Секция «Таможенное дело»

История развития Дата-центров. Их назначение, структура и классификация. Местонахождения самых крупных мировых Дата-центров

Аханов Я.О.
Научный руководитель: Ковалькова И.А.
Белорусский национальный технический университет

*Дата-центр*или же *центр обработки данных*– это специализированная площадка, где размещены сервера и прочее системное оборудование [3]. К основным услугам, которые оказывают Дата-центры относятся передача большого количества данных, их хранение и обработка. Дополнительно они могут предоставлять облачные решения, удалённые рабочие места и услуги резервного копирования. Обычно Дата-центры располагаются вблизи станций операторов мобильных сетей. В основном Дата-центры используются компаниями, которые в свою очередь предоставляют свои услуги населению, благодаря чему осуществляется доступ к сети интернет, с возможностью обмениваться данными, хранить данные в облаке и т.д.

История развития Дата-центровберёт своё начало ещё с рассвета компьютерной индустрии. Компьютерные системы того времени были достаточно сложными и нуждались вспециальных условиях для работы. Из-за того, что они требовали большого количества места и проводов для подключения разных компонентов, в таких комнатах начали активно использоваться серверные стойки, кабельные каналы и фальшполы. Эти системы требовали непрерывного охлаждения. Безопасность также была важным показателем, потому что оборудование стоило дорого и зачастую использовалось в военных целях. Поэтому были разработаны основные принципы доступа всерверные.

1980-е компьютеры начинают использовать повсеместно, при этом мало кто думал о требованиях по эксплуатации. Но с развитием ИТ-отрасли компании начинают тщательнее контролировать ИТ-ресурсы. Внедрениеархитектуры «клиент-сервер»вмикрокомпьютеры 1990-ых, называемые сегоднясерверами, переместилоих в старые серверные. Доступность дешёвого сетевого оборудования и новые стандарты сетевых кабелей дали возможность использоватьиерархическое проектирование и таким образом серверы были перемещены в другие комнаты.

Пик расцвета Дата-центров пришёлся на 1995-2000 года. Компании нуждались в устойчивом и высокоскоростном Интернете и бесперебойной работе оборудования, для разворачивания систем и установки своего

присутствия в сети. Размещение оборудования, которое было способно справиться с решением этих задач,для небольших компаний было невозможным. Тогда начинали строиться помещения, которые могли бы обеспечить бизнес необходимыми решениями для размещения компьютерных систем и их эксплуатации[3].

Структура.

Обычно, Дата-центры состоят из следующих видов инфраструктуры: *инженерной, телекоммуникационной, информационной.*

Информационная инфраструктура отвечает за хранение и обработку информации, включая в себя всё оборудование, необходимое для функционирования Дата-центра.

Телекоммуникационная инфраструктура отвечает за связь составляющих Дата-центра, а также за данные, которые получают пользователи от центра.

инженерную инфраструктуру входят источники электричества, способные работать при отключении центральных, а также системы поддержания необходимых уровня влажности и температуры, пожаротушения, управления питанием, контроля доступа. Дополнительно могут предлагаться услуги по защите от всевозможных атак.

Основное оборудование обычно закреплено в шкафах и стойках.

Классификация.

Дата-центры могут классифицироваться *по размеру*, *предназначению* и *надёжности*, которая является самым главным показателем работы. Согласно стандарту TIA-942 существует всего четыре уровня надёжности Дата-центров: базовый, с резервными компонентами, с возможностью параллельного проведения ремонтных работ, отказоустойчивый.

Tier 1. Базовый уровень– отказы оборудования или ремонтные работы приостанавливают работы всего центра, в Дата-центренет фальшполов, резервных источниковэлектричества и источников бесперебойного питания, защита от атак не предусмотрена.

Tier 2. С резервными компонентами –в наличии небольшой уровень резервирования, в центре присутствуют резервные источники электричества, но ремонтные работы приостанавливают деятельность Дата-центра;

Tier 3.С возможностью параллельного проведения ремонтных работ– во время ремонтных работ деятельность центра, благодаря наличию резервирования, не останавливается.

Tier 4. Отказоустойчивые– любые работы проводятся без остановки Дата-центра.Дата-центры этого уровня защищены от всех потенциальных угроз со стороны человека.Помимо этого предусмотрена защита от пожаров иштормов[2].

Любая современная крупная компания имеет свойДата-центр, однако одни из крупнейших и наиболее интересно устроенных Дата-центровпринадлежат компаниям Google, Apple и Ebay.

Google – всемирноизвестная компания, владеющая множествомДата-центров, среди которых выделяется центр расположенный на берегу Балтийского моря финского города Хамины. Часть всех серверов располагается в здании бывшей бумажной фабрики. На покупку зданий для этого центра компания потратила около 350 миллионов долларов. Для охлаждения оборудования и поддержания нужного уровня влажности центр использует воду Финского залива, поэтому и понадобилось здание бывшей фабрики [1].

Как и любая другаякомпания,*Apple* старается уменьшить издержки, снижая расходы электричества при этом, минимизируя вред, наносимый окружающей среде. На протяжении 7 лет абсолютно все их Дата-центры и практически все офисы работают на возобновляемых источниках электричества. Вокруг Дата-центра в Мейдене размещены солнечные плиты, которые занимают площадь около 400 000 квадратных метров, вырабатывающие около 40 миллиона киловатт-часов в год. Такого количества энергии хватает для обеспечения более чем половины серверов прочего оборудования, оставшуюся энергию производит станция, расположенная неподалёку [1].

Дата-центр компании *Ebay*расположен в Аризоне. Дата-центры из-за своей деятельности требуют надёжных систем терморегулирования для охлаждения, здесь же особенность в том, что центр расположен в одном из самых жарких мест США. Серверам для нормальной работы требуется температура 18-25 градусов по Цельсию, однако этот Дата-центр работает при температуре +45. Таких результатов удалось добиться благодаря внедрению инновационной технологии[1].

Подводя итог, хочется отметить, что Дата-центры – это полезное изобретение, позволяющее хранить сервера и громадные объёмы данных намного дешевлеи не беспокоиться об их безопасности. Создание Дата-центров является большим скачком в сфере IT-технологий, делая огромный вклад в наше общее будущее.

Литература

栀 Ā Ā ÀĀ ᵣĀ □ Ā □ де хранится интернет: 10 супермощных Дата-центров. Режим доступа: http://www.lookatme.ru/mag/live/inspiration-lists/204915-data-centres.

栀 Ā Ā ÀĀ ᵣĀ □ Ā □ адёжность инженерных систем ЦОД. Режим доступа:http://cons-systems.ru/inzhenernye-sistemy-tcod.

Дата-центр. Режим доступа:https://wiki2.org/ru/Дата-центр.

Основные факторы, влияющие на обеспечение информационной безопасности таможенных органов. Основные угрозы информационной безопасности таможенных органов

Данилова М.С.
Научный руководитель: Ковалькова И.А
Белорусский национальный технический университет

Защита информации – это деятельность по предотвращению утечки защищаемой информации, несанкционированного и непреднамеренного воздействий на защищаемую информацию.

Информационная безопасность – защищённость информации от незаконного ознакомления, преобразования, уничтожения, а также защищённость информации от воздействий, направленных на нарушение их работоспособности.

Безопасная информационная система – это система, которая:

защищает данные от несанкционированного доступа;

всегда готова предоставить данные своим пользователям;

надёжно хранит информацию и гарантирует неизменность данных.

Сущность обеспечения информационной безопасности таможенных органов отражена в «Основных направлениях развития таможенной службы Республики Беларусь», утверждённых приказом председателя Государственного Таможенного комитета от 08.04.2011 № 125-ОД.

Обеспечение информационной безопасности – проведение единой политики в области охраны и защиты информационных ресурсов и информации, система мер организационного, технического и иного характера, адекватных угрозам информационным ресурсам таможенных органов, техническим и программным средствам информационных технологий и, как следствие, интересам таможенных органов в целом[3].

Однако возникают факторы, которые необходимо учитывать при анализе реального состояния информационной безопасности и выявления ключевых проблем в этой области.

К таким факторам можно отнести:

ослабление контроля со стороны руководителей таможенных органов и их структурных подразделений за состоянием информационной безопасности, выполнением подчинёнными должностными лицами регламентов, должностных инструкций, нормативно-правовых актов;