DOI: https://doi.org/10.15688/NBIT.jvolsu.2019.1.5

УДК 004.9
ББК 32.973

АНАЛИЗ СОВРЕМЕННЫХ СИСТЕМ ХРАНЕНИЯ ДАННЫХ

Вадим Юрьевич Шевцов

Ассистент кафедры информационной безопасности,
Волгоградский государственный университет
vadim94.d@mail.ru
просп. Университетский, 100, 400062 г. Волгоград, Российская Федерация

Евгений Сергеевич Абрамов

Кандидат технических наук, доцент,
заведующий кафедрой безопасности информационных технологий,
Южный федеральный университет
abramoves@sfedu.ru
ул. Б. Садовая, 105, 344006 г. Ростов-на-Дону, Российская Федерация

Аннотация. В статье анализируются сетевые и облачные системы хранения данных. Приводится обзор их видов, свойств, угроз и методов защиты от данных угроз. Также приводится сравнение существующих сетевых и облачных систем хранения данных.

Ключевые слова: системы хранения данных, облачные технологии, NAS, SAN, DAS, атака, методы защиты.

Недавнее появление облачных хранилищ данных дало приемлемую и во многом более удобную альтернативу традиционным системам хранения данных (далее – СХД). При этом проблемы безопасности не обошли стороной данные системы, так как удаленное хранение данных неразрывно связано с удаленным доступом к ним.

Облачное хранилище данных – модель онлайн-хранилища, в котором данные хранятся на многочисленных, распределенных в сети серверах, предоставляемых в пользование клиентам, в основном третьей стороной [2; 3].

Для начала необходимо рассмотреть существующие СХД.

Автономные (сетевые) СХД:

– NAS – сетевая система хранения данных. Технология NAS (Network Attached Storage) развивается как альтернатива универсальным серверам, несущим множество функций. В отличие от них NAS-устройства исполняют только одну функцию – файловый сервер. NAS подключаются к локальной вычислительной сети и осуществляют доступ к данным для неограниченного количества гетерогенных клиентов (клиентов с различными ОС) или других серверов.

– SAN (Storage Area Network) – сеть хранения данных. Она представляет собой архитектурное решение для подключения внешних устройств хранения данных, таких как дисковые массивы, ленточные библиотеки, оптические накопители к серверам та-

ким образом, чтобы операционная система распознала подключенные ресурсы как локальные.

– DAS – система хранения с прямым подключением. Системы хранения данных DAS (Direct Attached Storage) – это запоминающее устройство непосредственное, подключенное к серверу или рабочей станции без помощи сети хранения данных. Это означает, что внешний RAID-массив подключается к серверу или нескольким серверам через свои неразделяемые порты SCSI или FC, причем каждый из таких портов доступен лишь одному серверу. При этом, необходимо четко понимать, что DAS означает именно неразделяемые порты RAID-массива, а не само устройство [4; 5].

Причины использования сетевых СХД:

– растущий объем хранимых данных;

– потребность в избыточности и резервировании;

– готовность и доступность данных;

– консолидация систем хранения для централизованного управления;

– увеличение надежности и улучшение производительности;

– виртуализация систем хранения;

– снижение общей стоимости;

– защита данных.

Теперь рассмотрим облачные СХД:

1. Объектное хранилище. Приложения, разработанные в облаке, как правило, используют такие преимущества объектного хранилища, как широкие возможности масштабирования и хранение свойств объектов в виде метаданных. Объектные хранилища идеально подходят для разработки с нуля современных приложений, для которых требуется гибкость и возможность масштабирования.

2. Файловое хранилище. Некоторым приложениям требуется доступ к совместно используемым файлам, следовательно, им необходима файловая система. Данный тип хранилища часто поддерживается сервером хранилищ, подключенным к сети (NAS).

3. Блочное хранилище. Другие корпоративные приложения, например, базы данных или системы планирования ресурсов предприятия (ERP), часто нуждаются в выделенном хранилище с низкими задержками для каждого из узлов. Такое хранилище работает аналогично хранилищу с прямым подключением (DAS) или сети хранения данных (SAN).

Преимущества облачных СХД:

– возможность доступа к данным с любого компьютера, имеющего выход в сеть Интернет;

– возможность организации совместной работы с данными;

– высокая вероятность сохранения данных даже в случае аппаратных сбоев;

– стоимость обычно зависит от используемого места хранилища;

– нет необходимости в приобретении, поддержке и обслуживании собственной инфраструктуры по хранению данных;

– все процедуры по резервированию и сохранению целостности данных производятся провайдером «облачного» центра;

– относительно невысокая совокупная стоимость владения;

– быстрое время до развертывания;

– широкие настройки управления информацией.

Далее проанализируем угрозы СХД различных типов.

Среди угроз в отношении сетевых СХД выделяют следующие:

– уничтожение;

– хищение;

– несанкционированное искажение;

– нарушение подлинности;

– подмену;

– блокирование доступа.

Источники угроз могут быть как внешние, так и внутренние [6–8; 10; 11]. Угроза часто является следствием наличия уязвимостей в конкретных узлах сети хранения. Возможные уязвимости определяют составляющие элементы и свойства архитектурных решений сетей хранения, а именно:

– элементы архитектуры;

– протоколы обмена;

– интерфейсы;

– аппаратные платформы;

– системное программное обеспечение;

– условия эксплуатации;

– территориальное размещение узлов сети хранения.

Сегодняшние реалии в области систем хранения данных таковы, что отсутствие дол-

жного внимания к ним в решении вопросов защиты информации может привести к непредсказуемым последствиям. До сих пор в обеспечении защиты данных внимание главным образом уделялось их надежности. Поэтому значительная часть средств вкладывалась в развитие систем резервирования и архивирования информации на дополнительные носители, построение каналов для тиражирования данных на альтернативные площадки и т. д. [1; 6; 9].

По мере того, как архитектура приобретает все большую открытость, ее элементы в силу возможных уязвимостей становятся целями для различного рода атак, что чревато нарушением целостности хранимой информации, ее утерей и компрометацией. В силу вышесказанного, контроль и управление облаками является серьезной проблемой безопасности. Гарантий, что все ресурсы облака посчитаны и в нем нет неконтролируемых виртуальных машин, не запущено лишних процессов и не нарушена взаимная конфигурация элементов облака нет.

Это высокоуровневый тип угроз, так как он связан с администрированием облака, как единой системы, и для него общую защиту нужно строить индивидуально. Далее подробно рассмотрим угрозы облачных хранилищ, атаки на облачную инфраструктуру и возможные решения для их предотвращения.

Использование межсетевого экрана подразумевает работу фильтра, с целью разграничить внутренние сети ЦОД на подсети с разным уровнем доверия. Это могут быть отдельно серверы, доступные из Интернета или серверы из внутренних сетей. В облачных вычислениях важнейшую роль платформы выполняет технология виртуализации. Для сохранения целостности данных и обеспечения защиты рассмотрим основные известные угрозы для облачных вычислений. Анализ угроз для облачных систем хранения данных представлен в таблице 1.

Атаки на облака и решения по их устранению:

1. Традиционные атаки на ПО.

Уязвимости операционных систем, модульных компонентов, сетевых протоколов и др. – традиционные угрозы, для защиты от которых достаточно установить межсетевой экран, firewall, антивирус, IPS и другие компоненты, решающие данную проблему. При этом важно, чтобы данные средства защиты эффективно работали в условиях виртуализации.

2. Функциональные атаки на элементы облака.

Этот тип атак связан с многослойностью облака общим принципом безопасности. Для защиты от функциональных атак для каждой части облака необходимо использовать следующие средства защиты: для прокси – эффективную защиту от DoS-атак, для веб-сервера – контроль целостности страниц, для сервера приложений – экран уровня приложений, для СУБД – защиту от SQL-инъекций, для системы хранения данных – правильные бэкапы (резервное копирование), разграничение доступа. При этом интеграция в единую систему данных механизмов защиты необходима на стадии построения облака.

3. Атаки на клиента.

Большинство пользователей подключаются к облаку, используя браузер. Здесь рас-

Таблица 1

Анализ угроз облачных систем хранения данных

Объект	Данные	Инфраструктура
Угрозы	• уничтожение информации; • несанкционированный доступ; • несанкционированное искажение; • нарушение подлинности; • подмена; • злоупотребления привилегиями; • закрытие облачного сервиса	• уязвимость программного обеспечения; • компрометация, кража учетных записей; • взлом интерфейсов и API; • целевые кибератаки; • MITM-атаки; • закрытие облачного сервиса; • отказ оборудования; • отказ каналов связи; • отказ в обслуживании

сматриваются такие атаки, как Cross Site Scripting, «угон» паролей, перехваты веб-сессий, «человек посредине» и многие другие. Единственная защита от данного вида атак является правильная аутентификация и использование шифрованного соединения с взаимной аутентификацией.

4. Атаки на гипервизор.

Гипервизор является одним из ключевых элементов виртуальной системы. Основной его функцией является разделение ресурсов между виртуальными машинами. Атака на гипервизор может привести к тому, что одна виртуальная машина сможет получить доступ к памяти и ресурсам другой. Также она сможет перехватывать сетевой трафик, отбирать физические ресурсы и даже вытеснить виртуальную машину с сервера. В качестве стандартных методов защиты рекомендуется применять специализированные продукты для виртуальных сред, интеграцию хост-серверов со службой каталога ActiveDirectory, использование политик сложности и устаревания паролей, а также стандартизацию процедур доступа к управляющим средствам хост-сервера, применять встроенный брандмауэр хоста виртуализации.

5. Атаки на системы управления.

Большое количество виртуальных машин, используемых в облаках требует наличие систем управления, способных надежно контролировать создание, перенос и утилизацию виртуальных машин. Вмешательство в систему управления может привести к появлению виртуальных машин «невидимок», способных блокировать одни виртуальные машины и подставлять другие.

Методами защиты систем хранения данных являются:

– аутентификация;
– разграничение доступа;
– шифрование;
– резервирование.

Методы защиты информации, а также перекрываемые угрозы и риски представлены в таблице 2.

Угрозы, не перекрываемые данными средствами защиты:

– отказ в обслуживании;
– уязвимость программного обеспечения.

Сравнение существующих систем хранения данных приведено в таблице 3.

Как вывод, СХД, к сожалению, сегодня имеют определенные недостатки, но со своими задачами справляются. А чтобы определить какой сервис будет подходящим, пользователю необходимо сформировать критерии по отношению к хранилищам и только потом приступить к эксплуатации выбранной СХД.

Таблица 2

Анализ методов защиты систем хранения данных

Методы защиты информации	Перекрываемые угрозы
Разграничение доступа	• несанкционированный доступ; • несанкционированное искажение; • нарушение подлинности; • подмена; • злоупотребления привилегиями
Шифрование файлов	• несанкционированный доступ; • несанкционированное искажение; • нарушение подлинности; • подмена; • взлом интерфейсов и API; • Mitm-атаки; • целевые кибератаки
Аутентификация	• компрометация, кража учетных записей; • злоупотребления привилегиями
Резервирование	• отказ оборудования; • отказ каналов связи; • закрытие облачного сервиса; • уничтожение информации

Таблица 3

Анализ существующих реализаций сетевых и облачных систем хранения данных

Тип технологии	Хранилище	Разграничение доступа	Логин /пароль	Двухфакторная аутентификация	Проверка целостности	Шифрование файлов	Резервирование	Механизм корзины
Облачные	DropBox	+	+	+				
NAS	Сетевое хранилище QNAP D4 Pro	+	+		+			
NAS	Сетевое хранилище WD My Cloud Home WDBVXC0060HWT-EESN	+	+		+	+		
DAS	DELL PowerVault MD3000		+			+	+	
NAS	WD My Cloud Personal	+	+	+	+	+	+	+
SAS	SEAGATE Exos ST4000NM0025		+			+	+	

СПИСОК ЛИТЕРАТУРЫ

1. Безопасность ваших систем хранения не дает уснуть? – Электрон. дан. – Режим доступа: https://www.kaspersky.ru/blog/how-secure-is-your-storage/3728/. – Загл. с экрана.

2. Выбираем облачное хранилище: каждому бизнесу – по потребностям. – Электрон. дан. – Режим доступа: https://www.kp.ru/guide/oblachnoe-khranilishche.html. – Загл. с экрана.

3. ГОСТ Р 53131-2008 «Защита информации». – Электрон. текстовые дан. – Режим доступа: https://meganorm.ru/Data2/1/4293809/4293809001.htm. – Загл. с экрана.

4. Джонс, М. Анатомия облачной инфраструктуры хранения данных / М. Джонс. – Электрон. текстовые дан. – Режим доступа: https://www.ibm.com/developerworks/ru/library/cl-cloudstorage/. – Загл. с экрана.

5. Основные системы хранения данных и их особенности. – Электрон. дан. – Режим доступа: http://www.itworkroom.com/main-shd/. – Загл. с экрана.

6. Сетевое хранилище QNAP D4 Pro. – Электрон. дан. – Режим доступа: https://qnap.ru/d4-pro. – Загл. с экрана.

7. Сетевое хранилище WD My Cloud Home WDBVXC0060HWT-EESN. – Электрон. дан. – Режим доступа: https://www.wd.com/ru-ru/products/personal-cloud-storage/my-cloud-home.html. – Загл. с экрана.

8. DELL PowerVault MD3000. – Электрон. дан. – Режим доступа: https://www.dell.com/ru/business/p/powervault-md3000/pd. – Загл. с экрана.

9. DropBox. – Электрон. дан. – Режим доступа: https://www.dropbox.com/. – Загл. с экрана.

10. SEAGATE Exos ST4000NM0025. – Электрон. дан. – Режим доступа: https://www.seagate.com/ru/ru/enterprise-storage/exos-drives/exos-e-drives/exos-7e8/. – Загл. с экрана.

11. WD My Cloud Personal. – Электрон. дан. – Режим доступа: https://www.wd.com/products/personal-cloud-storage/my-cloud.html. – Загл. с экрана.

REFERENCES

1. *Bezopasnost vashikh sistem khraneniya ne daet usnut?* [Does the Security of Your Storage Systems Keep You Awake?]. URL: https://www.kaspersky.ru/blog/how-secure-is-your-storage/3728.

2. *Vybiraem oblachnoe khranilishche: kazhdomu biznesu – po potrebnostyam* [Select Cloud Storage: Every Business Needs]. URL: https://www.kp.ru/guide/oblachnoe-khranilishche.html.

3. *GOST R 53131-2008. Zashchita informatsii* [GOST R 53131-2008. Information Protection]. URL: meganorm.ru/Data2/1/4293809/4293809001.htm.

4. Dzhons M. *Anatomiya oblachnoy infrastruktury khraneniya dannykh* [Anatomy of a Cloud Storage Infrastructure]. URL: https://www.ibm.com/developerworks/ru/library/cl-cloudstorage.

5. *Osnovnye sistemy khraneniya dannykh i ikh osobennosti* [Main Data Storage Systems and

Their Features]. URL: http://www.itworkroom.com/main-shd.

6. *Setevoe khranilishche QNAP D4 Pro* [QNAP D4 Pro Network Storage]. URL: https://qnap.ru/d4-pro.

7. *Setevoe khranilishche WD My Cloud Home WDBVXC0060HWT-EESN* [Network Storage WD My Cloud Home WDBVXC0060HWT-EES]. URL: https://www.wd.com/ru-ru/products/personal-cloud-storage/my-cloud-home.html.

8. DELL PowerVault MD3000. URL: https://www.dell.com/ru/business/p/powervault-md3000/pd.

9. DropBox. URL: https://www.dropbox.com.

10. SEAGATE Exos ST4000NM0025. URL: https://www.seagate.com/ru/ru/enterprise-storage/exos-drives/exos-e-drives/exos-7e8/.

11. WD My Cloud Personal. URL: https://www.wd.com/products/personal-cloud-storage/my-cloud.html.

THE ANALYSIS OF MODERN DATA STORAGE SYSTEMS

Vadim Yu. Shevtsov

Assistant Lecturer, Department of Information Security,
Volgograd State University
vadim94.d@mail.ru
Prosp. Universitetskiy, 100, 400062 Volgograd, Russian Federation

Evgeny S. Abramov

Candidate of Sciences (Engineering), Associate Professor,
Head of the Department of Information Technologies Security,
South Federal University
abramoves@sfedu.ru
B. Sadovaya St., 105, 344006 Rostov-on-Don, Russian Federation

Abstract. Today, Storage Area Network and Cloud Storage are the common Storage System. Storage Area Network includes NAS, SAN, DAS systems. Cloud Storage includes object storage, file storage, block storage.

Storage Area Network is an important technology because it may give a lot of data volume with a high recovery chance and secure access, work and central management with data.

Cloud Storage has many advantages: data mobility, teamwork, stability, scalability, quick start.

The main threats include destruction, theft, corruption, unauthentication, replacement, blocking. Storage Area Network components (architecture elements, protocols, interfaces, hardware, system software, exploitation) have a lot of vulnerabilities. Cloud Storage may be attacked by software, functional elements, clients, hypervisor, management systems.

A lot of companies design storage solutions: DropBox, QNAP, WD, DELL, SEAGATE.

Key words: SS, cloud technologies, NAS, SAN, DAS, attack, secure methods.