HITACHI
Inspire the Next

ОФИЦИАЛЬНЫЙ ДОКУМЕНТ

Постоянная доступность данных и восстановление в процессе эксплуатации: почему необходимо и то, и другое

Методология комплексных решений для защиты данных

Hitachi Data Systems

Апрель 2015 г.

Содержание

Краткий обзор

В этом техническом документе речь идет о проблемах, с которыми сталкиваются пользователи приложений, когда пытаются обеспечить их непрерывную работу и эффективно защитить данные от риска потери вследствие различных угроз. Здесь рассматриваются несоответствия между существующими методами и отраслевыми тенденциями, способные усугубить эти сложности. Приведено также краткое описание решения Hitachi Data Systems, эффективно устраняющего эти проблемы. Данный документ предназначен для людей, принимающих решения о приобретении технологий и влияющих на такие решения.

В настоящее время под защитой данных во основном подразумевается резервное копирование и восстановление, и практически нет организаций, которые удовлетворены имеющейся средой. В этом техническом документе разъясняются преимущества комплексного подхода с использованием других технологий, таких как отказоустойчивость в режиме Active/Active, непрерывная защита данных, моментальные снимки, репликация и архивирование.

Действительно, ни одна технология не может идеально подходить для всех приложений, нагрузок или требований к уровню обслуживания. Важно понимать, какое решение следует использовать в каждой ситуации и как эти решения работают вместе в рамках комплексного подхода для поддержания деятельности организации. Защита данных всегда была программно-определяемой задачей. Компания Hitachi Data Systems предлагает перейти к защите данных *на основе бизнес-требований*.

Проблемы, связанные с защитой данных

Как уже упоминалось, сейчас на рынке представлено много технологий управления данными и обеспечения доступности, защиты и восстановления. На самом деле их так много, что сложно определить, какие расположения, решения и их сочетания необходимы и подходят для конкретной ситуации.

Объем данных, которые нужно защищать

Список типов данных, требующих защиты, постоянно расширяется. До недавних пор защита корпоративных данных, как правило, не охватывала ноутбуки, ПК, удаленные офисы, а также среды тестирования и разработки. В связи с появлением большого числа государственных нормативных документов, судебных разбирательств и критически важной для бизнеса информации, которая часто хранится на устройствах пользователей, теперь необходимо обеспечивать надлежащую защиту и этих распределенных данных.

Защита крупных объектов

Сложно защищать один большой объект, который нельзя разделить на небольшие части перед резервным копированием. Например, передача набора данных объемом 84 ТБ по одному 10-гигабайтному соединению занимает 24 часа, т. е. обеспечить ежедневное резервное копирование такого объекта практически невозможно. В качестве решения предлагается синхронная или асинхронная репликация. Но сама по себе репликация не обеспечивает восстановление с предыдущего заданного момента времени и, следовательно, не защищает данные от удаления или повреждения.

Защита множества небольших объектов

Последовательное открытие, чтение, копирование и закрытие большого количества объектов (файлов) занимает слишком много времени. В файловых системах с бесчисленным множеством файлов (десятками миллионов) этот процесс может длиться несколько часов и выходить за рамки доступного интервала резервного копирования. Например, если каждую секунду можно создавать резервные копии 100 файлов, то за 24 часа удастся скопировать одним потоком только 8,6 млн файлов.

Длительное сохранение

При существующих технологиях сложно гарантировать возможность восстановления данных после продолжительного периода сохранения (например, в течение 20 лет и больше). Срок службы ленточных накопителей с течением лет увеличился, однако из-за периодических циклов обновления технологий и потребности постоянно контролировать окружающие условия их неудобно использовать в течение длительного времени.

Требования к уровням обслуживания

ИТ-отделам приходится не только справляться с описанными задачами, но и поддерживать бесперебойную работу всей инфраструктуры. Некоторые приложения и данные ценнее других, но для тех элементов, которые критически важны для бизнеса, любое время простоя недопустимо.

Есть несколько критериев эффективности защиты данных, связанных с доступностью защищаемых систем. Цель — свести эти показатели к нулю.

- **Интервал резервного копирования** — количество времени, на которое необходимо приостановить деятельность для выполнения резервного копирования. Если операции записи не будут остановлены, резервные копии данных будут повреждены или противоречивы. Традиционное инкрементное или полное

резервное копирование часто занимает много часов. В связи с этим интервал резервного копирования является критически важным показателем, который необходимо контролировать и улучшать.

- **Показатель точки восстановления (RPO)** — период времени между операциями резервного копирования. Этот показатель также можно представить как количество недавно созданных данных, для которых существует риск потери, поскольку если они не защищены, то их не удастся восстановить. Например, для традиционных операций резервного копирования, выполняемых каждую ночь, показатель точки восстановления составляет 24 часа.
- **Показатель времени восстановления (RTO)** — количество времени, которое требуется для восстановления деятельности после случая потери данных. Закономерен вопрос: какое время простоя каждого приложения или расположения допустимо, прежде чем это негативно скажется на деятельности предприятия? Время простоя критически важных приложений в больших компаниях часто может обходиться в миллионы долларов в час.

Унифицированное управление восстановлением

В большинстве организаций для защиты всех данных в выходные дни выполняется полное резервное копирование, а в будние дни — инкрементное. Такой шаблонный подход все больше демонстрирует свою несостоятельность, так как не все данные имеют одинаковую ценность.

Hitachi Data Systems рекомендует многоуровневый подход к защите, основанный на требованиях к уровням обслуживания для конкретных данных и достижении целевых показателей восстановления. Есть три основные причины, по которым организации защищают данные, обеспечивая возможность их восстановления. Каждая из этих причин требует различных технологий, оптимизированных для конкретного типа восстановления.

- **Восстановление в процессе эксплуатации** — это восстановление после проблем, возникших при эксплуатации, таких как ненамеренное удаление, действия злоумышленников, локализованный сбой аппаратного обеспечения, повреждение данных и т. п. Это наиболее частый вид восстановления среди операций защиты данных.
- **Восстановление после аварий** выполняется после катастроф в масштабе всего объекта, например землетрясений и цунами. К счастью, необходимость в нем возникает крайне редко. Это очень сложный и дорогостоящий вид восстановления, при котором обычно требуется перезапуск операций в альтернативном центре обработки данных.
- **Долгосрочное восстановление** обеспечивает обнаружение данных, которые хранятся длительное время, например 20 лет и более лет, и доступ к ним. Это могут быть записи, сохраняемые по требованию государственных органов либо в целях управления, сбережения или проведения исследований. Для обеспечения долгосрочного восстановления требуется применять определенный подход к управлению жизненным циклом данных. В рамках такого подхода необходимо осуществлять миграцию неактивных или требуемых файлов в архивный репозиторий, индексировать файлы для возможности восстановления в будущем и обеспечивать услуги сохранения, такие как контроль версий для аудита, хранение документов по юридическим причинам, контроль срока действия и уничтожение на битовом уровне.

На рис. 1 показаны некоторые доступные технологии, помогающие достичь определенных показателей точки и времени восстановления (RPO и RTO) для приложений. Например, непрерывная защита данных позволяет уменьшить показатель точки восстановления практически до нуля, тогда как репозиторий на основе дисков обеспечивает наименьший показатель времени восстановления. Используя выделенное программно-аппаратное устройство для дедупликации данных, например Hitachi Protection Platform, можно создать в высшей степени экономичный репозиторий для резервных копий, одновременно обеспечив максимальную пропускную способность.

Рис. 1. Организации могут выбирать различные решения для комплексной защиты и восстановления данных.

RPO — показатель точки восстановления, RTO — показатель времени восстановления, CDP — непрерывная защита данных

Кроме целевых показателей восстановления, организации также могут позаботиться о предотвращении потери данных за счет **повышения отказоустойчивости** систем, улучшив доступность приложений благодаря защите от сбоев аппаратного обеспечения, катастроф, отключений сети и других непредвиденных происшествий. Можно обеспечить непрерывное выполнение операций в центрах обработки данных.

При каждом из описанных типов восстановления организациям рекомендуется защищать ценную информацию более агрессивными методами, чем остальные данные. Это позволит сократить риски для важной информации и снизить стоимость защиты данных, имеющих меньшую ценность для организации. На рис. 2 показаны три возможных уровня приложений и технологии, позволяющие достичь нужных показателей точки и времени восстановления для каждого из них. Вы можете скорректировать этот список для своей организации с учетом особенностей среды и имеющихся потребностей.

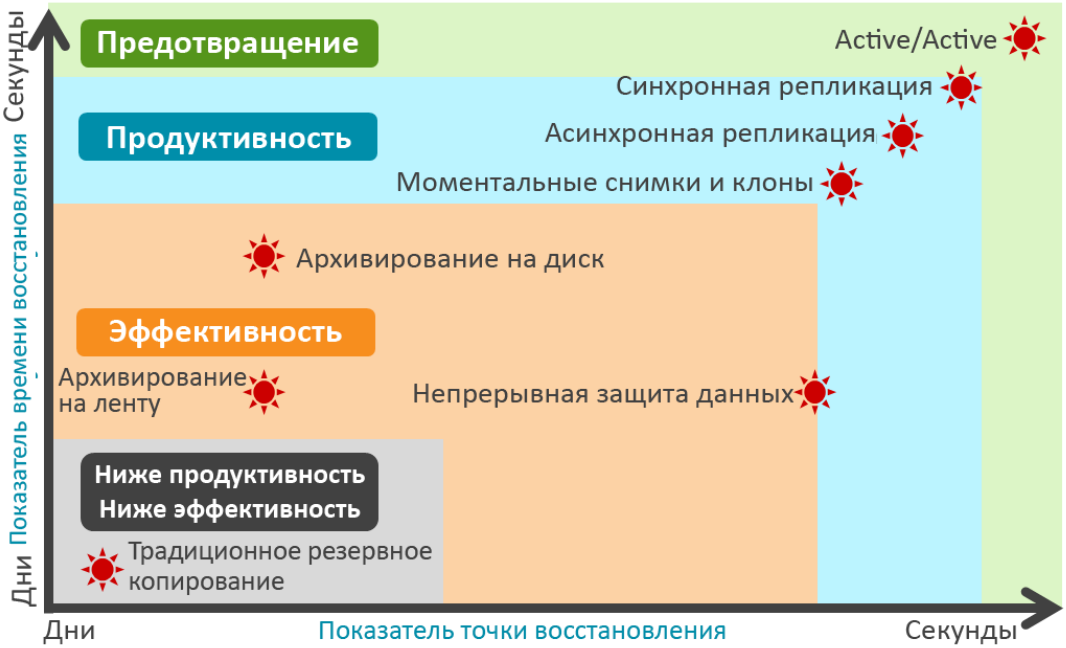
Рис. 2. Достигать необходимых показателей точки и времени восстановления можно с помощью различных уровней и технологий.

Цели защиты	Уровень 1 Критически важные данные	Уровень 2 Менее важные данные	Уровень 3 Некритичные данные
Отказоустойчивость в процессе эксплуатации Предотвращение аппаратных сбоев, отключения сети	Кластеры в режиме Active/Active	Кластеры в режиме Active/Passive	Многочисленные точки доступа
Восстановление в процессе эксплуатации Восстановление после повреждений, аппаратных сбоев, удаления...	Частое создание копий в массивах	Создание копий на диске, на объекте	Создание копий на ленте, на данном объекте или на другом
Восстановление после аварий Восстановление после катастроф на уровне объекта	Создание копий на другом объекте в реальном времени	Создание копий на другом объекте почти в реальном времени	Периодическое создание копий на другом объекте
Долгосрочное восстановление Восстановление после очень длительного хранения	Хранилище реплицированного контента	Хранилище контента с локальной защитой	Хранилище контента с локальной защитой

Защита данных на основе уровней обслуживания

Чтобы спроектировать идеальную инфраструктуру для защиты, сохранения и восстановления данных в организации, рекомендуется распределить необходимые уровни обслуживания по категориям. На рис. 3 использованы категории «Предотвращение», «Продуктивность», «Эффективность» и «Ниже продуктивность, ниже эффективность», помогающие определить ожидания и задать показатели точки и времени восстановления.

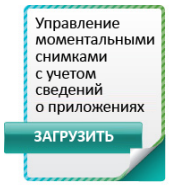
Рис. 3. Распределение требований к уровням обслуживания по категориям с учетом показателей точки и времени восстановления.



Определения
Показатель точки восстановления: потеря какого объема данных допустима?
Показатель времени восстановления: какое время простоя допустимо?

Предотвращение

Часто имеется определенный набор приложений, нагрузок и процессов, которые должны всегда оставаться работоспособными. Поддерживая их работоспособность в круглосуточном режиме, вы максимально увеличиваете эффективность и рентабельность организации и помогаете избежать катастрофических последствий из-за недоступности (таких как потеря заказов или штрафы).



Репликация и синхронизация, обеспечиваемые функционалом Global Active Device платформы Hitachi Virtual Storage Platform G1000 (VSP G1000), работают с кластеризованными серверами приложений. Они позволяют достичь максимального уровня непрерывной доступности, необходимого этим приложениям. Эти услуги выходят за пределы обычного восстановления после аварий, которое требует выполнения определенных действий вручную для эффективного аварийного переключения на другое расположение. Они действительно сводят к нулю показатели точки и времени восстановления. При использовании кластера в режиме Active/Active нет необходимости выполнять аварийное переключение после происшествия. Полный набор приложений и процессов уже запущен и доступен в другом расположении.

Кластеризация в режиме Active/Active предотвращает простои, тем самым обеспечивая уровень обслуживания с нулевыми показателями точки и времени восстановления.

Продуктивность

Среди главных недостатков традиционных технологий резервного копирования — длительное время создания резервных копий (интервал резервного копирования) и время, требуемое для восстановления (показатель времени восстановления). При полном резервном копировании все данные копируются из исходной системы в целевую. При инкрементном резервном копирования выполняется длительное сканирование исходного каталога, чтобы обнаружить изменения с момента предыдущего резервного копирования.

В обоих случаях резервное копирование и восстановление может длиться много часов, в течение которых защищаемые приложения обычно недоступны пользователям. Такие временные рамки были допустимы, когда работа компаний прекращалась в 18:00 и возобновлялась следующим утром. Однако сейчас условия изменились.

Чтобы обеспечить более эффективную защиту важных наборов данных, в VSP G1000 реализованы такие технологии, как современная аппаратная кластеризация в режиме Active/Active (см. выше), моментальные снимки, клонирование и репликация.

Технология создания моментальных снимков Hitachi Thin Image (HTI) позволяет выполнять в системах хранения данных Hitachi логическую репликацию данных на заданный момент времени с учетом изменений для немедленного коммерческого применения. Коммерческое применение может включать в себя операции резервного копирования и быстрого восстановления данных, поддержку принятия решений, обработку информации, а также тестирование и развертывание программного обеспечения.

Программное обеспечение Hitachi ShadowImage Replication является независимым от типа хоста решением для репликации данных без прерывания работы. С его помощью можно создавать копии любых данных, к которым имеет доступ ИТ-администратор, в рамках одной системы хранения данных Hitachi. ShadowImage также обеспечивает доступность приложений хоста, позволяя выполнять операции резервного копирования параллельно с работой производственных или бизнес-приложений.

Подготовку, планирование работы и контроль упомянутого ранее ПО для моментальных снимков и репликации можно осуществлять с помощью решения Hitachi Replication Manager (HRpM), которое входит в состав Hitachi Command Suite (HCS).

Однако при аппаратном создании моментальных снимков и клонов не учитываются сведения о приложениях. Когда приложение (например, система управления взаимодействием с клиентами — CRM) обрабатывает транзакцию, оно осуществляет запись в разные файлы и таблицы. Необходимо собрать вместе все эти изменения, чтобы создать согласованную с приложением копию и обеспечить надежное восстановление.

Для сред приложений Microsoft®, включая Exchange и SQL Server®, и для баз данных Oracle в средах Linux компания HDS предлагает программное обеспечение Hitachi Data Instance Director (HDID). HDID переводит эти приложения в состояние, готовое для создания моментальных снимков, прежде чем обращаться к услугам HTI или ShadowImage в системе хранения семейства VSP. HDID также координирует функцию клонирования каталогов систем Hitachi NAS Platform. Для других сред, включая приложения Microsoft, эту же функцию выполняет Hitachi Data Protection Suite с технологией CommVault IntelliSnap.

Hitachi также предлагает абсолютно надежное решение для защиты данных в средах VMware vSphere. Это продукт Hitachi Virtual Infrastructure Integrator, который упрощает управление данными для файловых и блочных хранилищ, с простым в использовании модулем политик на основе бизнес-требований для резервного копирования и восстановления. Данное решение помогает соблюдать соглашения об уровнях обслуживания в области резервного копирования и восстановления на уровне виртуальной машины, одновременно повышая степень использования ресурсов. Благодаря этому администраторы виртуальных машин могут управлять защитой данных с учетом сведений о приложениях с консоли VMware vCenter, что ведет к упрощению ИТ-операций. Virtual Infrastructure Integrator помогает организациям снижать риски для бизнеса за счет быстрого восстановления приложений, улучшающего показатели точки и времени восстановления.

Используя аппаратные возможности создания моментальных снимков и репликации, можно эффективно и быстро копировать данные. Делайте это чаще, чтобы сократить объем данных, который находится под угрозой в периоды между операциями резервного копирования.

Другой способ минимизировать потери критически важных данных и время простоя — применение непрерывной защиты данных на уровне хостов. Эти программные решения захватывают каждое изменение при его записи на диск, что устраняет потребность в интервале резервного копирования. Изменения данных могут отправляться в репозиторий резервных копий непрерывно или по заданному графику. При данном методе происходит захват большего объема данных, чем при других, поэтому непрерывная защита часто применяется для только краткосрочного восстановления в процессе эксплуатации, а для длительного сохранения периодически создаются моментальные снимки или резервные копии. HDS предлагает решение Hitachi Data Instance Director для непрерывной защиты данных в средах Microsoft Windows®.

Для сред, где необходимо лишь повысить производительность имеющегося решения для резервного копирования и восстановления, чтобы добиться своевременного выполнения операций, HDS предлагает решение Hitachi Protection Platform (HPP). Этот специализированный модуль дедупликации данных обеспечивает лучшую в отрасли масштабируемость и производительность.

В основе большинства проблем, связанных с защитой данных, лежит рост объемов данных. Полное резервное копирование занимает слишком много времени, приводя к недопустимым простоям. Восстановление данных в случае проблем также выполняется длительное время и приводит к простоям. Кроме того, следует учесть, что на каждый 1 ТБ первичного хранилища часто требуется от 3 до 5 ТБ хранилища для резервных копий. Вы можете представить себе, насколько большие затраты потребуются на оборудование, техническое обслуживание, программное обеспечение, управление и природоохранные мероприятия.

Один из основных способов, позволяющих справиться с несомненным ростом объемов данных, — сокращение объема данных, требующих защиты. Контроль можно реализовать с помощью эффективных политик управления жизненным циклом данных, которые автоматически убирают неактивные данные из первичной системы хранения. Если эти данные необходимо хранить, они перемещаются на уровень архивного хранилища, обладающий функциями самоуправления и самозащиты. Когда исчезает потребность в хранении данных, они автоматически удаляются из первичного или архивного хранилища.

Hitachi Data Systems предлагает ведущее решение для архивного хранилища с самоуправлением и самозащитой — Hitachi Content Platform (HCP). Многие программные решения для управления архивами, жизненным циклом данных и контентом могут отправлять данные в HCP для долгосрочного управления. В число этих решений входят: HDID, Hitachi Data Protection Suite (на базе CommVault), Rocket Arkivio AutoStor и Symantec Enterprise Vault.

Ниже продуктивность, ниже эффективность

Можно по-прежнему использовать традиционные методы полного и инкрементного резервного копирования, которые применялись с начала эры компьютерных технологий. Если не требуется обеспечивать непрерывную доступность наборов данных, например, в ночное время, и допускается длительное время восстановления после сбоев, такие методы могут быть экономически выгодными. Резервное копирование остается рентабельным благодаря внедрению дедупликации данных, позволяющей исключать большие объемы дублирующихся данных, которые создаются при полном резервном копировании.

Согласно прогнозам IDC, продажи традиционного программного обеспечения для резервного копирования в корпоративном сегменте продолжат расти примерно на 5 % в год. Эти оценки показывают, что такие методы резервного копирования, как запись на ленточные накопители, исчезнут еще не скоро. Хотя этот метод не годится для критически важных данных и приложений, ему по-прежнему находится применение.

Компания Hitachi Data Systems может помочь вашему предприятию организовать резервное копирование и восстановление на базе решения Hitachi Data Protection Suite или Symantec NetBackup (см. приложение). Наши высококвалифицированные инженеры по обслуживанию клиентов помогут сделать правильный выбор с учетом особенностей вашей среды.

Защита данных на основе бизнес-требований

По мере развития информационных технологий и их проникновения практически во все сферы нашей жизни обеспечение их доступности становится все более важной и сложной задачей. Чтобы справиться с этой проблемой, которую часто признают наиболее сложной в сфере корпоративных ИТ во всем мире, компания HDS предлагает набор ведущих на рынке надежных аппаратных и программных решений, а также услуг. Наши специалисты помогут спроектировать и развернуть наиболее экономичное комплексное решение, которое будет соответствовать особенностям вашей среды и требованиям к доступности приложений и способности восстановления.

Приложение. Набор решений Hitachi Data Systems для защиты данных

	Продукт	Функциональность	Поддержка платформ	Интернет
Моментальные снимки и репликация	Global Active Device	Кластер систем хранения в режиме Active/Active	Hitachi Virtual Storage Platform (VSP G1000)	
	Hitachi NAS File Clone	Аппаратное клонирование данных	Hitachi NAS Platform (HNAS)	
	Hitachi NAS Replication	Аппаратная репликация	HNAS	
	Hitachi Thin Image	Аппаратные моментальные снимки	Семейство VSP, Hitachi Unified Storage VM (HUS VM)	
	Hitachi ShadowImage Replication (на уровне системы)	Аппаратное клонирование данных	Семейство VSP, HUS VM	
	Hitachi TrueCopy Extended Distance	Зеркалирование и аварийное переключение в глобальном масштабе	Семейство VSP, HUS VM	
	Hitachi TrueCopy (синхронная удаленная репликация)	Зеркалирование и аварийное переключение в масштабе города	Семейство VSP, HUS VM	
	Hitachi Universal Replicator	Аппаратная репликация	Семейство VSP, HUS VM	
	Hitachi Replication Manager	Управление моментальными снимками и репликацией	Hitachi Command Suite	
	Hitachi Protection Platform	Программно-аппаратное решение для дедупликации данных, виртуальная библиотека ленточных накопителей	Symantec NetBackup, IBM® Tivoli® Storage Manager	

Управление моментальными снимками	Hitachi Data Instance Director	Управление моментальными снимками и репликацией с учетом сведений о приложениях	Hitachi Thin Image и Hitachi ShadowImage Replication, Hitachi TrueCopy, Hitachi Universal Replicator	
	Hitachi Data Protection Suite на базе CommVault с функцией CommVault IntelliSnap	Управление моментальными снимками с учетом сведений о приложениях	Hitachi Thin Image и Hitachi ShadowImage Replication; поддержка широкого спектра приложений	
	Hitachi Virtual Infrastructure Integrator	Детализированное резервное копирование и восстановление виртуальных машин с помощью моментальных снимков	HNAS, семейство VSP, HUS VM	
Непрерывная защита данных	Hitachi Data Instance Director	Непрерывная защита данных, архивирование, репликация	Серверы Microsoft Windows®	
Резервное копирование	Hitachi Data Protection Suite	Резервное копирование, создание моментальных снимков, архивирование и дедупликация в масштабе предприятия	Широкая поддержка операционных систем, приложений и систем хранения	
	Symantec NetBackup	Резервное копирование, создание моментальных снимков, архивирование и дедупликация в масштабе предприятия	Широкая поддержка операционных систем, приложений и систем хранения	

Архивирование	Hitachi Data Instance Director	Детализированное архивирование файлов и электронной почты на платформе Hitachi Content Platform	Файлы Windows и электронная почта Microsoft Exchange	
	Symantec Enterprise Vault	Архивирование и обнаружение в масштабе предприятия	Широкий спектр поддерживаемых платформ и приложений	
	Rocket Arkivio Autostor	Управление жизненным циклом файлов	Windows, Linux	

Hitachi Data Systems

Представительство в России
107045, Россия, Москва, ул. Трубная, д. 12, 8-й этаж
тел.: +7 495 787 21 30
www.hds.ru / hds.rcis@hds.com

Представительство в Украине
Украина, Киев,
ул. Н. Гринченко, д. 4в
тел.: +38 (044) 390 5950

Представительство в Казахстане
Республика Казахстан, Алматы,
ул. Байсеитовой, 11/13
тел.: +7 727 3278700 / e-mail: hds.rcis@hds.com

WP-478-C Р. Вайнинг (R. Vining), апрель 2015 г.