НИУ МЭИ

Кафедра: «Безопасность и информационные технологии»

Оценка информационных рисков при использовании облачных сервисов

Студент: Трифонов Р.А.
Группа: ИДз-61-18:
Научный руководитель: доц. Петров С.А.

Москва-2023

Актуальность

- Расширение применения облачных сервисов
- Зависимость от облачных сервисов
- Комплексность облачных сред
- Расширение угроз кибербезопасности
- Законодательные требования и регулирование
- Повышение осведомленности пользователей

Цель и задачи проекта

Цель работы – исследование облачных сервисов и выработка рекомендаций по нивелированию проблемного поля их использования.

Задачи:

1. Провести исследование предметной области, дать определение понятию облачные сервисы;
2. Рассмотреть существующие методы защиты информации при работе с облачными технологиями;
3. Провести анализ наиболее известных кампаний и их рисков;
4. Изучить использование облачных сервисов в учебном процессе;
5. Осуществить экономический анализ работы ВУЗ-ов с облачными хранилищами.

Обзор предметной области

Облачный сервис - в широком смысле это использование компьютерных ресурсов, которые непосредственно не находятся рядом с пользователем и не управляются им напрямую, для обеспечения вычислительной мощности.

Виды облачных систем:

– Частные

– Публичные

– Гибридные

Обзор предметной области

Достоинства	Недостатки
Потребность в приобретении оборудования	Необходимо постоянное подключение к сети
Использование фактические потребленных ресурсов и их эксплуатация.	
Упрощение работы персонала	В первую очередь безопасность данных зависит от поставщика облачных услуг.
Информационная защита	Высокая зависимость от облачного провайдера.
Резервное копирование данных	Если на территории государства находится центр обработки данных, то он имеет возможность получить доступ ко всей информации, хранящейся в нем.
Упрощение разработки	

Преимущества и недостатки облачных систем

У каждого вида облачной системы есть свои преимущества и недостатки, но я выделю основные общие пункты:

Преимущества:

– ответственность за работоспособность оборудования лежит на провайдере;

– взять готовую настроенную услугу проще, чем выстраивать собственную инфраструктуру;

– арендовать мощности может быть дешевле, чем тратиться на собственные серверы.

Недостатки:

– полная зависимость от поставщика;

– без интернета пользователь не сможет работать с сервисом.

Риски при защите информации в облачных сервисах

Проблемы с обеспечением облачной безопасности делятся на **внешние и внутренние**

Так же к проблемам облачной безопасности могу отнести:

- майнинг криптовалют;
- эксплойты облачных туннелей;
- неправильная конфигурация.

Риски при защите информации в облачных сервисах

Первоочередный риск, доступ к конфиденциальной информации со стороны провайдера услуг.

При оценке данного риска **основную угрозу** представляет собой **несанкционированный доступ** к таким объектам, как:

– база данных как сервис;

– виртуальный сервер;

– данные, передаваемые в незащищенном виде;

– иные объекты.

Риски при защите информации в облачных сервисах

Для минимизации данного риска рекомендуется применить следующие меры:

– шифровать конфиденциальные данные, хранимые в базе данных:

– шифровать данные при передаче:

– удалять системных пользователей и/или пакеты, созданные провайдером, с виртуальных серверов:

– запретить на уровне сетевых сегментов публичный доступ к базам данных;

– мониторить управленческие события на уровне облака;

– обязательно использовать многофакторную аутентификацию для доступа к облаку;

– контролировать целостность контейнеров и используемого программного обеспечения.

Оценка рисков

Оценка уровня риска являющегося допустимым, зависит от оценки требований к безопасности и ценности информационных активов. Приложения и процессы могут легко оказаться столь же жизненно важными, как сама информация.

Оценка рисков

Для оценки экономической эффективности затрат на информационную безопасность существует две модели подсчетов – **доходная** и **затратная**.

Оценка рисков

Для сохранения безопасности данных в облаке необходимо:

– шифровать данные;

– использовать надежные пароли и многофакторную аутентификацию;

– внимательно читать SSL, именно в нем прописано, какие обязательство несет провайдер, как он защищает ваши данные;

– настроить мониторинг сети;

– обезопасить api;

– выполнить все рекомендации по защите от ddos атак.

Оценка рисков

Главный риск на примере одного из популярных облачных хранилищ Dropbox

Бывшие сотрудники потенциально имеют доступ к бизнес-данным после прекращения трудовых отношений, что может привести к утечке и злонамеренному использованию информации.

Единственный способ обойти это – локально зашифровать данные с помощью продукта шифрования, сертифицированного PCI.

Оценка рисков

В целях минимизации возможности возникновения утечки информации следует принимать меры, которые включают обеспечение конфиденциальности и целостности:

– определить конфиденциальные данные и установить для них соответствующую защиту;

– разработать политику контроля доступа и только после этого давать права на пользование, редактирование, перемещение и копирование данных в облако и с него;

– внедрение современного криптографического решения компании до загрузки на облако с собственными ключами;

– придерживаться правила, что все данные хранящиеся в IT-инфраструктуре компании не должны передаваться за ее пределы и т.д.

Экономическая и финансовая выгода

Использование облачных хранилищ данных может привести к экономической эффективности в нескольких аспектах:

- снижение затрат на обеспечение и поддержку инфраструктуры;
- повышение масштабируемости и гибкости;
- увеличение безопасности и сохранности данных;
- улучшение производительности;
- снижение рисков и упрощение процессов.

Экономическая и финансовая выгода

Один из способов увеличения экономической и финансовой выгоды при использовании облачных сервисов, который можно предложить — это использование комбинированных облачных решений.

Экономические риски

Для оценки экономических рисков при использовании облачных сервисов можно разработать специальный алгоритм, который будет учитывать следующие параметры:

- Стоимость облачного сервиса
- Стоимость интеграции с существующими системами
- Стоимость поддержки и обслуживания
- Уровень безопасности
- Возможность масштабирования
- Повторные затраты
- Различные сценарии использования

Экономические риски

Согласно анализу, образовательные учреждения используют модель облака «ПО как сервис» (SaaS), которая дает следующие преимущества:

– организация совместной работы для большого коллектива преподавателей и учащихся;

– организация разных форм контроля;

– перемещение в облако используемых систем управления обучением (LMS);

– новые возможности для исследователей по организации доступа, разработке и распространению прикладных моделей.

Yandex Cloud

Одной из широко распространенных платформ является Yandex Cloud

Yandex Cloud

Одной из широко распространенных платформ является Yandex Cloud

Основные возможности данной платформы:

– бэк-офисная платформа – облачные справочные системы;

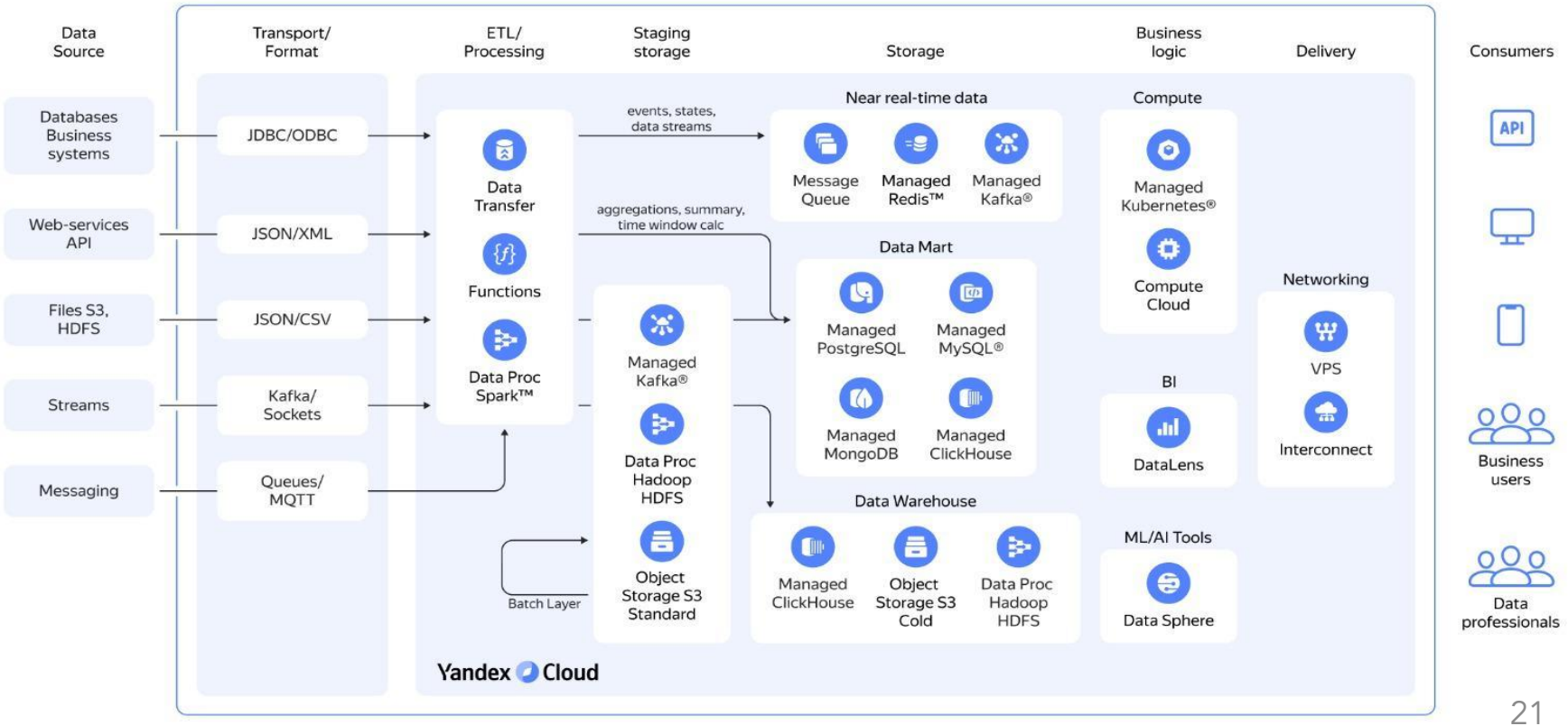
– цифровая инфраструктура и информационная безопасность – сервисы защиты от спама;

– обеспечение работы интеграционного слоя – файловое хранилище;

– работа с данными – аналитические облачные сервисы;

– надежность витрин цифрового университета – cdn.

Yandex Cloud



Заключение

В рамках научной работы были решены следующие задачи:

1. Проведено исследование предметной области, дано определение понятию облачные сервисы;
2. Рассмотрены существующие методы защиты информации при работе с облачными технологиями;
3. Проведен анализ наиболее известных кампаний и их рисков;
4. Изучено использование облачных сервисов в учебном процессе.

Спасибо за внимание!

Москва-2023