столкнулись с 2022 года. Вектор требований бизнеса к кибербезопасности смещается с вопроса «может ли такое произойти с нами?» на вопрос «что мы будем делать, если такое произойдет с нами?», ответить на который не всегда сможет кибербезопасность, но должна ответить киберустойчивость.

Ключевые материалы:

- White Paper от Всемирного экономического форума The Cyber Resilience Index: Advancing Organizational Cyber Resilience[2].
- Resilience Management Model от Software Engineering Institute[3].
- Cyber resilience review от CISA[4] с серией гайдлайнов по каждой практике.
- Cyber Resiliency Metrics, Measures of Effectiveness and Scoring[5] от MITRE, предлагающее продвинутую оценку эффективности киберустойчивости в организации.

[2] https://www.weforum.org/publications/the-cyber-resilience-index-advancing-organizational-cyber-resilience/

[3] https://www.sei.cmu.edu/library/cert-resilience-management-model-cert-rmm-version-12/

[4] https://www.cisa.gov/resources-tools/services/cyber-resilience-review-crr

[5] https://www.mitre.org/sites/default/files/2021-11/prs-18-2579-cyber-resiliency-metrics-measures-of-effectiveness-and-scoring.pdf

ФАЗЫ УПРАВЛЕНИЯ НЕПРЕРЫВНОСТЬЮ БИЗНЕСА В КОНТЕКСТЕ КИБЕРУСТОЙЧИВОСТИ

Рассмотрим основные этапы реагирования на киберинциденты и восстановления **через призму непрерывности бизнеса** и обозначим ключевые проблемы российских компаний на каждом этапе реагирования, а также поделимся рекомендациями для совершенствования процессов реагирования и восстановления.

С точки зрения киберустойчивости киберинцидент, влияющий на непрерывность деятельности компании, рано или поздно произойдёт, а значит, организация должна быть готова к реагированию и восстановлению. Именно за эти этапы ответственны практики непрерывности бизнеса, включающие в себя кризисное реагирование и коммуникации, восстановление бизнес-процессов и ресурсов и последующее возвращение в штатный режим.

Мы взглянули на инцидент, связанный с вирусом-шифровальщиком, с точки зрения непрерывности бизнеса и разобрали отдельные практики, отвечающие за реагирование и восстановление.

1. **Управление: планирование и подготовка процесса непрерывности бизнеса**
2. **Кризис-менеджмент: реагирование на инциденты**
3. **Непрерывность бизнеса: обеспечение непрерывности деятельности компании**
4. **Непрерывность бизнеса: восстановление и возврат к штатному функционированию**

Далее представлен анализ текущего состояния некоторых практик киберустойчивости для соответствующих этапов жизненного цикла киберинцидента.

1. УПРАВЛЕНИЕ: ПЛАНИРОВАНИЕ И ПОДГОТОВКА ПРОЦЕССА НЕПРЕРЫВНОСТИ БИЗНЕСА

Этот этап выстраивания киберустойчивости предполагает организацию в компании всех процессов управления практиками, включая область действия, владельцев и ответственность. Рассмотрим, как управление непрерывностью выстраивается в компаниях как отдельный процесс или часть общей киберустойчивости.

Отправной точкой для оценки эффективности практик управления непрерывностью бизнеса является как наличие процесса, управляющего такими практиками, так и правильные его границы.

В 31%

опрошенных нами компаний нет выделенного процесса

В 61%

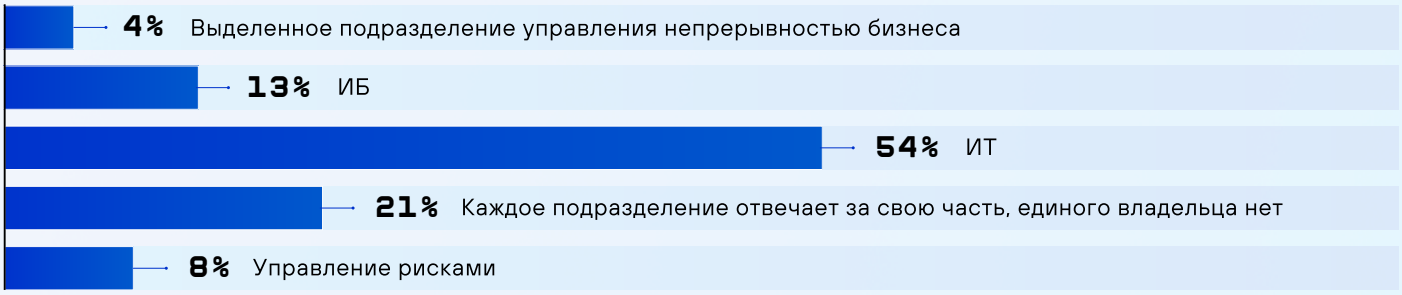
управление непрерывностью распространяется только на ИТ- и ИБ-функции

Зачастую это обусловлено традиционной для России практикой, когда владельцем процесса является ИТ-подразделение — в его область интереса входят, как правило, инфраструктурные сервисы и бизнес-системы.

Недостатки подхода с точки зрения киберустойчивости

Выбор стратегий реагирования и принятия решений должен учитывать возможности и требования бизнеса, опираться на BIA и не замыкаться на ИТ: если киберустойчивость будет распространяться только внутри ИТ- и ИБ-подразделений, фокус будет смещён на восстановление конкретных инструментов для работы бизнеса (например, информационные системы), а не на восстановление бизнеса и поддержание его репутации во время инцидента.

Какое подразделение является основным владельцем процессов управления непрерывностью?



Недостаточное внимание к бизнес-процессам и их зависимостям приводит к последующим серьёзным ошибкам при приоритизации восстановления ИТ-систем, когда некритичные сервисы восстанавливаются быстрее, чем действительно необходимые для функционирования бизнеса. Также определение критичности, как показывает наш проектный опыт, зачастую носит субъективный характер или опирается на устаревшие исторические данные, вследствие чего важные системы выпадают из фокуса.

Кейс из практики

В одной из компаний частота резервного копирования кадровой системы была определена экспертным путём внутри ИТ на основе средней частоты вносимых в неё изменений. При возникновении инцидента с повреждением базы она была восстановлена на состояние нескольких дней назад, что оказалось критичным для бизнеса, так как подходил срок сдачи отчётности и за эти несколько дней в базу вносилось большее число изменений, чем обычно. Бизнес не был вовлечён в определение критичности используемых ресурсов, а ИТ-подразделение не подозревало о пиковых нагрузках на процесс в определенное время.

В целом, мы наблюдаем ограниченность практик непрерывности бизнеса на рынке. В большинстве компаний либо существуют отдельные, не связанные друг с другом, процесс реагирования и восстановления после ИТ-сбоев и процесс управления нештатными и чрезвычайными ситуациями, либо же второй процесс отсутствует как таковой.

Варианты для повышения киберустойчивости организации

Интеграция практик управления непрерывностью бизнеса во все процессы компании, а также вовлечённость руководства — ключевые факторы успеха киберустойчивости. Одним из инструментов для реализации таких требований может служить BIA — как основной инструмент, помогающий сфокусироваться на требованиях бизнеса к киберустойчивости.

2. КРИЗИС-МЕНЕДЖМЕНТ: РЕАГИРОВАНИЕ НА ИНЦИДЕНТЫ

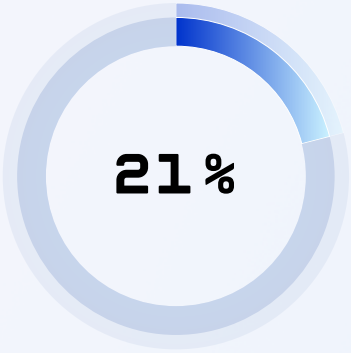
На данном этапе в компании планируется процесс реагирования на инцидент. С точки зрения кибербезопасности для реагирования обычно достаточно плейбуков и плана информирования CISO. Однако с точки зрения киберустойчивости практики кризис-менеджмента являются связующим звеном между кибербезопасностью и последующим восстановлением бизнеса, так как определяют дальнейшее взаимодействие между подразделениями — роли, полномочия и ответственность за принимаемые решения.

Кризис-менеджмент предполагает наличие у организации предварительно проделанной работы по развитию процесса реагирования, то есть само реагирование становится плановым: определены работники и роли, задействованные в управлении кризисом, подготовлены планы коммуникаций. На практике мы чаще всего наблюдаем ситуационное реагирование, где всё определяется уже в момент инцидента.

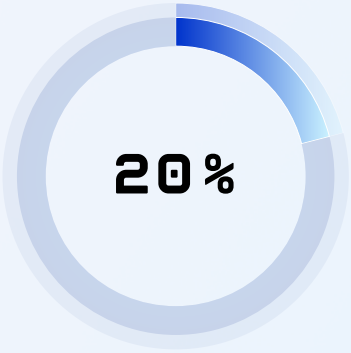
Недостатки подхода с точки зрения киберустойчивости

Отсутствие выстроенного процесса реагирования при масштабном инциденте приводит к потере времени на принятие ключевых решений. Из-за сбора команды, разработки и согласования коммуникаций, погружения в детали инцидента компания восстанавливается дольше, что уменьшает шанс остаться устойчивой после кризиса, так как восстановление может не произойти в целевое время.

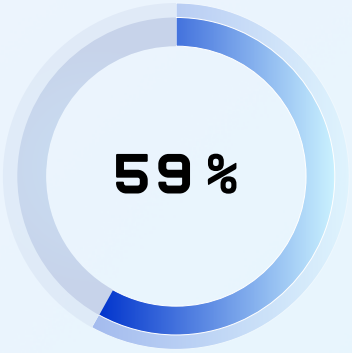
Есть ли в организации определенная команда реагирования на кризисную ситуацию (выделенные роли/должности, которые участвуют в реагировании)?



Да, внутри подразделения (координаторы в ИТ и/или в ИБ)



Да, на уровне всей организации (топ-менеджмент, маркетинг, ИТ, ИБ, HR, бизнес)



Нет, участники реагирования собираются ситуационно в зависимости от инцидента

Не менее важным аспектом снижения последствий масштабного инцидента является и скорость оповещения работников организации.

70%

компаний используют корпоративные каналы или мессенджеры

В **16%**

компаний используются автоматизированные инструменты

Это объясняется не только недостаточным вниманием к процессу реагирования, но и возможными рисками при автоматизации процесса — случайной/преждевременной отправкой коммуникации или сбоем в системе автоматизации в нужный момент.

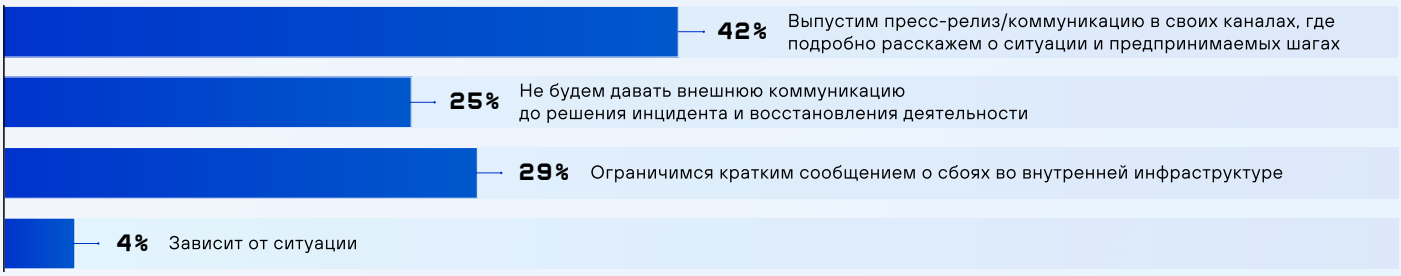
С точки зрения эффективной коммуникации однозначных рекомендаций к использованию конкретного инструмента не существует. Каждая компания самостоятельно определяет: использовать каскадную рассылку через руководителей или напрямую информировать всех сотрудников. Наиболее важным в таком случае является периодическое тестирование каналов и скорости оповещений.

Крупные инциденты, произошедшие за 2024 год, постепенно меняют отношение компаний ко внешним коммуникациям. Если раньше в случае шифрования данных компании могли долго тянуть с внешними коммуникациями, то сегодня «практика умалчивания» не столь распространена. Важно отметить, что открытость и детальное информирование о ходе реагирования и восстановления чаще применяют организации, которые уже сталкивались с масштабными сбоями в своей работе.

Варианты для повышения киберустойчивости организации

Основной задачей для организации является выстраивание эффективного процесса реагирования. Должны быть сформулированы критерии, когда событие или потенциальный инцидент кибербезопасности может перейти в масштабный кризис и требуется подключение практик кризис-менеджмента. Простой и понятный план кризисного реагирования, включающий стратегию коммуникаций компании, ответственных и роли по управлению кризисом, снизит затраты времени при реагировании и поможет фокусироваться на инциденте, не отвлекаясь на сопутствующие организационные процессы.

Коммуникационная стратегия является частью плана реагирования на кризис и призвана ускорить как внутренние, так и внешние коммуникации компании. Следует заранее утвердить стратегию — например, раскрывать ли детали инцидента или дать краткое сообщение о сбое.



3. НЕПРЕРЫВНОСТЬ БИЗНЕСА: ОБЕСПЕЧЕНИЕ НЕПРЕРЫВНОСТИ ДЕЯТЕЛЬНОСТИ КОМПАНИИ

Для того чтобы компания была киберустойчивой, крайне важным является продолжение работы ключевых направлений её деятельности во время инцидента. На этом этапе в компании должно быть понимание, могут ли бизнес и его наиболее критичные составляющие продолжать функционировать во время инцидента, как именно и что для этого нужно.

Более половины опрошенных компаний имеют хотя бы один план обеспечения непрерывности бизнеса, который, однако, часто имеет формальный характер и необходим для соответствия регуляторным требованиям. Для успешной активации такой план должен быть протестирован, а в его создание должны быть вовлечены представители бизнеса. В то же время из-за высокой зависимости современных организаций от ИТ-систем задача не всегда выполнима, потому что бизнес-процессы могут не иметь альтернативных способов исполнения. В таком случае во время кризисной ситуации становится важной приоритетность восстановления различных процессов. Чем меньше ключевые продукты, сервисы или услуги компании будут недоступны, тем ниже потери, как финансовые, так и репутационные.

Для определения критичности бизнес-процессов с точки зрения практик непрерывности бизнеса применяется BIA. Инструмент позволяет ранжировать процессы компании с точки зрения нарастания ущерба во время их простоя и определять, что и в каком порядке должно восстанавливаться.

Недостатки подхода с точки зрения киберустойчивости

В стрессовых условиях организация опирается на опыт отдельных экспертов, который может быть ошибочным. Например, процессы отгрузки и логистики товара могут уступать по приоритетности процессу продаж по результатам BIA. Оставаться на связи с клиентами для компании может быть важнее, чем доставка продукции без задержек.

20%

компаний применяют BIA как инструмент приоритизации

59%

компаний полагаются на ситуационное определение критичности

В **21%**

приоритетность восстановления не определяется

BIA несет дополнительные выгоды для ИТ- и ИБ-подразделений

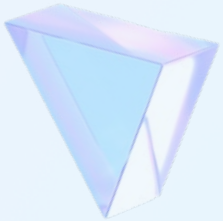
40% компаний используют результаты анализа для обоснования бюджета на киберустойчивость.

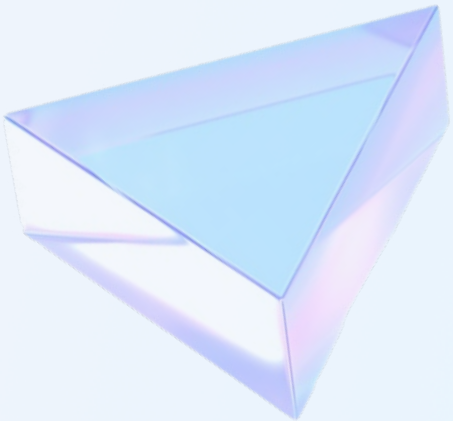
Варианты для повышения киберустойчивости организации

Основным критерием оценки эффективности практики является зрелость бизнес-процессов компании с точки зрения непрерывности. Это достигается внедрением периодического анализа воздействия на бизнес, в рамках которого также могут быть изучены альтернативные варианты функционирования процессов для последующей подготовки планов обеспечения непрерывности. Совокупность планов и понимания очередности восстановления в кризисной ситуации повышает шансы компании оставаться киберустойчивой во время инцидента.

Кейс из практики

Определение потенциальных потерь от простоя критически важных процессов компании помогло департаменту ИТ обосновать бюджет на модернизацию системы резервного копирования. Сравнив величину инвестиций для достижения требуемого бизнесом времени восстановления и размер ущерба при текущей системе резервного копирования, было принято решение о модернизации.

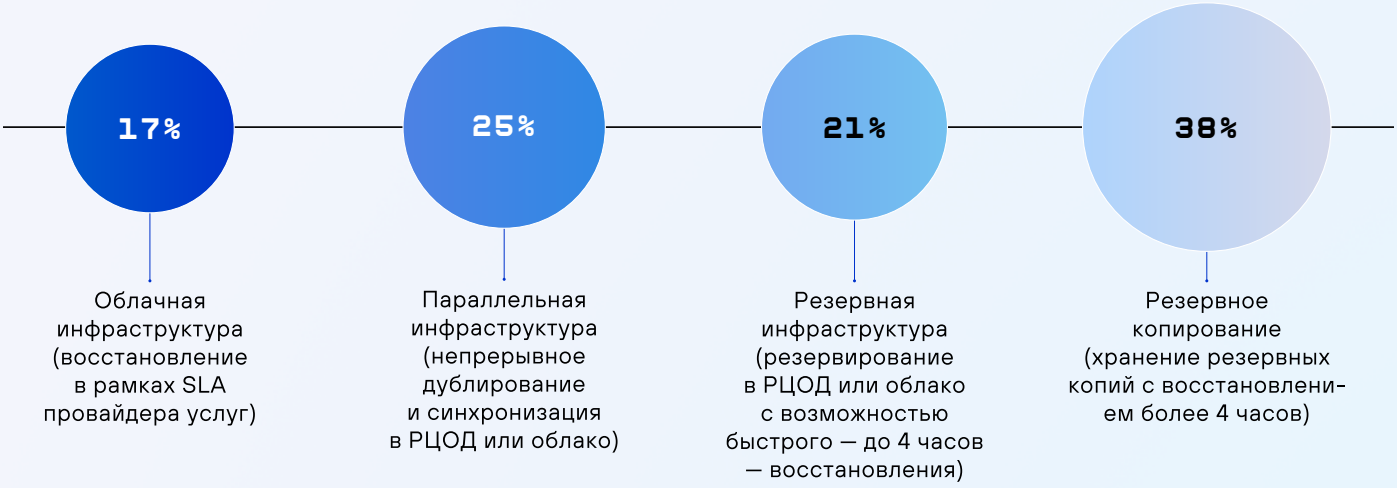




4. НЕПРЕРЫВНОСТЬ БИЗНЕСА: ВОССТАНОВЛЕНИЕ И ВОЗВРАТ К ШТАТНОМУ ФУНКЦИОНИРОВАНИЮ

На данном этапе в компании должны быть определены необходимые ресурсы, в первую очередь ИТ-системы, для восстановления работы бизнеса, а также очередность, скорость и возможность их восстановления.

Скорость восстановления ИТ-систем и актуальных данных определяет размер ущерба, понесённого организацией. Учитывая, что управление непрерывностью бизнеса для многих организаций ассоциируется с ИТ, практики аварийного восстановления (Disaster Recovery) наряду с кибербезопасностью находятся на более высоком уровне зрелости по сравнению с остальными составляющими киберустойчивости, такими как кризисное реагирование и восстановление бизнеса.



Главной проблемой при восстановлении ИТ-ресурсов компании остаётся слабое вовлечение бизнеса и смежных подразделений.

В подтверждение практического опыта выявлено:

25%

компаний, проводящих Business Impact Analysis, используют его результаты в том числе для определения критичности ИТ-систем

63%

при классификации исходят из своих экспертных знаний внутри подразделения ИТ или из текущих мощностей инфраструктуры

Одним из факторов оценки эффективности киберустойчивости является надежная система кибербезопасности. Это подталкивает компании включать средства защиты в область действия практик аварийного восстановления и расширять синергию ИТ- и ИБ-подразделений.

>30%

компаний уже оценивают свои системы обеспечения кибербезопасности как критически важные для киберустойчивости и обеспечивают возможность их быстрого восстановления.

Недостатки подхода с точки зрения киберустойчивости

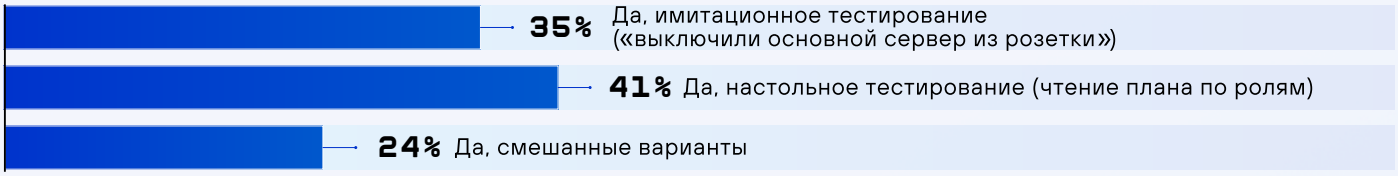
Смещение фокуса в обеспечении киберустойчивости создает для компании ложные ожидания: инвестиции выделяются, строится катастрофоустойчивая инфраструктура, но при возникновении инцидента оказывается, что ожидания бизнеса в части доступности ИТ-систем не соответствуют текущим параметрам резервирования. В конечном итоге только треть компаний восстанавливается в целевое для бизнеса время.

Эффективное взаимодействие ИТ и ИБ также важно при тестировании DR-планов. Сценарий тестирования, предполагающий атаку вируса-шифровальщика, может включать в себя в том числе практический анализ защищённости контура резервного копирования. Защита резервных копий при таком инциденте не менее важна, однако сейчас мы видим, что этому вопросу уделяется недостаточное внимание.

* можно было дать несколько вариантов ответа

Кейс из практики

При настольном тестировании киберустойчивости и совместной отработки действий командами ИБ и ИТ при реализации инцидента с вирусом-шифровальщиком мы выявили критическую зависимость аварийного восстановления от системы хранения паролей. При реальном шифровании база паролей могла бы быть утрачена, что усложнило бы восстановление критичных ИТ-ресурсов. Для решения проблемы были предложены альтернативные варианты хранения паролей с доступом к ним только во время кризисной ситуации.



70%

компаний проводят тестирование DR-планов, однако наиболее популярным остаётся настольное тестирование, которое не даёт должной степени уверенности в способности восстановить ИТ-инфраструктуру.

Варианты для повышения киберустойчивости организации

Выстраивание процессов и написание планов принесут пользу при реагировании и восстановлении, но не помогут компании восстановиться без наличия резервных копий, инфраструктуры и необходимых специалистов. Комплексные проверки и тестирования как «бумажной» составляющей, так и готовности ИТ-инфраструктуры дадут ответ, насколько компания киберустойчива.

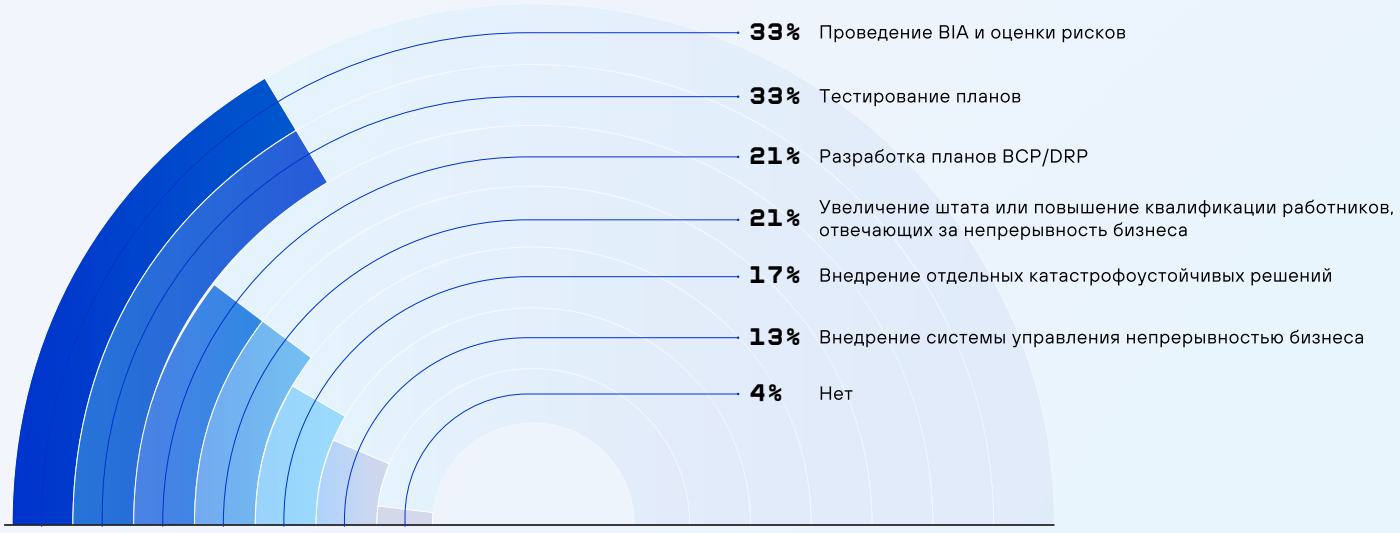
Трудоёмкость и ресурсозатратность организации имитационного тестирования (полноценной симуляции инцидента), на наш взгляд, являются основными причинами отказа от этого вида учений.

ЗАКЛЮЧЕНИЕ

Зрелость практик, обеспечивающих киберустойчивость организаций, находится на разных уровнях: упор на кибербезопасность со стороны подразделений ИБ и на восстановление систем в ИТ приносит результат, но не делает компанию киберустойчивой.

Взгляд только на некоторые практики, а не на весь процесс целиком может привести к закономерному результату — например, отличной защите периметра и высоким показателям восстановления из резервных копий, но полному отсутствию защиты контура СРК. Так, плохо организованные процессы реагирования и восстановления приводят к существенному ущербу.

Зрелые практики непрерывности бизнеса являются важной составляющей антихрупкой ИТ-архитектуры компании — процесс восстановления уже ставят в приоритет.



* можно было дать несколько вариантов ответа

Построение антихрупкой ИТ-архитектуры невозможно без принятия факта, что киберинцидент может произойти, а значит, нужно быть готовым отреагировать на него и восстановить бизнес, не ограничиваясь вовлечением в определенную практику. Ситуация, в которой кризисы становятся катализатором развития, а восстановление превращается в управляемый процесс, ведущий к укреплению всей инфраструктуры ИТ, — новый уровень зрелости российского бизнеса. Это переход на новый уровень.

JET
SECURITY
TEAM

security@jet.su
jetcsirt.su