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

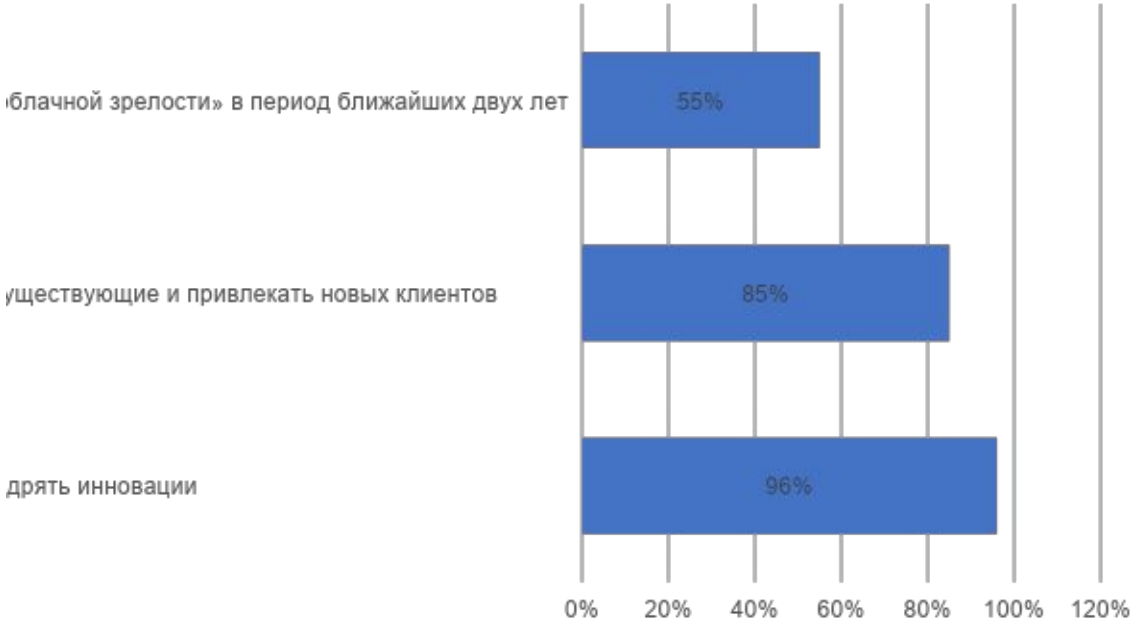
– Публичные

– Гибридные

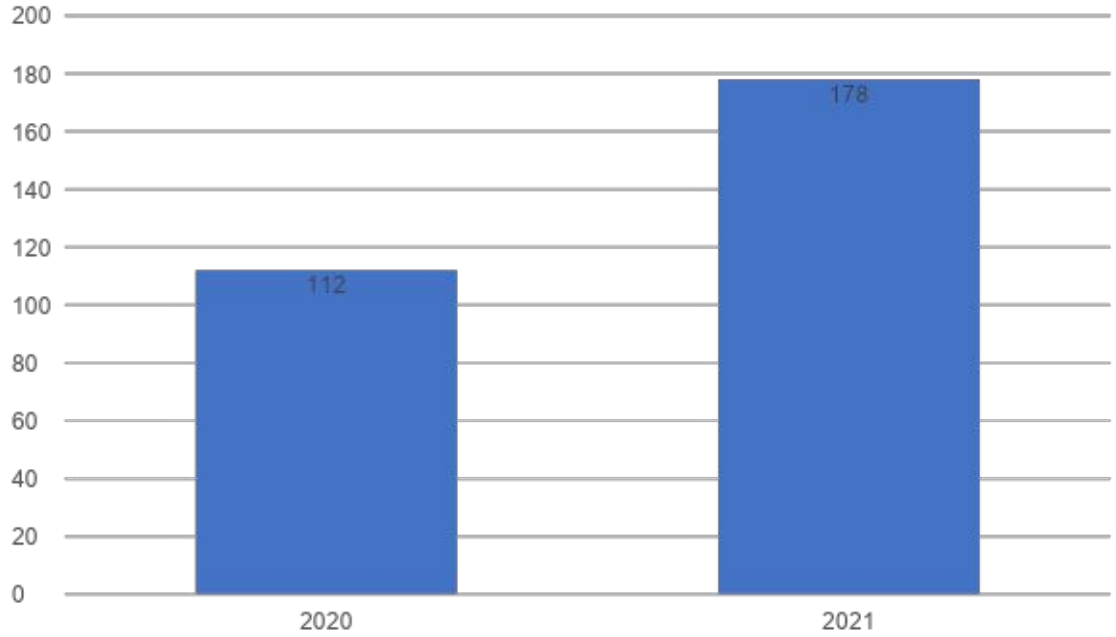
Обзор предметной области

Достоинства	Недостатки
Потребность в приобретении оборудования	Необходимо постоянное подключение к сети
Использование фактически 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	

Опрос о работе Oracle Research



Оценка Synergy Research Group



Расходы при различных сценариях внедрения облачных технологий

Виды расходов	Разработка нового приложения		Полная миграция приложения в облачные технологии	Продолжение эксплуатации приложения, созданного по традиционной модели
	по традиционной модели	с помощью облачной технологии		
Разовые: **на оборудование, разработку или усовершенствование приложения**	Высокие	Нет		
	Высокие		Средние	Нет
утилизацию оборудования	Нет		Средние	Нет
обучение персонала	Низкие, средние	Средние		Нет
Периодические: **на аренду облачных сервисов**	Нет	Средние		Нет
техническую поддержку				
заработную плату сотрудников	Высокие	Средние		Высокие
аренду помещения и инфраструктуры	Высокие	Нет		Высокие

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;

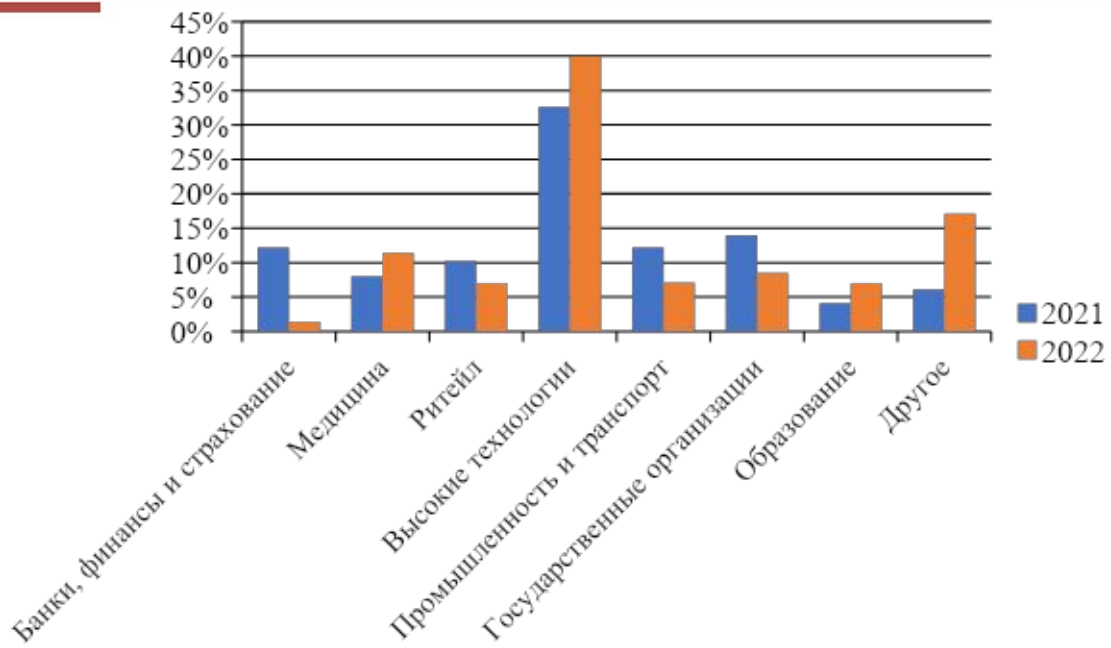
– арендовать мощности может быть дешевле, чем тратиться на собственные серверы.

Недостатки:

– полная зависимость от поставщика;

– без интернета пользователь не сможет работать с сервисом.

Исследования Аналитического центра компании InfoWatch



Риски при защите информации в облачных сервисах

К основным рискам при защите информации в облачных сервисах относятся:

- Утечка данных
- Потеря данных
- Несанкционированный доступ к данным
- Недостаточная защита от вредоносного программного обеспечения.

Риски при защите информации в облачных сервисах

Возможные способы получения доступа к облаку:

– вредоносное ПО;
– кросс-облачная атака;
– атака по боковому каналу;
– отказ в обслуживании;
– атака на вычислительные ресурсы;
– техники социальной инженерии;
– небезопасный API.

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:

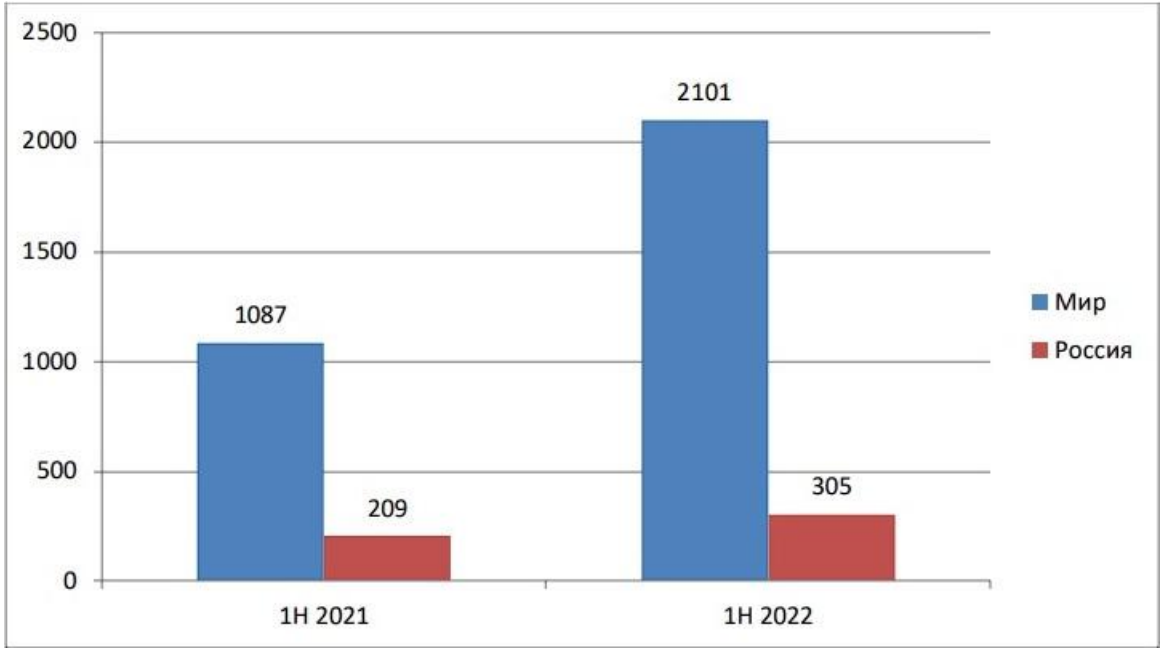
– база данных как сервис;

– виртуальный сервер;

– данные, передаваемые в незащищенном виде;

– иные объекты.

Оценка случаев раскрытия конфиденциальной информации



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;

– внедрить современное криптографическое решение 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;

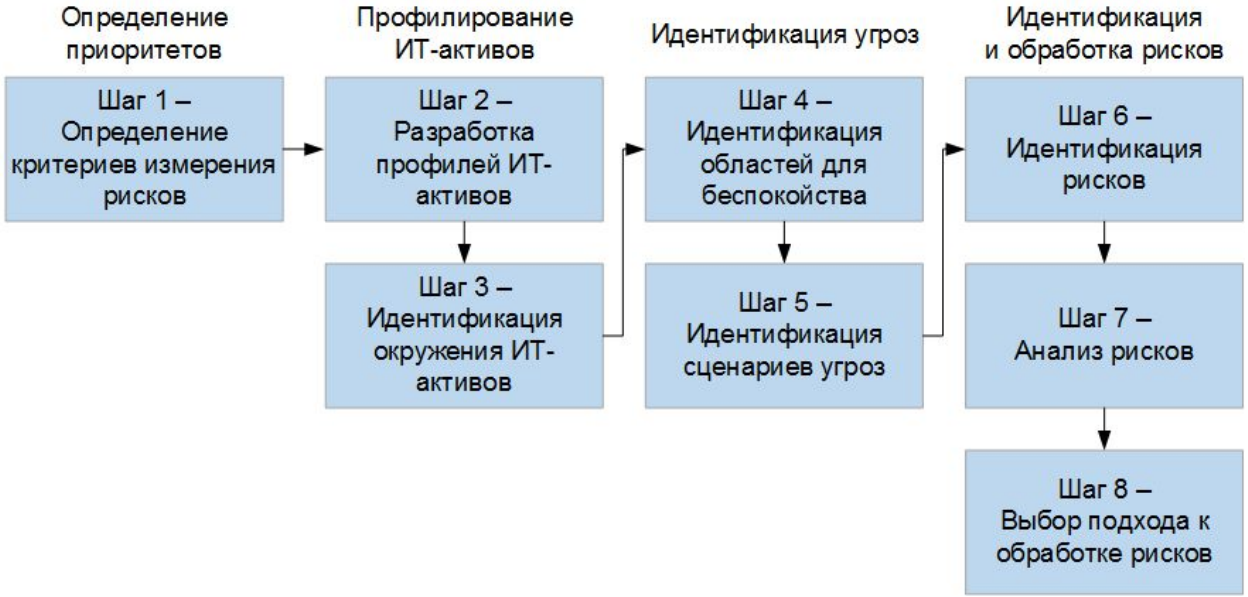
– перемещение в облако используемых систем управления обучением (LMS);

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

Основные методы управления рисками информационной безопасности

1. Метод CORAS
2. Метод OCTAVE
3. Матричный метод анализа
4. Метод Return on Investment for Security (расчет возврата инвестиций в безопасность)

Логическая взаимосвязь действий по методике OCTAVE



Типы контрмер безопасности

Тип контрмеры	Пример
Профилактические	1. Стандарты, процедуры, должностные инструкции 2. Аудит системы безопасности 3. Сетевые экраны 4. Системы обнаружения вторжений 5. Антивирусы 6. Средства шифрования 7. Формирование архивов
Лечебные	Резервные режимы работы
Принадлежат обоим типам	1. Планирование непрерывности бизнеса/ планирование восстановления бизнеса 2. Обучение

Преобразование вероятности угроз к ежегодной частоте

Уровень	Описание	Частота
Незначительный	Вряд ли произойдет	0,05
Очень низкий	Событие происходит 2-3 раза в год	0,6
Низкий	Событие происходит 1 раз в год	1,0
Средний	Событие происходит 1 раз в полгода	2,0
Высокий	Событие происходит 1 раз в месяц	12,0
Очень высокий	Событие происходит несколько раз в месяц	36,0
Экстремальный	Событие происходит несколько раз в день	365,0

Последствия, преобразованные в стоимость ликвидации нарушений

Степень тяжести нарушения	Описание	Потери, руб.
Несущественная	При осознанной угрозе нарушение не будет иметь последствий	0
Низкая	Нарушение не ведет к финансовым потерям, но выявление хакера происшествия потребует значительных затрат	15 000
Существенная	Происшествие принесет некоторый материальный и моральный вред	150 000
Угрожающая	Потеря репутации, конфиденциальной информации. Затраты на восстановление данных, проведение расследований	1 500 000
Серьезная	Потеря клиентов, деловой репутации. Восстановление практически всех данных на электронных и бумажных носителях	3 000 000
Критическая	Потеря системы или перевод в другую безопасную среду	7 500 000

Расчет показателя ожидаемых потерь для «МЭИ»

Актив	Потенциальная угроза	Вероятность	Последствия	Частота в год	Потери, руб.	ALE, руб.
Интернет-каналы	Разрушение ключевой инфраструктуры	Незначительная	Серьезные	0,005	3 000 000	150 000
	Отказ системы охлаждения	Средняя	Существенные	2	150 000	300 000
	Нарушение конфиденциальности информации	Низкая	Серьезные	1	3 000 000	3 000 000
	Повреждение аппаратных средств инфраструктуры	Очень низкая	Угрожающие	0,6	1 500 000	900 000
	Неправильное построение инфраструктуры	Низкая	Существенные	1	150 000	150 000
	Атака на сетевую структуру провайдера	Очень низкая	Существенные	0,6	150 000	90 000
	Отказ DNS	Незначительная	Угрожающие	0,05	1 500 000	75 000
Система эл. почты	Атака на систему электронной почты	Очень высокая	Существенные	36	150 000	5 400 000
Бизнес-приложения	Проблема вывода документов на печать	Высокая	Несущественные	12	0	0
	Проблемы чтения/сохранения файлов данных	Высокая	Несущественные	12	0	0
	Нарушения надежной работы бизнес-приложений	Низкая	Угрожающие	1	1 500 000	1 500 000
	Вывод из строя корпоративной системы документооборота	Высокая	Угрожающие	12	1 500 000	18000000
ИТОГО						29565000

Инвестиции в систему корпоративной защиты для «МЭИ»

№	Статьи затрат	Стоимость, руб.
1	Затраты на покупку лицензий	2 358 048
2	Затраты на проектные работы	369 785
3	Техническая поддержка (30% от стоимости лицензий ежегодно)	707 414

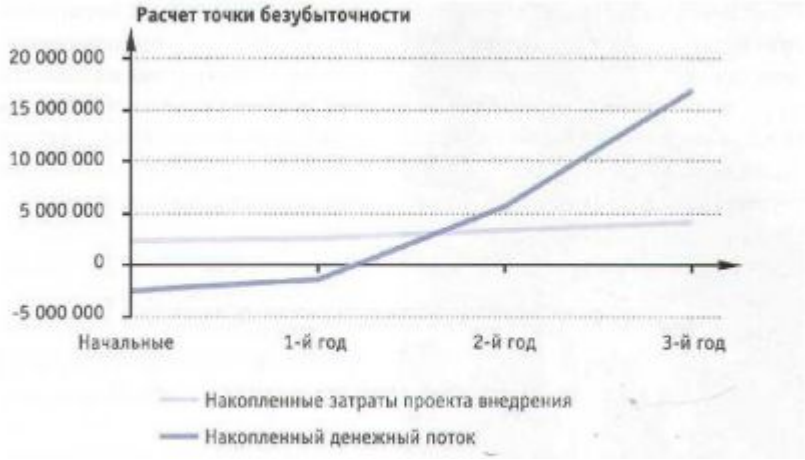
Расчет показателей возврата инвестиций на систему информационной безопасности для «МЭИ»

Показатели	Начальные затраты, руб.	1 год, руб.	2 год, руб.	3 год, руб.	Общее, руб.
Затраты на внедрение	2 358 048	369 785	707 414	707 414	4 142 661
Накопленные затраты проекта внедрения	2 358 048	2 727 833	3 435 247	4 142 661	-
Ставка дисконтирования	14%	-	-	-	-
Чистая приведенная стоимость (NPV) затрат на проект внедрения	3 645 614	-	-	-	-
Текущий показатель TCO	п/а	26 383 744	26 383 744	26 383 744	79 151 232
Целевой показатель TCO	п/а	19 864 933	19 864 933	19 864 933	59 594 799
Фактический показатель TCO	п/а	25 079 982	21 820 576	19 864 933	-
Выгоды при оптимизации показателя TCO	0	1 303 762	4 563 167	6 518 811	12 385 740
Показатель ожидаемых потерь (ALE)	0	29 565 000	29 565 000	29 565 000	88 965 000
Эффективность системы корпоративной защиты	-	85%	85	85%	-
Ежегодные сбережения (AS)	0	50 268	3 309 674	5 265 317	
Показатель выгод при оптимизации показателя TCO и ежегодные сбережения	0	1 354 030	7 872 841	11 784 128	21 010 999
Накопленный показатель выгод при оптимизации показателя TCO и ежегодные сбережения	0	1 354 030	9 226 871	21 010 999	-
Денежный поток	- 2 358 048	984 245	7 165 427	11 076 714	16 868 338
Чистая приведенная стоимость (NPV) доходов от проекта внедрения	- 2 358 048	- 1 373 803	5 791 624	16 868 338	-
Чистая приведенная стоимость (NPV) доходов от проекта внедрения	10 577 426	-	-	-	-
Внутренняя норма рентабельности (IRR)	145%	-	-	-	-

Расчет точки безубыточности проекта внедрения системы информационной безопасности

Точка безубыточности = 1,6 лет.

Проект внедрения можно считать экономически выгодным, так как чистая приведенная стоимость доходов от проекта внедрения положительна и больше чистой приведенной стоимости затрат на проект внедрения в 2,9 раза.



Yandex Cloud

Одной из широко распространенных платформ является Yandex Cloud

Yandex Cloud

Основные возможности данной платформы:

– бэк-офисная платформа – облачные справочные системы;

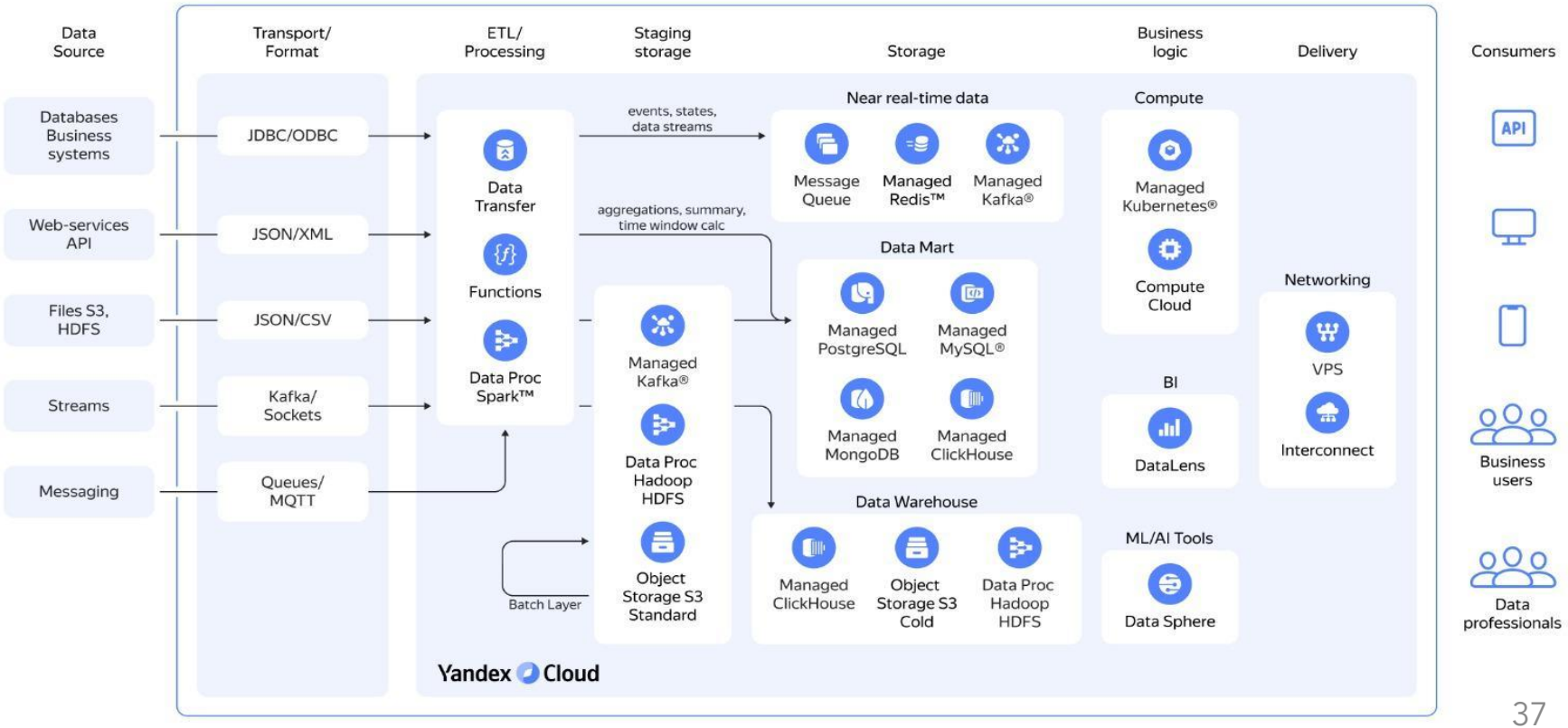
– цифровая инфраструктура и информационная безопасность – сервисы защиты от спама;

– 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.
5. Произведен расчет экономической эффективности рисков на примере «МЭИ»

Спасибо за внимание!

Москва-2023