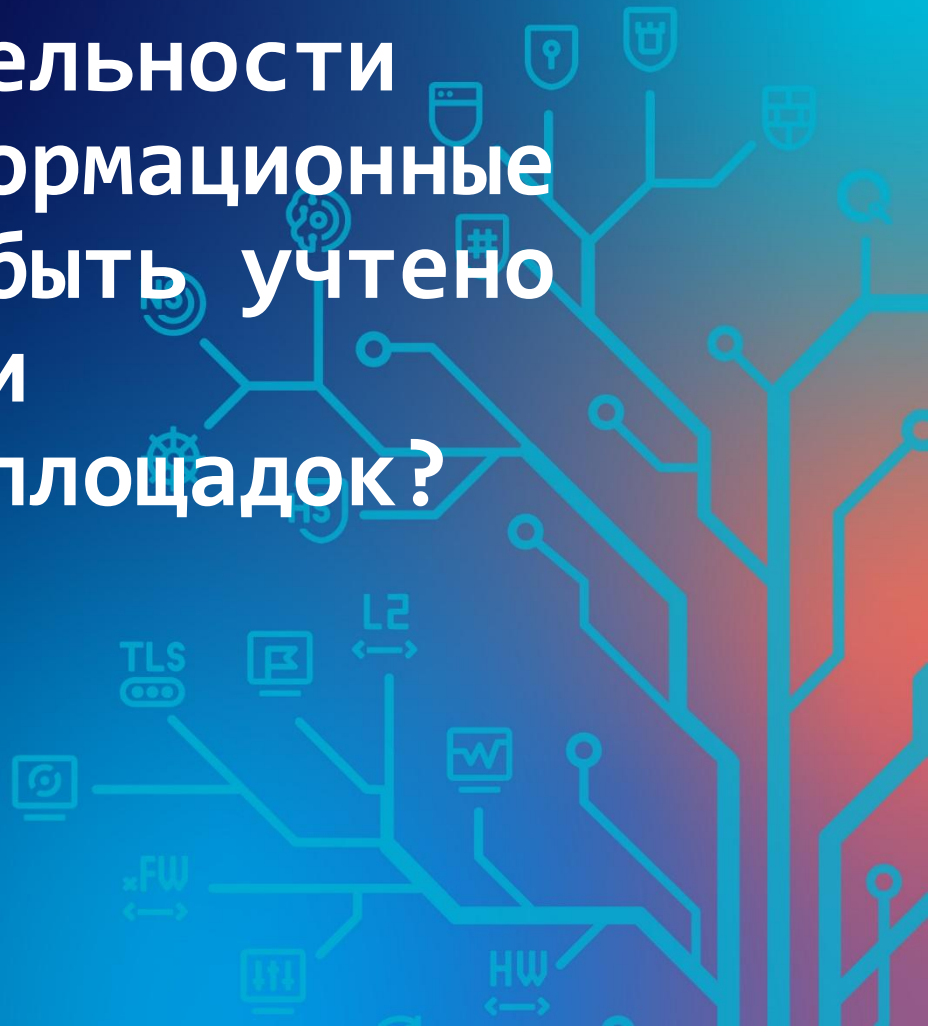
Устойчивость деятельности предприятия и информационные риски. Что может быть учтено при проектировании производственных площадок?

Владимир Голованов
Заместитель начальника отдела



infotecs

Содержание

Устойчивость функционирвоания. Что это такое?

устойчивость (resilience): Способность организации противостоять нарушению, будучи затронутой им.
[п. 3.14 ГОСТ Р ИСО/МЭК 27031-2012]

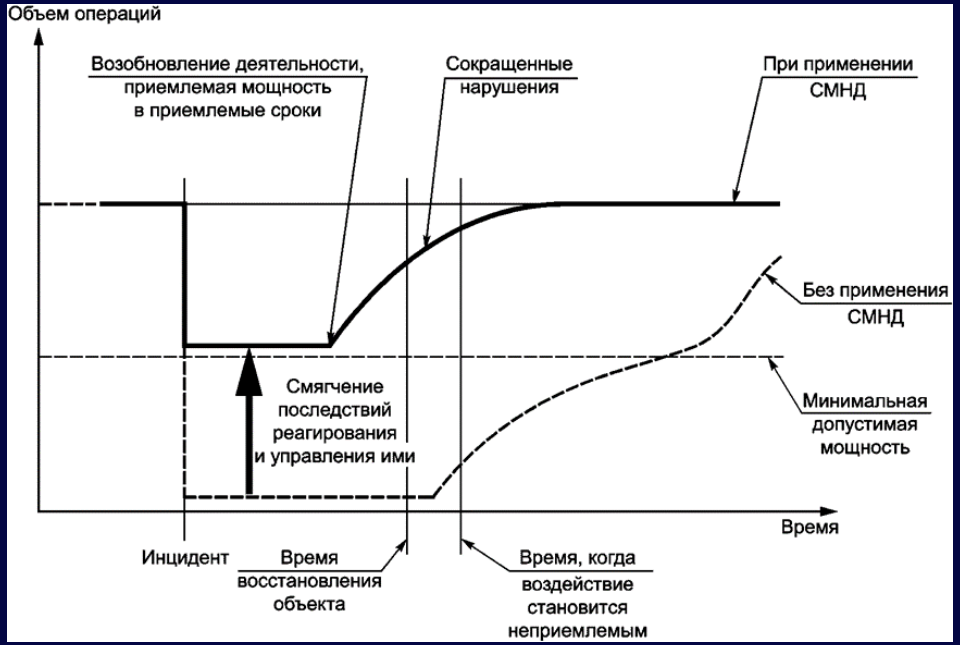
нарушение (disruption): Ожидаемый (например, ураган) или непредвиденный (например, нарушение/прекращение энергоснабжения, землетрясение или атака на системы/инфраструктуру ИКТ) инцидент, который нарушает обычный ход операций на площадке организации.
[п. 3.6 ГОСТ Р ИСО/МЭК 27031-2012]

ГОСТ Р ИСО/МЭК 27031-2012 Информационная технология. Методы и средства обеспечения безопасности. Руководство по готовности информационно-коммуникационных технологий к обеспечению непрерывности бизнеса (ISO/IEC 27031:2011, IDT)

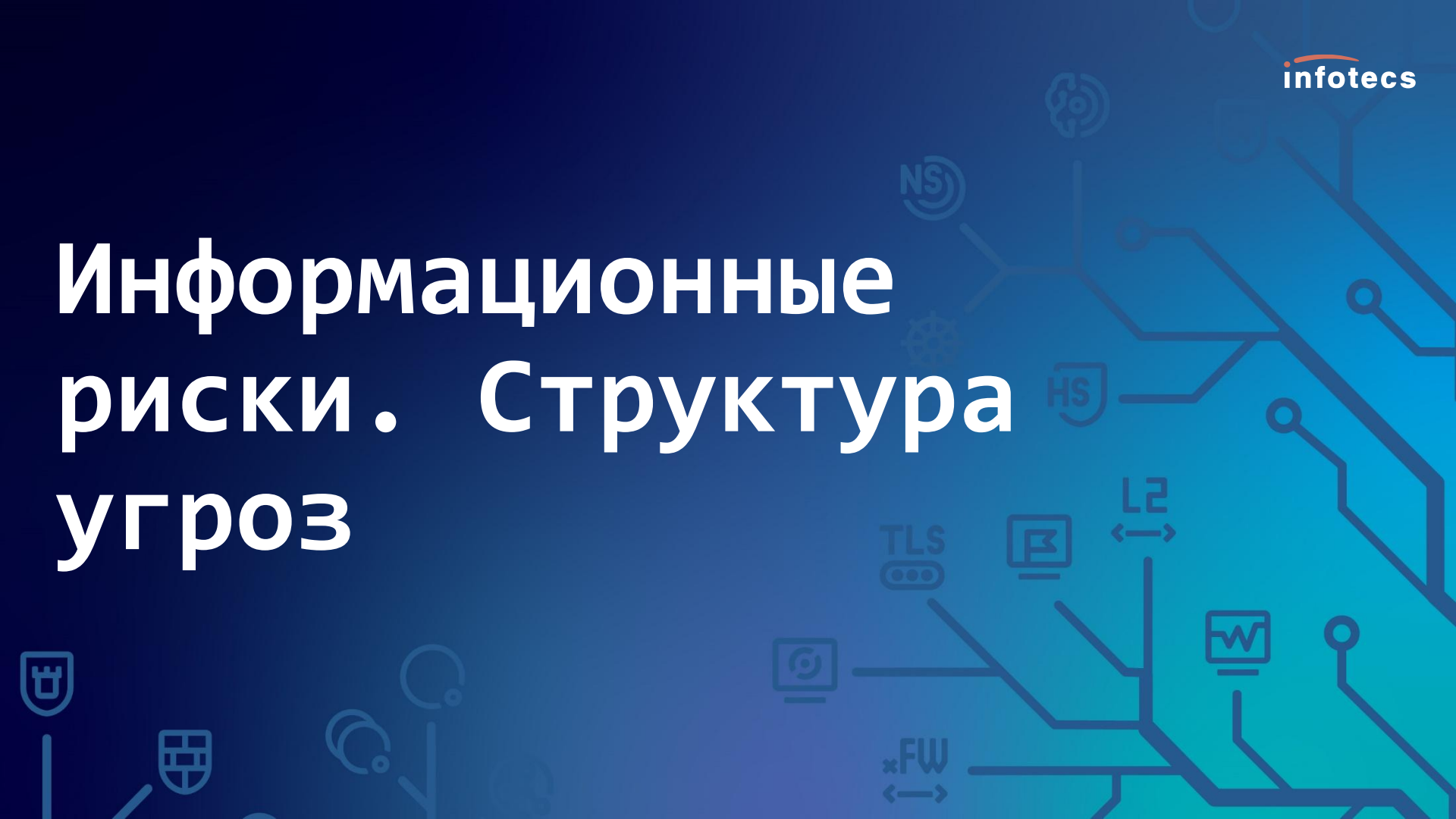
Пример эффективности ОНД при внезапных нарушениях

Обеспечение непрерывности деятельности (ОНД) может [должно] помочь для смягчения последствий в определенных ситуациях

Примечание: Относительное расстояние между этапами, изображенными на диаграмме, не подразумевает никаких конкретных временных рамок.



Информационные риски. Структура угроз



Примеры типовых угроз [для обработки данных]

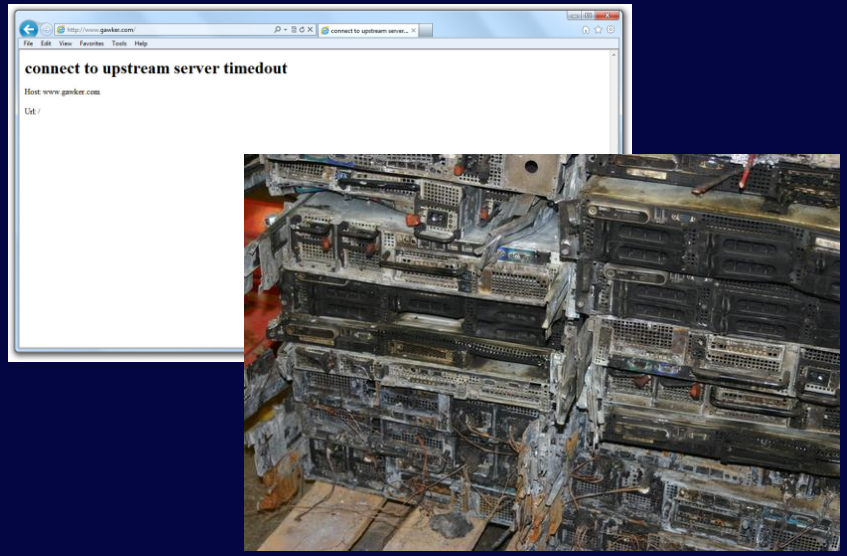
- Угрозы физической природы
- Угрозы природного характера
- Сбои в инфраструктуре
- Технические сбои
- Человеческие действия
- Компрометация функций или услуг
- Организационные угрозы

ISO/IEC 27005:2022 Information security, cybersecurity and privacy protection — Guidance on managing information security risks

Примеры типовых угроз. Киберриски

- Сбои в инфраструктуре
- Технические сбои
- Человеческие действия
- Компрометация функций или услуг
- Организационные угрозы

Примеры типовых угроз. Угрозы природного характера



- Климатическое явление
- Сейсмическое явление
- Вулканическое явление
- Метеорологическое явление
- Наводнение
- Пандемия/эпидемическое явление

https://www.dotcom-monitor.com/blog/hurricanqe-sandy-data-centers-datagram-website-servers-down/

https://pikabu.ru/story/avarii_v_datatsentrakh_kotoryie_byilo_pochti_nevozmozhno_predusmotret_4624749?ysclid=mhvnkarbtz551203801

Примеры типовых угроз. Угрозы физической природы

- Пожар
- Наводнение/затопление
- Загрязнение, вредное излучение
- Крупная авария
- Взрыв
- Пыль, коррозия, замерзание

https://www.fondsk.ru/news/2025/10/09/kto-spalil-cifrovoy-suverenitet-yuzhnoy-korei.html

Инциденты с ИТ на предприятиях

В Южной Корее остановилась работа всей цифровой инфраструктуры

Огонь охватил сервера Национальной службы Информационных Ресурсов (NIRS): **там размещались все государственные сервисы, базы данных и облачные системы.**

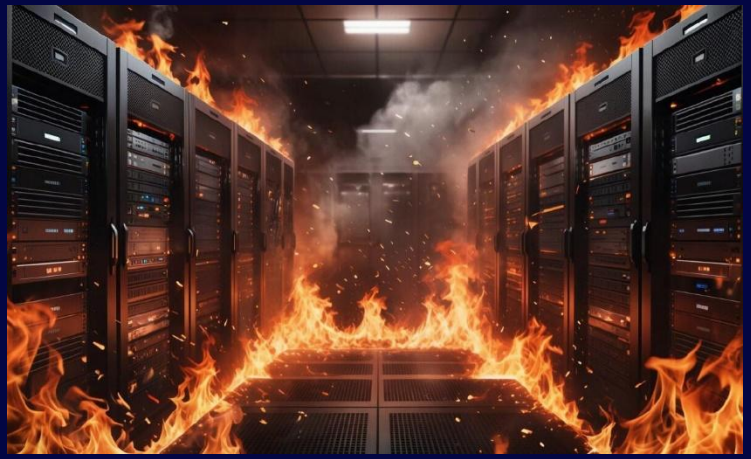
Всего были приостановлены 647 государственных сервисов, из них 96 уничтожены полностью.

Сгорели:

- Местные госуслуги;
- Система удостоверения личности;
- Государственное облако хранения документов — миллионы записей утеряны безвозвратно;
- Государственная почта;
- Образовательные базы университетов;
- Финансовые и административные сервисы.

https://www.fondsk.ru/news/2025/10/09/kto-spalil-cifrovoy-suverenitet-yuzhnoy-korei.html

В Южной Корее остановилась работа всей цифровой инфраструктуры



После пожара в дата-центре остановилась работа практически всей государственной цифровой инфраструктуры.

858 терабайт данных **сгорели вместе с резервными копиями — они хранились на сервере в соседней комнате.**

Один из высокопоставленных чиновников, отвечавших за восстановление систем, покончил с собой (https://www.yna.co.kr/view/AKR20251003046900001: «…умер от напряжения…»).

Рекомендации

Использовать стандартизированные подходы и технологии

7.2.2 Помещения

Системы восстановления ИКТ и критические данные, по возможности, должны быть физически отделены от рабочей площадки, **чтобы предотвратить влияние на них одного и того же инцидента**.

ГОСТ Р ИСО/МЭК 27031-2012 Информационная технология. Методы и средства обеспечения безопасности. Руководство по готовности информационно-коммуникационных технологий к обеспечению непрерывности бизнеса (ISO/IEC 27031:2011, IDT)

Использовать стандартизированные подходы и технологии

infotecs

7.2.3 Технология

Должны быть реализованы технологические стратегии ИКТ. К ним можно отнести один или несколько из следующих механизмов реализации:

a) **горячий резерв**, когда инфраструктура ИКТ дублируется на двух площадках;

b) **теплый резерв**, когда восстановление происходит на дополнительной площадке с частично подготовленной инфраструктурой ИКТ;

c) **холодный резерв**, когда инфраструктура создается или конфигурируется с нуля на альтернативной площадке;

d) **механизмы поставки/аутсорсинг**, в соответствии с которыми внешние поставщики услуг предоставляют аппаратные средства и иные ИТ мощности; и

e) **составной механизм** предыдущих стратегий: подход "выбери и смешай".

ГОСТ Р ИСО/МЭК 27031-2012 Информационная технология. Методы и средства обеспечения безопасности. Руководство по готовности информационно-коммуникационных технологий к обеспечению непрерывности бизнеса (ISO/IEC 27031:2011, IDT)

Выводы

Что следует иметь ввиду?

Помнить, что при использовании в деятельности Компани средств информатизации следует понять: **это арендуемые мощности или собственные**?

Если это собственные модности, то с возведением оснвной площадки создание производства не заканчивается, **следует озаботиться резервными мощностями и площадками**

Пренебрежение этим может привести **к катастрофе** (а может пронесёт? ☺)

Подписывайтесь
на наши соцсети,
там много интересного

infotecs

infotecs

Спасибо за внимание!