

От защиты к непрерывности

Семейство ГОСТ Р 57580 как основа киберустойчивости



Текст

ТАРАС МАКАРЕНКО,

РУКОВОДИТЕЛЬ НАПРАВЛЕНИЯ «СТРАТЕГИЯ И РИСКИ» КОМПАНИИ ИНФОРМЗАЩИТА

Киберустойчивость — это способность организации предвидеть негативные киберсобытия, противостоять им, восстанавливаться и адаптироваться к ним, сохраняя непрерывность ключевых операций. В отличие от традиционного подхода, ориентированного только на предотвращение угроз, киберустойчивость исходит из принципа «киберинциденты неизбежны» и делает упор на готовность к восстановлению в приемлемые для бизнеса сроки. Такой сдвиг в акцентах означает, что для бизнеса важно минимизировать влияние киберинцидентов — обеспечить работу критичных процессов даже в условиях успешной кибератаки, затронувшей критические системы организации.

Экономика киберустойчивости несложна: каждая минута простоя — прямые потери и удар по доверию клиентов. 93% крупных компаний оценивают простой дороже 25 млн рублей в час, почти половина — свыше

100 млн рублей в час, поэтому стейкхолдеры требуют метрики устойчивости, планы восстановления и регулярные тренировки, регуляторы усиливают требования к непрерывности и надежности, а страховые компании при киберстраховании проверяют наличие планов реагирования и резервных копий.

Четыре компонента киберустойчивости от «Информзащиты» на базе семейства стандартов ГОСТ Р 57580

Опираясь на более чем 30-летний практический опыт «Информзащиты» в области ИБ, управления рисками и реагирования на киберинциденты, а также обеспечения непрерывности и киберустойчивости, мы разработали методологию киберзащиты как целостную систему из четырех взаимосвязанных компонентов. Каждый из них отвечает за свой аспект готовности организации к киберинцидентам и эффективному восстановлению после них:

- 1) **ВИА (Business Impact Analysis)** — оценка влияния киберинцидентов на бизнес;
- 2) **оценка рисков ИБ** — выявление и оценка киберрисков, имеющих наибольшее влияние на бизнес;
- 3) **обеспечение ИБ** — система управления и обеспечения ИБ;
- 4) **BCM (Business Continuity Management)** — система управления непрерывностью бизнеса и восстановлением при киберинцидентах.

В качестве одного из практических подходов к реализации киберустойчивости мы рассмотрели серию стандартов ГОСТ Р 57580, разработанную при участии Банка России и предназначенную для практического внедрения и оценки зрелости киберустойчивости финансовых организаций. В инфографике привели ключевые аспекты этой серии и их влияние на киберустойчивость.

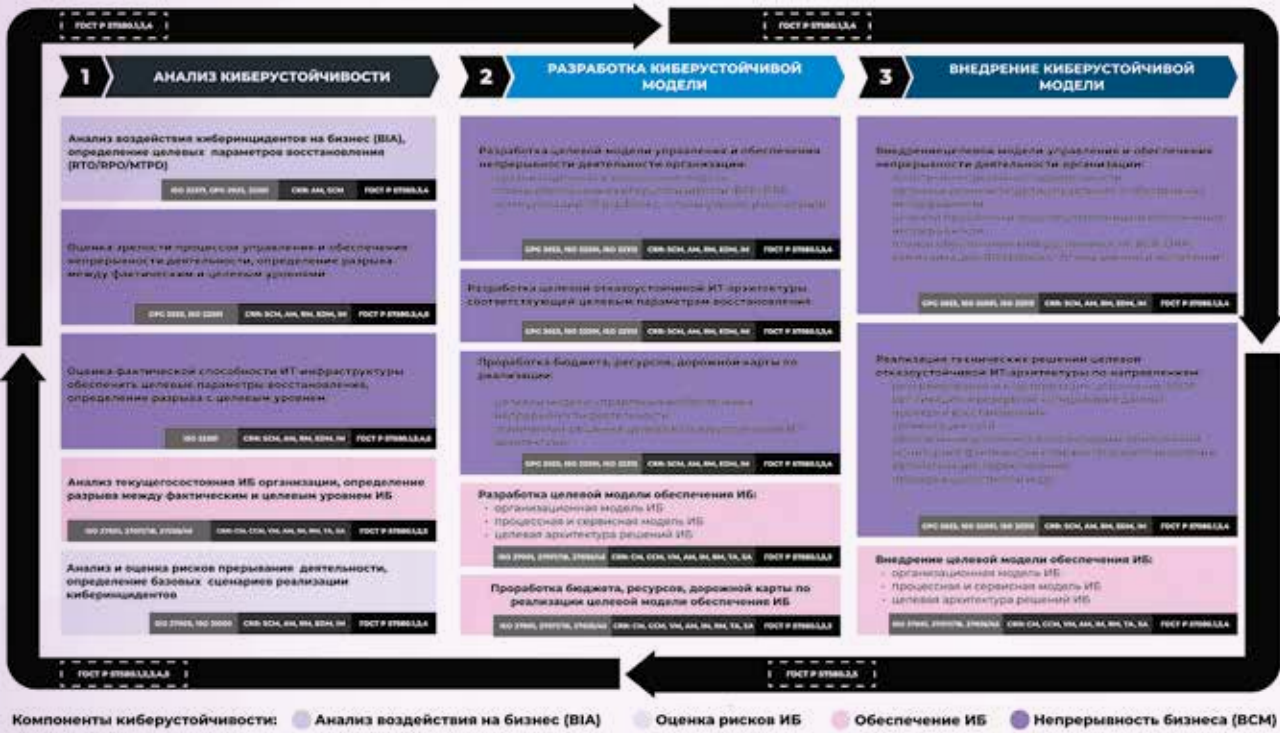
Четыре компонента киберустойчивости работают не изолированно, а как единая система: выход одного является входом для другого. Результаты ВИА используются в оценке рисков ИБ — как база для оценки уровня последствий киберинцидентов. ВИА и оценка рисков ИБ задают параметры для ИБ и BCM: на основе RTO/RPO критичных процессов формируются требования к резервным решениям и плану восстановления, определяется фокус ИБ-контролей и учитываются внешние зависимости от поставщиков и аутсорсеров. Киберустойчивость — не статичное состояние, а постоянное развитие ВИА, риск-оценки, ИБ-мер и BCM на основе инцидентов и учений. Семейство стандартов ГОСТ 57580 рекомендует итеративный цикл постоянного улучшения ки-



берустойчивости «планируй — реализуй — контролируй — совершенствуй».

В качестве альтернативы и одновременно практического дополнения к серии стандартов ГОСТ Р 57580 мы рассмотрели методологию Cyber Resilience Review (CRR) — процессно-ориентированный подход, разработанный агентством по кибербезопасности и безопасности инфраструктуры (CISA) Министерства внутренней безопасности США (DHS) для оценки киберустойчивости организаций.

Экономика киберустойчивости несложна: каждая минута простоя — прямые потери и удар по доверию клиентов. 93% крупных компаний оценивают простой дороже 25 млн рублей в час, почти половина — свыше 100 млн рублей в час



CRR сфокусирован на операционной устойчивости — способности организации поддерживать ключевые услуги и управлять киберрисками как в штатном, так и в кризисном режимах. Она опирается на модель CERT-RMM и оценивает зрелость десяти процессов: управление активами, средствами контроля, конфигурацией, уязвимостями, инцидентами, непрерывностью обслуживания, рисками, внешними зависимостями, обучением и ситуационной осведомленностью.

Семейство стандартов ГОСТ Р 57580, как показывает наш анализ, сопоставимо с методологией CRR. При этом последняя в большей степени выступает как практический «сканер» программы киберустойчивости для оценки зрелости, тогда как рассматриваемое семейство ГОСТ — как прикладной инструмент внедрения организационных и технических мер.

Практические рекомендации по внедрению киберустойчивости от «Информзащиты» на базе ГОСТ Р 57580 и CRR

В заключение представим наши практические рекомендации по внедрению киберустойчивости и продемонстрируем, как семейство стандартов ГОСТ Р 57580 и методика CRR могут использоваться на отдельных шагах и этапах реализации подобных проектов. Представленный в инфографике подход в первую очередь будет интересен руководителям ИБ и ИТ, а также владельцам ключевых бизнес-процессов, вовлеченным в разработку и реализацию программ киберустойчивости в своих организациях.

Эффективность программы киберустойчивости определяется качеством ее управления. В крупных организациях целесообразно учреждать межфункциональный комитет по непрерывности бизнеса и киберустойчивости с участием ИТ, ИБ, руководителя по непрерывности (BCM-координатора), представителей ключевых бизнес-линий. Комитет утверждает политику, рассматривает результаты BIA и оценки рисков,

Киберустойчивость — не статичное состояние, а постоянное развитие BIA, риск-оценки, ИБ-мер и ВСМ на основе инцидентов и учений. Семейство стандартов ГОСТ 57580 рекомендует итеративный цикл постоянного улучшения киберустойчивости «планируй — реализуй — контролируй — совершенствуй»

согласует бюджеты и принимает отчеты по учениям и инцидентам.

В оргструктуре закрепляются роли: BCM-координатора (владелец BCP и ответственный за его актуализацию), менеджера по киберрискам, а также команды SOC и CERT/CIRT. Ответственность разграничивается: ИТ отвечает за резервную инфраструктуру и резервное копирование; ИБ — за мониторинг и реагирование на атаки; бизнес — за разработку и исполнение BCP. CISO и BCM-координатор не реже одного раза в квартал представляют топ-менеджменту отчет по киберустойчивости с ключевыми метриками и статусом мероприятий, поддерживая приоритет темы и ресурсное обеспечение.