# ISO/IEC 27031:2011 — Information technology — Security techniques — Guidelines for information and communications technology readiness for business continuity

ИСО 27031 предоставляет руководство по концепциям и принципам, лежащим в основе роли информационных и коммуникационных технологий (ИКТ) в обеспечении непрерывности бизнеса.

Стандарт:

Предлагает структуру(согласованный набор методов и процессов) для любой организации - частной, правительственной и неправительственной;

Определяет все соответствующие аспекты, включая критерии эффективности, структуру и детали реализации, для повышения готовности ИКТ как части СМИБ организации, помогая обеспечить непрерывность бизнеса;

Позволяет организации измерить непрерывность, безопасность и, следовательно, готовность ИКТ.

Область применения и цель

Стандарт охватывает все события и инциденты (не только связанные с информационной безопасностью), которые могут оказать влияние на инфраструктуру и системы ИКТ. Поэтому он расширяет практику обработки и управления инцидентами информационной безопасности, планирования готовности к ИКТ и предоставления услуг.

Готовность ИКТ для обеспечения непрерывности бизнеса (ГИКТОНБ) поддерживает управление непрерывностью бизнеса, «гарантируя, что услуги ИКТ настолько устойчивы, насколько это уместно, и могут быть восстановлены до заранее определенных уровней в сроки согласованные с организацией».

Готовность ИКТ важна для обеспечения непрерывности бизнеса, потому что:

* ИКТ широко распространены, и многие организации сильно зависят от ИКТ, поддерживающих важные бизнес-процессы;
* Обеспечивает высшему руководству уверенность в надлежащем сохранении уровня информационной безопасности (конфиденциальность, целостность и доступность) при обеспечении строгого следования политикам информационной безопасности;
* Планирование непрерывности бизнеса является неполным без адекватного рассмотрения и защиты доступности и непрерывности ИКТ.
* Организация потенциально получает конкурентное преимущество благодаря продемонстрированной способности обеспечивать непрерывность бизнеса и поддерживать предоставление услуг и продуктов во время нарушения;
* Обеспечивает достоверный способ определения статуса услуг ИКТ организации в поддержке ее целей обеспечения непрерывности бизнеса, рассматривая вопрос "Способна ли наша ИКТ реагировать?", а не "Является ли наша ИКТ безопасной?".

Готовность ИКТ включает в себя:

* Подготовку ИКТ организации (то есть ИТ-инфраструктуры, операций и приложений), а также связанных процессов и людей к непредвиденным событиям, которые могут изменить среду риска и повлиять на ИКТ и непрерывность бизнеса;
* Использование и оптимизацию ресурсов для обеспечения непрерывности бизнеса, аварийного восстановления, аварийного реагирования и реагирования на инциденты в сфере безопасности ИКТ, а также действий по управлению.

Готовность ИКТ должна, конечно, уменьшить влияние (т.е. степень, продолжительность и / или последствия) инцидентов информационной безопасности на организацию.

Чтобы программа ГИКТОНБ была эффективной, она должна быть процессом, полностью интегрированным с управленческой деятельностью верхнего звена организации, одобренным и поддержанным высшим руководством. Для поддержки и менеджмента программы может потребоваться ряд специалистов с практическим опытом в области и персонал других ведущих направлений деятельности и служб. Количество ресурсов, требуемых для поддержки такой программы, будет зависеть от величины и сложности организации.

Организация должна иметь документально оформленную политику ГИКТОНБ. Политика должна предоставлять организации документально оформленные принципы, к выполнению которых она будет стремиться и по которым может измеряться эффективность

Стандарт также включает циклический подход PDCA (Plan-Do-Check-Act), расширяющий традиционный процесс планирования непрерывности бизнеса для более широкого учета ИКТ. Он включает в себя «методы оценки сценариев отказов», такие как FMEA (анализ отказов и эффектов), с акцентом на выявление «инициирующих событий», которые могут спровоцировать более или менее серьезные инциденты.

