

Отказоустойчивость: **Disaster recovery**



Александр
Зубарев



Александр Зубарев

Председатель цикловой комиссии “Информационной
безопасности инфокоммуникационных систем”

АКТ (ф) СПбГУТ



[Александр Зубарев](#)



Вспомним материал прошлой лекции

Вопрос: Какие главные отличия в фичах между Open Source версиями Nginx и HAProxy?

Вспомним материал прошлой лекции

Вопрос: Какие главные отличия в фичах между Open Source версиями Nginx и HAProxy?

Ответ:

В **HAProxy** есть:

- встроенная поддержка активных проверок живости бекендов;
- есть статистика, с него можно собирать метрики более нативно, чем с `nginx`;
- у него есть встроенная поддержка работы с базами данных.

В **nginx** есть:

- возможность писать кастомные модули и код на `lua`.

Предисловие


Сегодня мы поговорим о Disaster recovery.

Рассмотрим:

- Типы аварийного восстановления;
- Процессы планирования аварийного восстановления;
- Анализ воздействия на бизнес;
- Анализ рисков;
- Допустимое время восстановления;
- Допустимая точка восстановления (допустимые потери данных).

План занятия

1. [Типы аварийного восстановления](#)
2. [План восстановления](#)
3. [Решение для восстановления в случае DR](#)
 - a. [Drass](#)
 - b. [Baas](#)
4. [BIA](#)
5. [Анализ рисков](#)
6. [RPO](#)
7. [RTO](#)
8. [Итоги](#)
9. [Домашнее задание](#)



Типы аварийного восстановления



Аварийное восстановление

Аварийное восстановление (Disaster recovery) — восстановление ИТ-инфраструктуры и доступа к ней после стихийного бедствия или сбоя, возникшего по вине человека, например после кибератаки или отказа оборудования.

Частью плана аварийного восстановления могут быть самые разные методы. Аварийное восстановление — это один из аспектов непрерывности бизнеса.

Типы аварийного восстановления

- Резервное копирование;
- «Горячая» резервная площадка;
- «Холодная» резервная площадка;
- Аварийное восстановление ЦОД;
- Аварийное восстановление как услуга (DRaaS);
- Копии на определенный момент времени;
- Мгновенное восстановление;
- Виртуализация.

Типы аварийного восстановления

- **Резервное копирование** — самый простой тип аварийного восстановления, который подразумевает хранение данных в другом расположении или на удаленном накопителе.

Однако одно резервное копирование обеспечивает лишь минимальную защиту непрерывности бизнеса, поскольку нельзя сделать резервную копию самой ИТ-инфраструктуры.



Типы аварийного восстановления

- **«Горячая» резервная площадка** — постоянная поддержка наличия актуальных копий данных.

Этот метод более трудоемкий и дорогой, чем предыдущий, но значительно сокращает время простоев.

Типы аварийного восстановления

- **«Холодная» резервная площадка.** Этот тип аварийного восстановления подразумевает, что организация устанавливает базовую инфраструктуру на другом, редко используемом объекте, где сотрудники смогут работать после стихийного бедствия или пожара.

Это способствует поддержанию непрерывности бизнеса, поскольку работа продолжается.

Однако такой подход не обеспечивает защиту или восстановление важных данных, поэтому его необходимо совмещать с другими типами аварийного восстановления.

Типы аварийного восстановления

- **Аварийное восстановление ЦОД.** Физические элементы ЦОД могут обеспечить защиту данных и способствовать ускоренному аварийному восстановлению при некоторых типах аварий.

Например, средства пожаротушения помогут защитить данные и компьютерную технику при пожаре. Резервный источник питания поможет компаниям справиться с перебоями в электроснабжении без перерывов в работе.

К сожалению, ни одно из этих физических средств аварийного восстановления не поможет при кибератаке.



Типы аварийного восстановления

- **Аварийное восстановление как услуга (DRaaS).** В случае аварии или кибератаки поставщик услуги DRaaS перемещает вычислительные процессы организации в собственную облачную инфраструктуру.

Это позволяет компании бесперебойно продолжать работу из расположения поставщика, даже если ее серверы отключены.

Типы аварийного восстановления

- **Копии на определенный момент времени.** Такие копии, также известные как моментальные снимки, позволяют делать копию всей базы данных в указанный момент времени.

Данные можно восстановить из этой резервной копии, но только, если она хранится во внешней среде или на ВМ, не поврежденной при аварии.



Типы аварийного восстановления

- **Мгновенное восстановление.** Этот метод аналогичен копированию на определенный момент времени, однако при мгновенном восстановлении вместо копирования базы данных делается снимок всей ВМ.

Типы аварийного восстановления

- **Виртуализация.** Организации могут делать резервные копии некоторых процессов и данных или даже создавать рабочие реплики целых вычислительных сред на внешних ВМ, которые не будут затронуты при физических авариях.

Использование виртуализации в рамках плана аварийного восстановления также позволяет компаниям автоматизировать часть соответствующих процессов и ускорить восстановление.



План восстановления



План аварийного восстановления

Наличие плана на случай аварии обеспечивает два основных преимущества:

Сокращение расходов. Планирование на случай аварии позволяет компании сэкономить, а это может быть решающим фактором, который поможет избежать банкротства при стихийном бедствии.

Ускоренное восстановление. В зависимости от стратегии аварийного восстановления и используемых средств компании могут быстрее вернуться к работе после аварии или даже продолжить работу без прерываний. Организации, не имеющие стратегии и плана аварийного восстановления, могут разориться.



План аварийного восстановления

Параметры Disaster Recovery (DR) :

Принцип работы — непрерывная репликация ИТ-инфраструктуры на резервную площадку в режиме реального времени.

Процесс восстановления — переключение на резервную площадку в случае аварии.

Необходимые ресурсы — резервная площадка (резервный ЦОД или облако).

Роль в отказоустойчивости — ключевой инструмент обеспечения отказоустойчивости и непрерывности бизнеса —
Работоспособная копия ИТ-инфраструктуры.



Решение для восстановления в случае DR

Решения для восстановления

Рассмотрим решения для восстановления в случае ЧС:

- DRaaS (Disaster-Recovery-as-a-Service);
- BaaS (Backup as a Service);
- Active-Active (растянутый кластер на основе HA).



DRaaS

Аварийное восстановление как услуга (DRaaS)

DRaaS (Disaster-Recovery-as-a-Service) — услуга облачного резервного копирования и восстановления.

- Поддержка кластеров любого размера;
- Поддержка и кворумных и ресурсозависимых кластеров;
- Поддержка практически любой избыточной конфигурации;
- Автоматическая репликация конфига на все узлы кластера;
- Возможность задания порядка запуска ресурсов, а также их совместимости на одном узле;
- ...

Аварийное восстановление как услуга (DRaaS)

- Поддержка расширенных типов ресурсов: клонов (запущен на множестве узлов) и с дополнительными состояниями (master/slave и т.п.);
- Единый кластерный шелл (crm), унифицированный, скриптуемый.

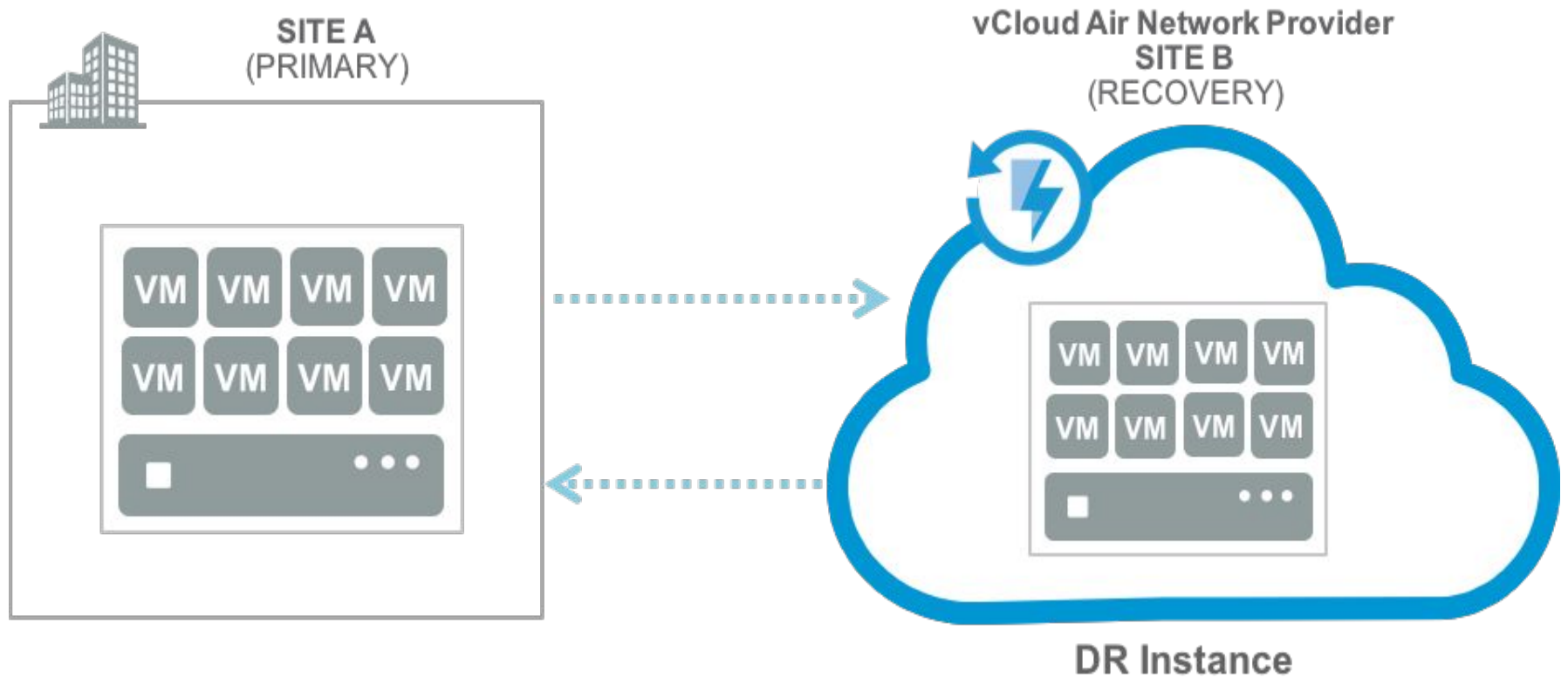
Пример использования:

[VMware vCloud Availability](#)

[VMware vCloud Director](#)

[VMware vCloud Air Network](#)

DRaaS



ИСТОЧНИК

Аварийное восстановление как услуга (DRaaS)

Важные параметры работы системы аварийного восстановления:

- **Частота копирования** — репликация данных происходит в режиме реального времени. От данного параметра зависит стоимость решения.
- **Актуальные и дискретные данные (RPO)** — оперативный замер времени состояния данных, которые фиксируются в последний момент работы системы.
- **Скорость восстановления (RTO)** — Время за которое можно будет уже выполнить восстановление системы после сбоя.
-

Аварийное восстановление как услуга (DRaaS)

- **Гибкость настройки** — режим восстановления — может восстанавливать как всю инфраструктуру, так и отдельный сервер, отдельную программу на сервере или конфигурацию.
- **Автоматизированность** — репликация происходит или в заданный промежуток времени или синхронно
- **Отказоустойчивость** — зависит от сервиса, но как правило всевозможные технологии высокой доступности.

Результат: Резервирование всего сервиса на горячую.

(DRaaS)

Другие представители DRaaS на рынке:

- [Acronis](#)
- [Veeam](#)
- [CommVaul](#)
- [Microsoft](#)
- [zertot](#)
- [Cisco](#)
- и др.



BaaS



Резервное копирование как услуга (BaaS)

ВaaS подразумевает предоставление пользователю надежного облачного сервиса для создания резервных копий инфраструктуры.

ВaaS позволяет защищать информацию от потери при сбоях в работе оборудования.

Используется ВaaS в локальных, удаленных и гибридных средах, которые нуждаются в отказоустойчивой системе защиты информации в определенном информационном активе организации.

Резервное копирование как услуга (BaaS)

Важные параметры работы системы копирования как услуги:

- **Частота копирования** — копирование проводится по расписанию (например раз в неделю).
- **Актуальные и дискретные данные (RPO)** — восстановление может быть из любой копии, но число копий ограничено и в принципе последняя копия может быть неактуальна.
- **Скорость восстановления (RTO)** — время восстановления данных может быть пару дней, неделю, месяц или дольше в зависимости от объема данных.
- ...

Резервное копирование как услуга (BaaS)

- **Гибкость настройки** — ограничено производителем программного обеспечения, например, частотой выполнения, объемом данных.
- **Автоматизированность** — как правило, запускают в ночное время, тк создает дополнительную нагрузку на сервер.
- **Отказоустойчивость** — не обеспечивает резервирование всей инфраструктуры, только программного обеспечения

Результат: Копия данных.

(BaaS)

Другие представители BaaS на рынке:

- [De Novo](#)
- [Veeam](#)
- [DEAC](#)
- и др.



BIA (Business Impact Analysis)



Оценка воздействия на бизнес

BIA (оценка воздействия на бизнес) — метод, который позволяет исследовать, как ключевые виды отказов, нарушений, разрушений могут повлиять на ключевые виды деятельности и процессы организации, а также идентифицировать и количественно определить необходимые возможности для управления организацией в этих условиях.

Оценка воздействия на бизнес

Процесс метода ВИА обеспечивает согласование и понимание:

- идентификации и критичности ключевых бизнес-процессов, функций, связанных ресурсов и ключевых взаимосвязей, существующих в организации;
- влияния отказов/нарушений/разрушений на возможности организации достигать установленных критических целей бизнеса;
- необходимых возможностей управления воздействием отказов/нарушений/разрушений и восстановлением нормального хода деятельности организации.

Оценка воздействия на бизнес

Метод BIA используют при определении:

- критичности процессов организации;
- времени их восстановления (RTO – Recovery Time Objective);
- необходимых ресурсов (активы, персонал, навыки, технологии, производственные площади и информация).

Оценка воздействия на бизнес

ВИА входные данные для выполнения оценки воздействия на бизнес:

- группа анализа и разработки плана непрерывности бизнеса;
- информация о целях, окружающей среде, видах деятельности и взаимосвязях организации;
- подробное описание видов деятельности и функционирования организации, включающих процессы, вспомогательные ресурсы, взаимосвязи с другими организациями, соглашения об аутсорсинге, причастные стороны;
- ...

Оценка воздействия на бизнес

- ...
- экономические и производственные последствия, вызванные нарушением критических процессов;
- подготовленные анкеты;
- список опрашиваемых лиц в соответствующих областях деятельности организации и/или причастных сторон.

Оценка воздействия на бизнес

В процессе ВИА обычно используют :

- анкетирование,
- интервью,
- структурированные совещания,
- их комбинацию.

Это позволяет достичь понимания функционирования критических процессов, влияния нарушений этих процессов и необходимого времени восстановления RTO и ресурсов.

Оценка воздействия на бизнес

Ключевые этапы метода BIA:

- определение критичности ключевых процессов и ключевых видов продукции, работ, услуг организации на основе оценки для них опасностей, угроз и уязвимостей;
- определение экономических и производственных последствий нарушений/разрушений идентифицированных критических процессов за определенные периоды времени;
- идентификация взаимосвязей с ключевыми внутренними и внешними причастными сторонами. На этом этапе может быть полезно составление карт взаимосвязей в системе и в цепи поставок;
-

Оценка воздействия на бизнес

- определение имеющихся необходимых ресурсов для обеспечения непрерывности работ после нарушения/разрушения на минимальном приемлемом для организации уровне;
- идентификация альтернативных способов выполнения работ и процессов, существующих или запланированных к разработке. Альтернативные способы выполнения работ и процессов могут быть применены в ситуации недостатка или отсутствия необходимых ресурсов или возможностей во время нарушения/разрушения;
-

Оценка воздействия на бизнес

- определение максимально допустимого периода простоя при нарушении/разрушении (MAO – Maximum Acceptable Outage Time) для каждого процесса, основанного на идентифицированных последствиях и критических факторах выполняемых видов деятельности;
- определение целевого времени восстановления (RTO) для любого специализированного оборудования, информационных технологий и других активов организации;
-



Оценка воздействия на бизнес

- установление уровня подготовленности критических процессов для управления в условиях нарушения, которое может включать оценку уровня резервированности процесса (например, наличия запасного оборудования) или существование альтернативных поставщиков.

Оценка воздействия на бизнес

Итоги выполнения проверки:

- перечень ранжированных по приоритетам критических процессов и соответствующих взаимозависимостей;
- зарегистрированные экономические и производственные воздействия, вызванные нарушением критических процессов;
- вспомогательные ресурсы, необходимые для идентифицированных критических процессов;
- возможные сроки простоя и восстановления критических процессов и взаимосвязанных информационных технологий.



Анализ рисков



Анализ рисков

Анализ рисков — это процесс выявления и анализа потенциальных проблем, которые могут негативно повлиять на основные бизнес-инициативы или важные проекты.

Цель анализа — избежать возникновения этих рисков или снизить возможный ущерб.

Анализ рисков

Выделяют три основных этапа анализа рисков:

- Выявление рисков.
- Анализ рисков.
- Снижение рисков в цепи поставок.



Выявление рисков

Выявление рисков — могут быть связаны с внутренними факторами, такими как структура цепочки поставок, политики управления запасами и транспортировки, или с внешними факторами, например, природными катастрофами, экономической и политической обстановкой.

Анализ рисков

Анализ рисков — на этом этапе риски оцениваются по набору показателей и выделяются самые опасные. К наиболее распространенным показателям для анализа относятся:

- вероятность и частота возникновения риска;
- последствия или ожидаемые потери;
- величина риска = вероятность последствия;
- время на восстановление;
- время жизнеспособности.



Снижение рисков в цепи поставок

Снижение рисков в цепи поставок — на последнем этапе разрабатывается план, и предпринимаются необходимые меры. При разработке плана важно оценить его эффективность и то, как изменятся показатели в результате запланированных действий.



RPO (Recovery point objective)



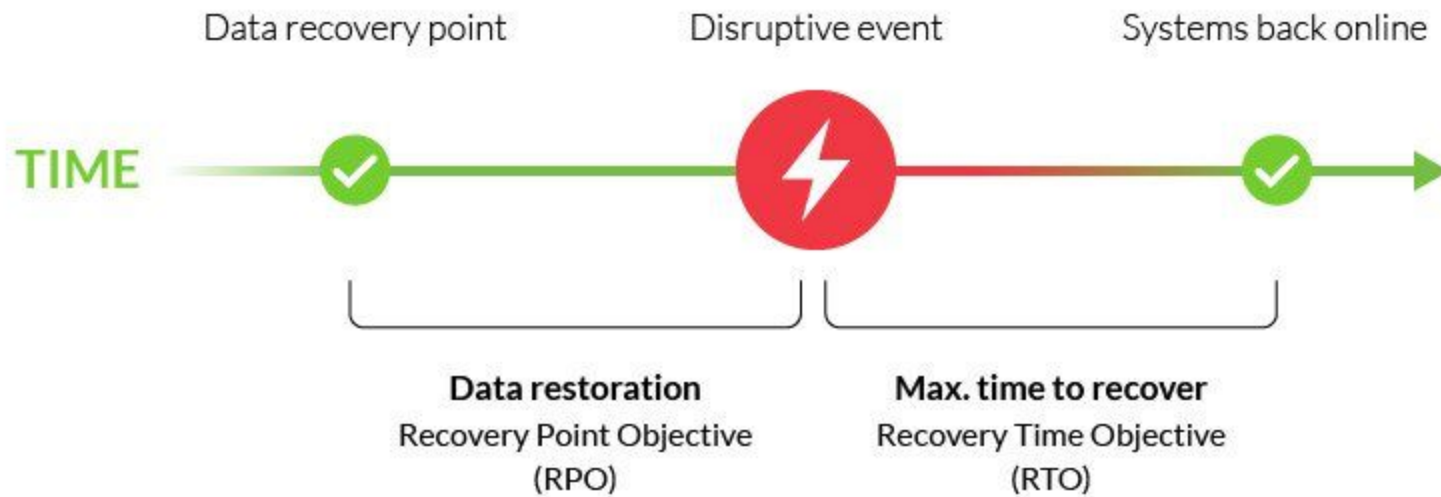
RPO

RPO (recovery point objective) это максимальный период времени, за который могут быть потеряны данные в результате инцидента. Время восстановления файлов из резервного хранилища не должно превышать показателя RPO.

Например, RPO равен 90 минутам, будут потеряны данные, наработанные не более, чем за последние полтора часа. Соответственно, snapshot должен проводиться не реже, чем раз в 90 минут.

Резервироваться могут не только файлы на дисках, но и настройки приложений, серверных ОС, а также состояние процессов в оперативной памяти.

RPO



<https://www.imperva.com/learn/availability/recovery-point-objective-rpo/>

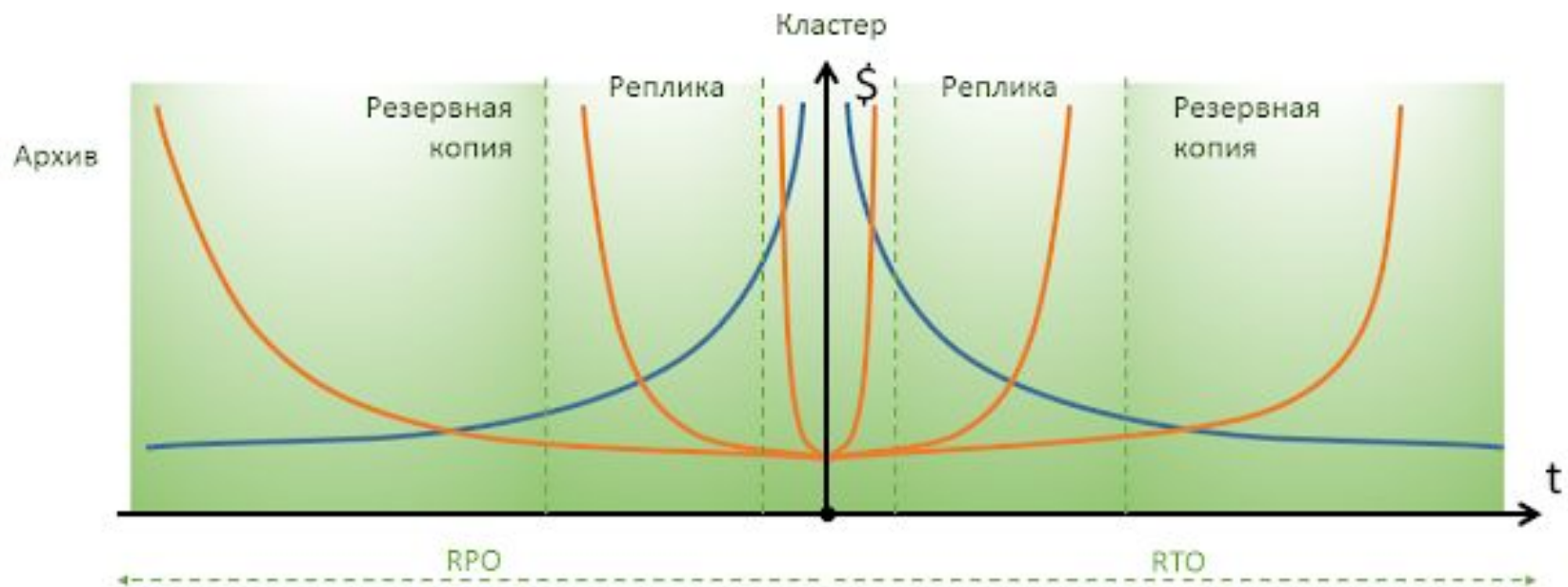


RPO

RPO устанавливается с учетом того, какой объем данных может потерять пользователь (клиент) в случае инцидента.

Определиться с этим помогает расчет точки безубыточности, когда стоимость потери данных равна стоимости обеспечения их доступности. Затраты на восстановление в идеале не должны быть избыточными или недостаточными.

RPO





**RTO (recovery time
objective)**



RTO

RTO (recovery time objective) это промежуток времени, в течение которого система может оставаться недоступной в случае аварии.

RTO может составлять от нескольких секунд — например, при репликации в облаке, до нескольких дней, когда бэкап пишется на физические носители — например, на магнитную ленту.

Выбор остается за заказчиком: если это клиентский портал банка, время простоя не должно превышать нескольких минут, если персональный сайт — он может «полежать» и сутки.



Итоги

Итоги

Сегодня мы рассмотрели типы аварийного восстановления, анализ воздействия на бизнес, анализ рисков, RTO, RPO.

Получили представление о процессах планирования аварийного восстановления.

Познакомились с представителями DRaaS и BaaS.





Домашнее задание

Домашнее задание

Давайте посмотрим ваше [домашнее задание](#).

- Вопросы по домашней работе задавайте **в чате** мессенджера Slack.
- Задачу можно сдавать **по частям**.
- Зачёт по домашней работе проставляется после того, как **приняты задача полностью**.

**Задавайте вопросы и
пишите отзыв о лекции!**

Имя Фамилия

