

Достаточно ли каски и бронежилета?! Неочевидные угрозы.

10.11.2022

Profit
Security Day

The logo for Linkmaster Kazakhstan. It features the word "Link" in a large, white, sans-serif font. The letter "i" in "Link" is stylized with a red and white striped pattern. To the right of "Link" is the word "master" in a smaller, white, sans-serif font, followed by a registered trademark symbol (®). Below "master" is the word "Kazakhstan" in a red, sans-serif font.

История

2007	Дистрибьютор Fluke Networks в Казахстане
2009	Дистрибьютор продукции FNET, Fluke IG, FCAL на территории стран Средней Азии и Кавказа
2011	Авторизованный сервисный центр Fluke
2014	Аккредитация поверочной лаборатории ISO 17025
2017	Открыт филиал в Узбекистане
2021	Аккредитация калибровочной лаборатории ISO 17025
2022	Дистрибьютор/Партнер 50+ производителей – мировых лидеров отрасли

Структура

Структура группы



- Продажа оборудования
- Аренда оборудования
- Обучение



- Метрологическая лаборатория
- Сервисный центр
- Авторизованный сервисный центр
Fluke, Furukawa

Миссия

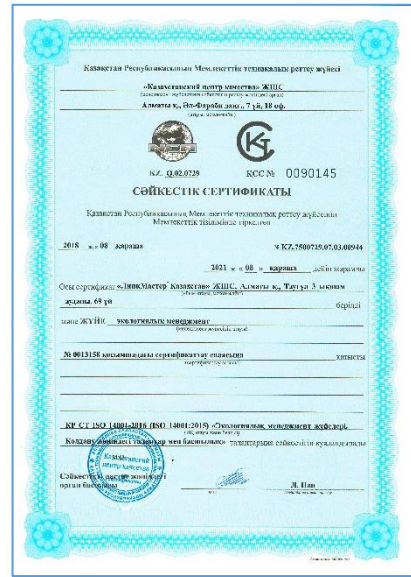
Мы осуществляем поставки со склада и под заказ клиентам в странах Средней Азии и Кавказа монтажного, тестового, измерительного оборудования и программных продуктов, комплексов для научно-исследовательской деятельности, разработки, метрологического обеспечения, испытаний и безопасности в области энергетики, микро-/радиоэлектроники, телекоммуникаций и информационных технологий, IP-телефонии от мировых лидеров, а также осуществляем поверку, калибровку, ремонт всего спектра поставляемого оборудования и проводим обучение работе на нем.

Сертификаты

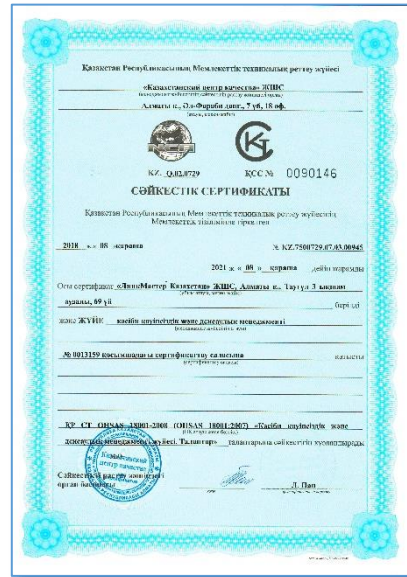
ISO 9001-2015



ISO 14001-2015



ISO 45001-2018



ISO 27001-2015



ISO 17025



Заказчики

- Правительственные организации
- Учреждения образования
- Научно-исследовательские организации
- Аэрокосмические организации
- Нефтегазовые предприятия
- Предприятия легкой и тяжелой промышленности
- Сервисные компании
- Медицинские компании
- Финансовые компании
- Военные структуры
- Телекоммуникационные компании
- Подрядные организации

Производители*



* Основные производители, представляемые ЛинкМастер Казахстан

Достаточно ли каски и бронежилета?!

- Программно-аппаратная ИБ
- Контроль физического доступа
- Резервирование каналов связи
- Резервирование оборудования
- Климатконтроль
- Электропитание
- Укрепление здания
- ???????



Классификация датацентров по стандарту TIA-942

TIER 1

- **Малый бизнес**
- Среднее время работы 99,671 %
- Простой не более 28,8 часа в год
- Без резервирования

TIER 2

- **Средний бизнес**
- Среднее время работы 99,749 %
- Простой не более 22 часов в год
- Резервные источники питания и охлаждения

TIER 3

- **Крупный бизнес**
- Среднее время работы 99,982 %
- Простой не более 1,6 часа в год
- Резервный источник питания на 72 часа работы
- Инженерные системы зарезервированы однократно

TIER 4

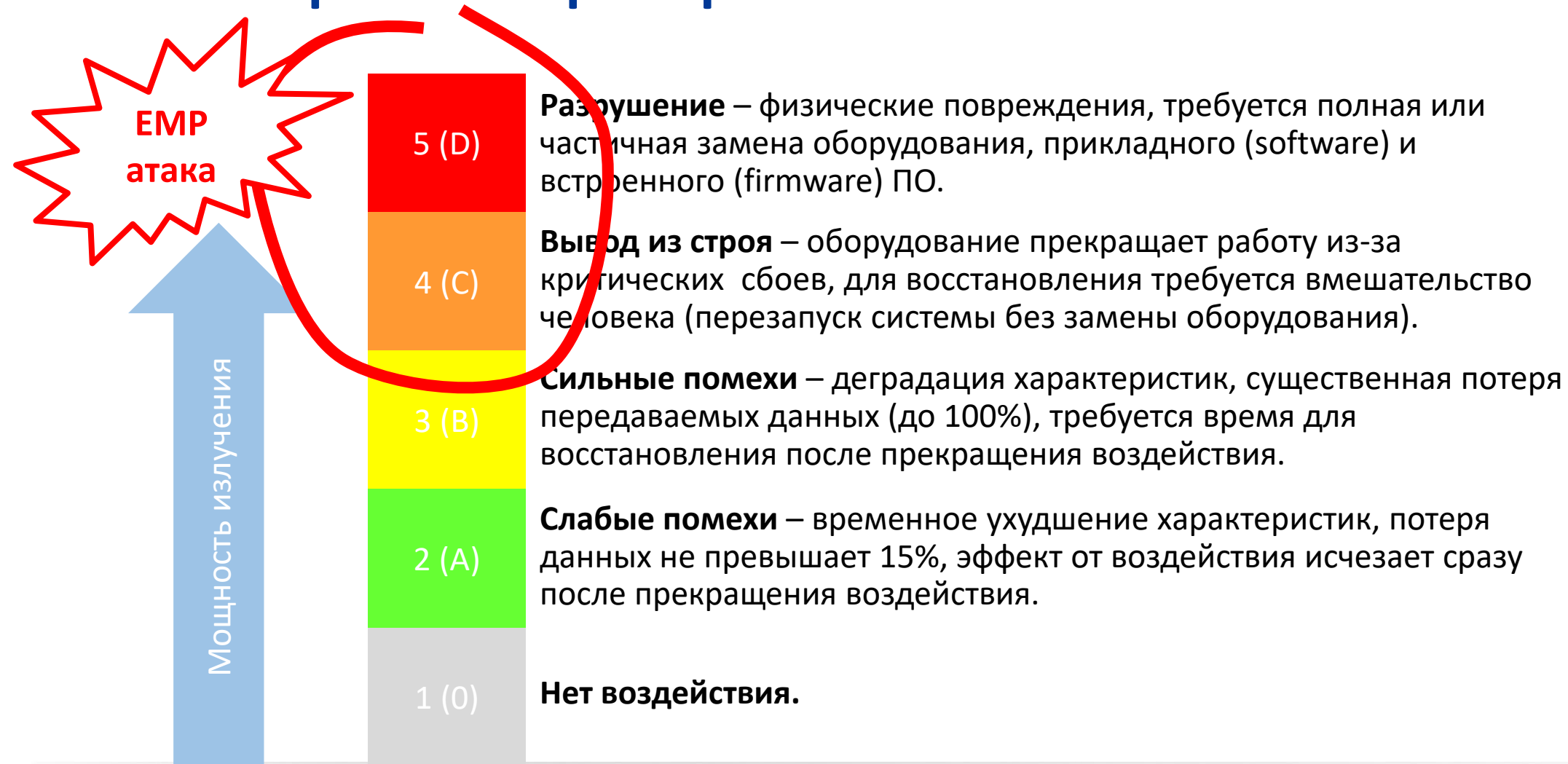
- **Корпорации**
- Среднее время работы 99,995 %
- Простой не более 26 минут в год
- Резервные источники питания на 96 часов
- Инженерные системы зарезервированы двукратно



В настоящее время большинство ЦОДов хорошо защищены от природных катастроф и отказов оборудования, но не от электромагнитных импульсов (**ЕМР-атак**).

Успешно проведенная ЕМР-атака может полностью уничтожить все электронное оборудование (сервера, активное сетевое оборудование), ПО и данные.

Классификация воздействия ВЧ ЭМ излучения на электронные приборы



XXI век: электромагнитное неядерное оружие (США)



Проект «CHAMP», до 100 ЭМ выстрелов за один вылет

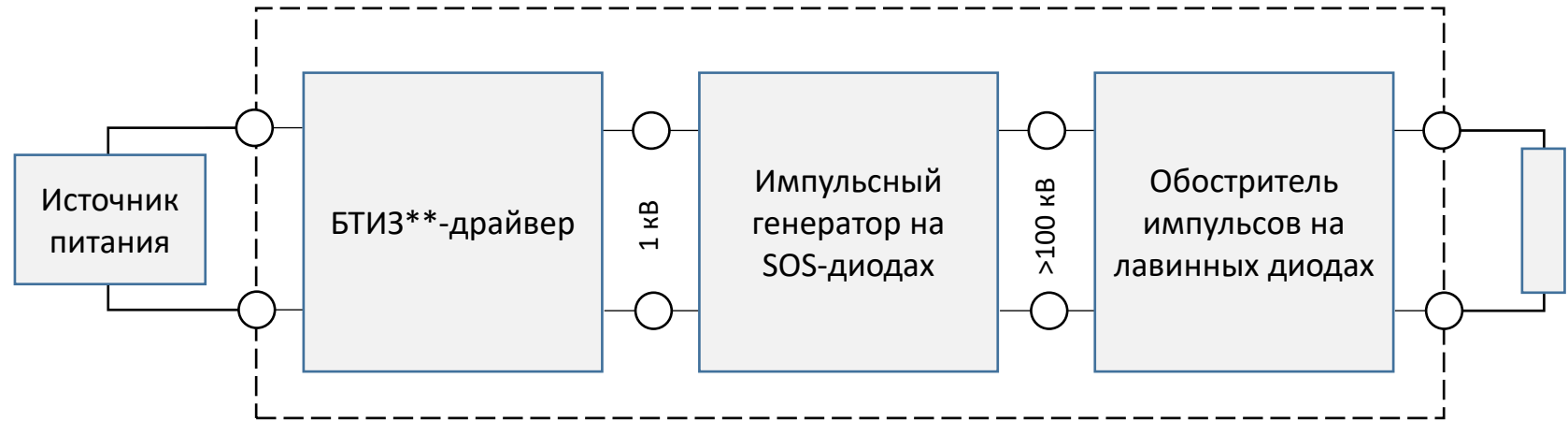
- По сведениям военных экспертов ЭМ оружие могло быть использовано США во время войны в Ираке в 2003 году для поражения радиолокационной защиты авиабаз.
- В 2009 году компания Boeing получила контракт на разработку проекта CHAMP (Counter-electronics High-powered microwave Advanced Missile).
- В 2011 году впервые были проведены успешные испытания БПЛА на базе лаборатории the U.S. Air Force Research Laboratory (AFRL) в штате Юта.
- В 2020 году МО США приняло комплексы на вооружение.

В мирное время угрозы нет?

Точечные EMP-атаки: схемы и компоненты в свободном доступе*



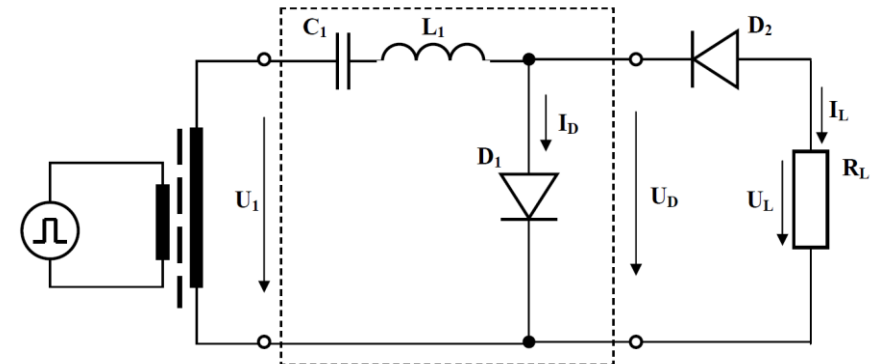
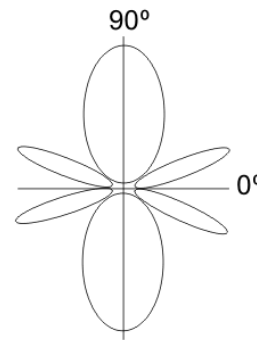
Диодная сборка SOS-180-12
(180 кВ / 12 кА / 600 г / ~ \$400)



300 кВ / диско-конусная антенна



150 кВ / антенна «Бабочка»



* – реализация требует специальных знаний и навыков, требуется точное согласование элементов; ** – биполярный транзистор с изолированным затвором

Уязвимая, критически важная инфраструктура



Объекты, подверженные действию ЭМ импульсов

- **Энергетика**
 - генерирующие предприятия, передающие и распределительные сети
- **Нефтяная промышленность**
 - добывающие, транспортные и перерабатывающие предприятия
- **Телекоммуникационная отрасль**
 - системы проводной и беспроводной связи, датацентры
- **Производственные предприятия**
 - оборудование предприятий легкой и тяжелой промышленности
- **Медицинские учреждения**
- **Транспорт**
 - самолеты, наземное навигационное оборудование, корабли, поезда, метрополитены, автотранспорт с электронным зажиганием
- **Финансовые институты**
 - банки, страховые компании, процессинговые центры
- **Силовые ведомства**
 - вооружение и специальная техника МВД и МО



Атаки с использованием электромагнитных импульсов

Напряженность электрического поля, В/м



Цели EMP-атаки:

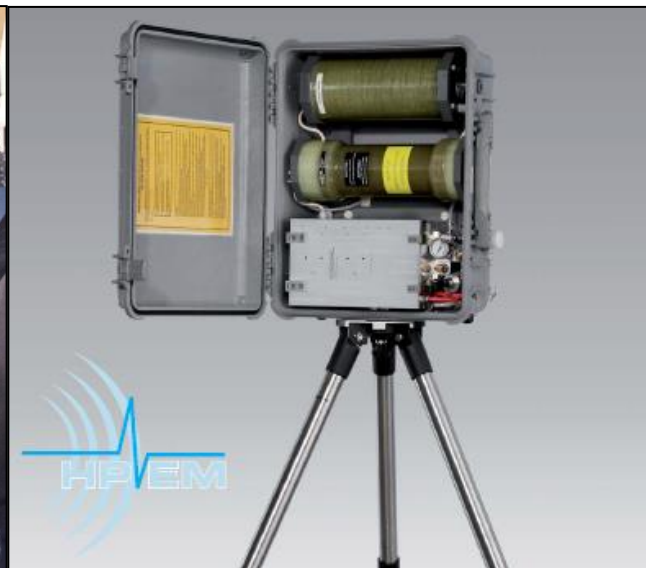
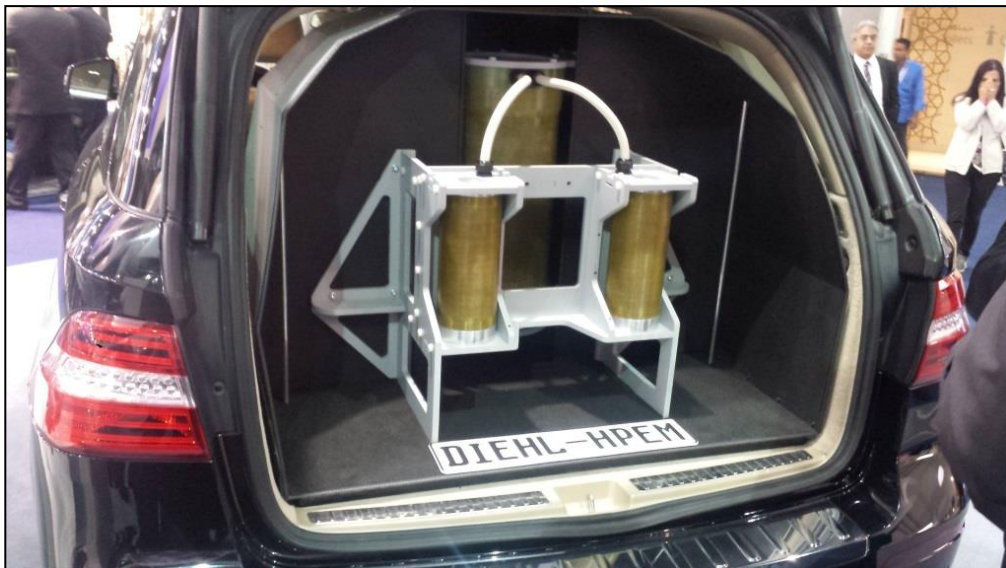
- Временное отключение работающей электронной системы
- Вывод электронной системы из строя (полное или частичное разрушение схем)
- Уничтожение хранимых данных
- Нарушение работы отдельных элементов электронной системы (нарушение целостности системы)

Ущерб:

- Увеличение времени простоя оборудования
- Потеря критически важных данных
- Появление брешей в безопасности
- Дополнительные затраты на диагностику и ремонт оборудования

IEMI – Intentional Electromagnetic Interference
HEMP – High Altitude Electromagnetic Pulse
EMP – Electromagnetic pulse

Источники ЭМ импульсов



IEMI-генераторы имеют различные конструкции и размеры: грузовик, минивен, рюкзак, портфель.

В интернете доступны компоненты и схемы IEMI-генераторов*, которые могут использовать террористы и криминалитет.

Стоимость готовых IEMI-генераторов начинается от нескольких тысяч долларов США, наносимый ущерб исчисляется сотнями тысяч и даже миллионами долларов США.

* – пазотроны, магнетроны, *tilo*-структуры, клистроны, супер-релтроны, гиротроны, гироклистроны, *sos*-диоды.

Реакция правительства США на потенциальную угрозу



В 2015 году разработан и утвержден Конгрессом США «Critical Infrastructure Protection Act» (CIPA). Внесены поправки в другие законодательные акты, связанные с национальной безопасностью, энергетикой и космическими программами США.



С 1990 года развивается стандарт MIL-STD-188-125 «Защита наземных сооружений, имеющих критически важное значение в телекоммуникационных целях».



ETS-Lindgren – единственная компания, которая предлагает решения для защиты от EMP-атак, протестированные и сертифицированные по стандарту MIL-STD-188-125 на базе Little Mountain Test Facility (лаборатория на военной базе ВВС США в штате Юта, управляемая компанией Боинг).



An **ESCO Technologies** Company

- Инновационные разработки для детектирования, измерения и управления электромагнитной, магнитной и акустической энергией с 1932 года (Ray Proof)
- Штаб квартира в Сиде Парк, штат Техас в США (Cedar Park, Texas, USA)
- Офисы, центры разработки и производства в Финляндии, Франции, Германии, Великобритании, ОАЭ, Бразилии, Китае, Индии, Японии, Сингапуре и Тайване
- Более 10 тысяч реализованных проектов, в том числе для Intel, Boeing, национальных университетов и министерств обороны ряда государств



An **ESCO Technologies** Company

Уровень защиты 1

- Защита оборудования от повреждения

Среда, защищенная от EMP:

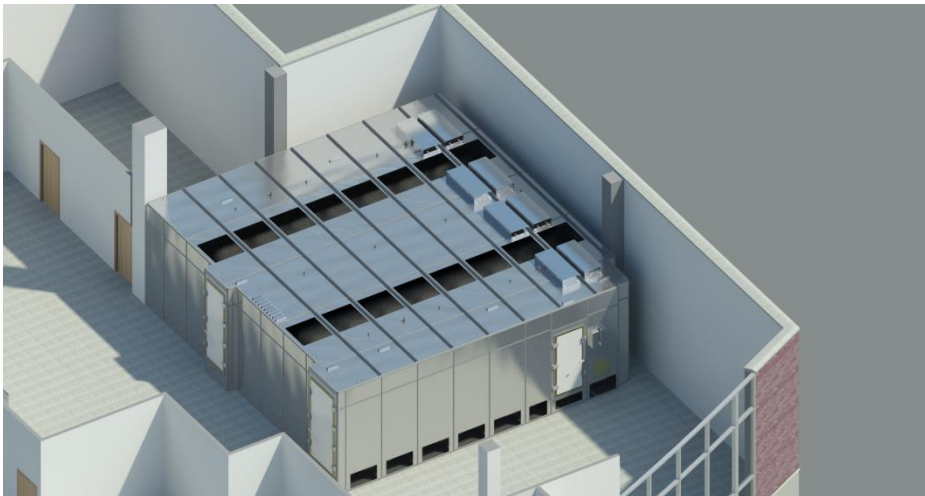
- ЭМ изоляция пространства
- ЭМ защита точек входа
- Системы питания, охлаждения и другие вспомогательные системы находятся вне защищаемого периметра. После их восстановления возможен незамедлительный запуск датацентра.

Уровень защиты 2

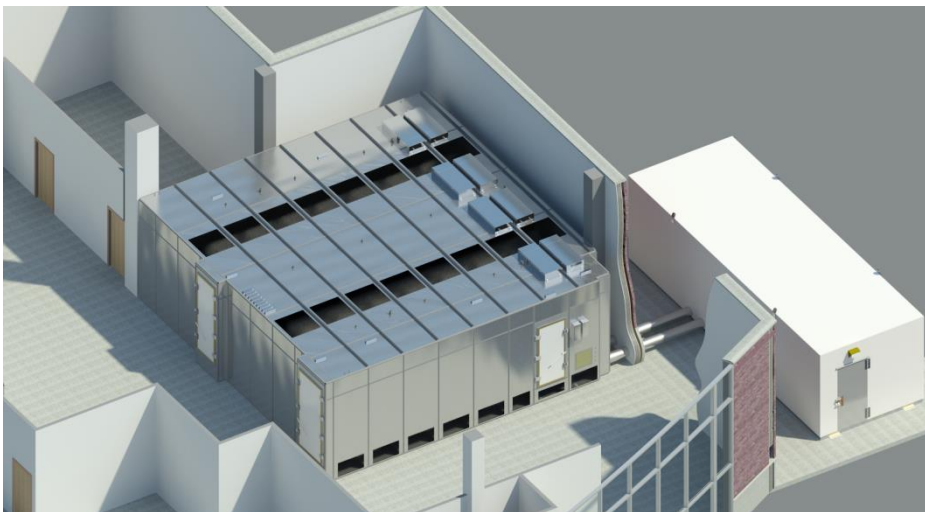
- Защита оборудования от повреждения
- Продолжение бесперебойной работы оборудования

Независимая защищенная инженерная система:

- В случае проведения EMP-атаки все оборудование датацентра продолжает непрерывную бесперебойную работу, используя защищенные инженерные системы.



Red Edge™
PROTECTION LEVEL 1
(«Выживание»)



Red Edge™
PROTECTION LEVEL 2
(«Выживание и работа»)



RedEdge™ Экранирование



- Сварные экранированные комнаты
- Модульные двухслойные панельные сборные конструкции



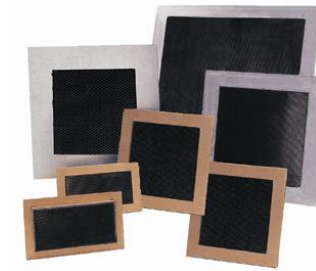
- Любые размеры и конфигурации
- Возможно финишное (эстетическое) оформление интерьера и экстерьера по выбору заказчика
- Долговечные износостойкие двери
- Гальванизированная оцинкованная или нержавеющая сталь

RedEdge™ Фильтры



- ЕМР/НЕМР фильтры для подачи электроэнергии в защищаемый периметр
- Гарантированная многоуровневая защита от перенапряжения, ЭМ импульсов и ВЧ/СВЧ помех
- Готовые решения для однофазных и трехфазных систем
- Передача чистой электроэнергии различных стандартов (до 480 В и 400 А)

RedEdge™ Точки входа



Защищенные входы для подачи/передачи:

- воздуха
- воды
- противопожарных составов
- ВЧ/СВЧ сигналов
- данных по оптическим и медным линиям связи/передачи данных



Оценка затрат на защиту от ЕМР-атак

- Усиление устойчивости к ЕМР-атакам военных и коммерческих систем, включая защиту вычислительной техники и коммуникационного оборудования, в среднем добавляет от 3 до 10% к общей стоимости при включении элементов защиты в исходный проект.
- Модернизация уже существующих военных или коммерческих систем в среднем добавляет к общей стоимости системы более 10%.
- Усиление устойчивости к ЕМР-атакам проще и экономически более эффективно при учете на ранних этапах проектирования, чем при модернизации существующих систем!

Примеры реализации проектов



Контакты

Республика Казахстан,
050035, г. Алматы,
мкр. Мамыр-4, дом 117/6

www.linkmaster.kz

www.metrolab.kz

тел.: +7(727)390-18-70,
эл. почта: info@linkmaster.kz