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

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 информационных рисков и экономической эффективности;
4. Изучить использование облачных сервисов;
5. Осуществить экономический анализ работы с облачными хранилищами.

Актуальность

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

Риски при защите информации в облачных сервисах

К основным рискам при защите информации в облачных сервисах относятся:

- Утечка данных
- Потеря данных

Существует множество информационных рисков

- Несанкционированный доступ к данным
- Недостаточная защита от вредоносного программного обеспечения

1. Вредоносное ПО.
2. Кросс-облачная атака.
3. Атака по боковому каналу.
4. Отказ в обслуживании (DoS, DDoS).
5. Атака на вычислительные ресурсы.
6. Техники социальной инженерии.
7. Небезопасный API.

8. Кража или утечка логинов и паролей от аккаунта в облаке.

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) – **универсальный метод**, на базе которого были посчитаны все 4 основных риска

Преобразование вероятности угроз к ежегодной частоте TRA

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 страховой компании «МАКС»

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 страховой компании «МАКС»

№	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
	ИТОГО	3 435 247

Период окупаемости инвестиционных проектов, связанных с внедрением информационных технологий, не должен превышать трех лет, поэтому период оценки эффективности данного проекта внедрения равен трем годам

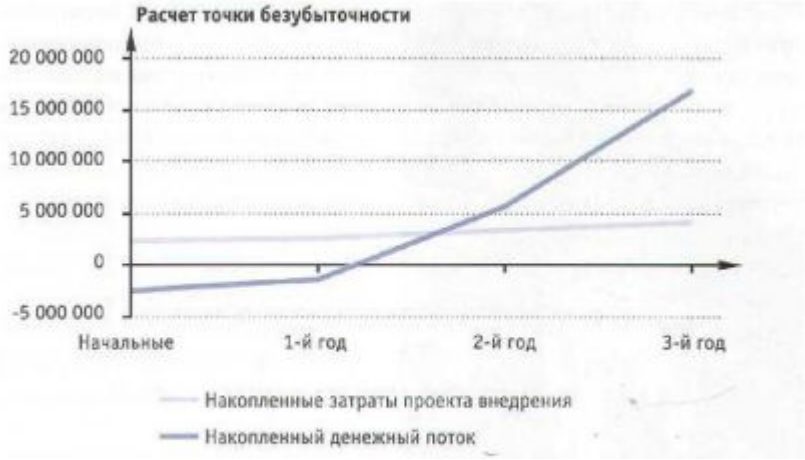
Расчет показателей возврата инвестиций на систему информационной безопасности для страховой компании «МАКС»

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.

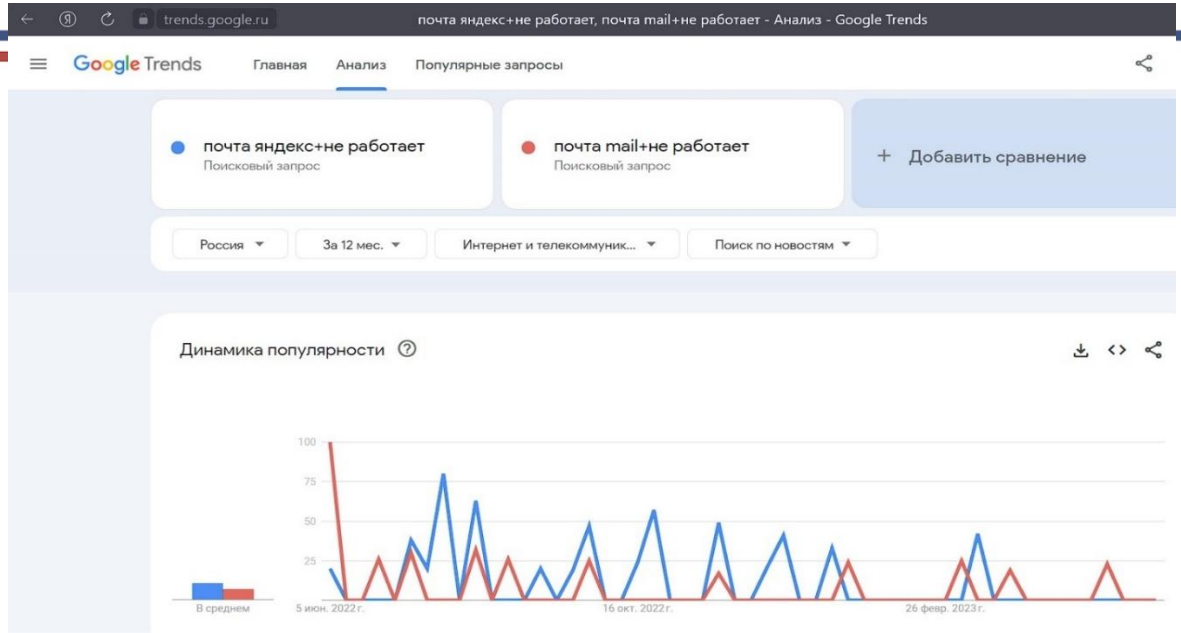
Проект внедрения можно считать экономически выгодным, так как чистая приведенная стоимость доходов от проекта внедрения положительна и больше чистой приведенной стоимости затрат на проект внедрения в 2,9 раза.



Типы контрмер безопасности

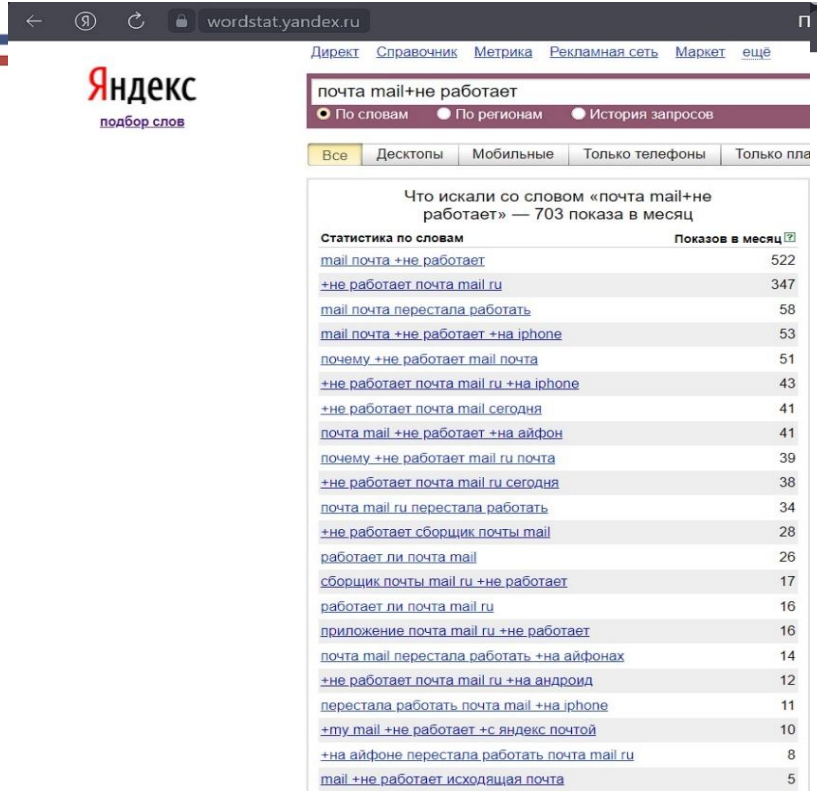
Тип контрмеры	Пример
Профилактические	1. Стандарты, процедуры, должностные инструкции 2. Аудит системы безопасности 3. Сетевые экраны 4. Системы обнаружения вторжений 5. Антивирусы 6. Средства шифрования 7. Формирование архивов
Лечебные	Резервные режимы работы
Принадлежат обоим типам	1. Планирование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

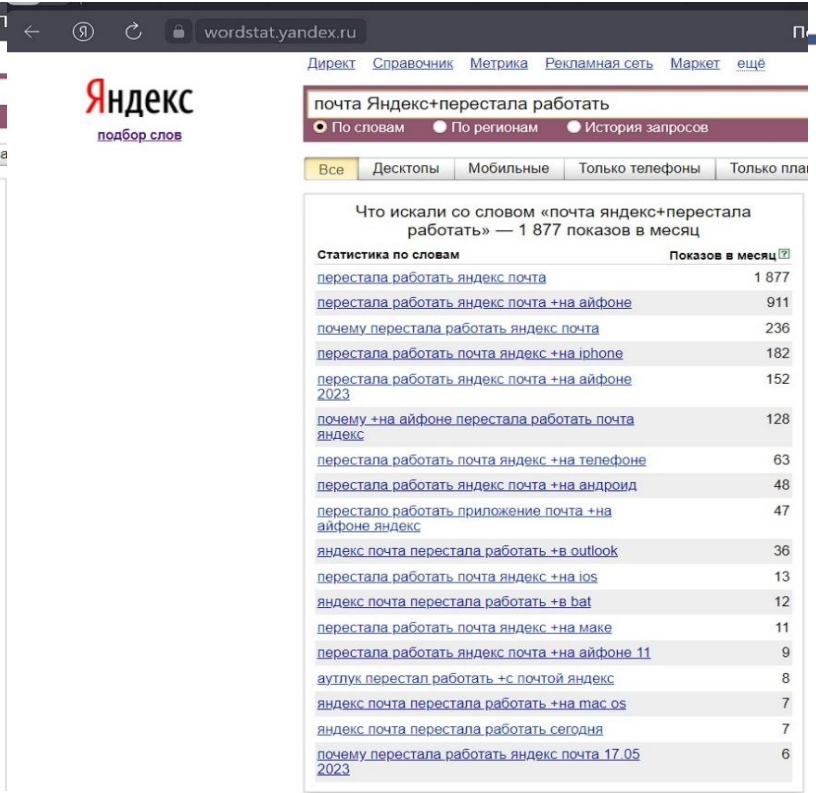
Динамика популярности запроса в Google Trends «**почта** mail.ru + **перестала работать**» **и** «**почта яндекс**+ **перестала работать**»



Вывод: почта mail.ru довольно часто дает сбои, в последнее время, и нельзя забывать про размер этих компаний и соотносить его с количеством результатов

Wordstat
«**почта** mail.ru + **перестала работать**» **и** «**почта яндекс+ перестала работать**»





За сутки в почту mail входять 2.5 млн. человек по сровнению 63.4 млн в яндекс

Уровни риска

Уровень важности	Описание	Балл
Незначительный	«не работает в bat», «не работает сегодня», «работает ли»	1
Средний	«не работает на айфоне», «на телефоне», «на IOS» (плавающий 2-3)	2
Высокий	«Почта не работает», «перестала работать», «перестала работать в Outlook», «сборщик почты не работает», «не работает исходящая почта»	3

Получаем «mail почта» 3 836 против 380 у «Яндекс почта»

Оценка несистемных рисков для страховой компании «МАКС» и рекомендации

В качестве оценки риска предлагается **подход оценивания на основе мнения аудитории**.

С помощью Google Trends **и** Wordstat произведена оценка потенциальных несистемных рисков в работе облачного сервиса с точки зрения пользовательской аудитории путём анализа интенсивности запроса по ключевым словам.

Т.к. риск оказался высоким сформулированы безопаснее будет Перейти с mail.ru на более безопасный сервис, например, Яндекс.

Применимый мной подход является универсальным, его можно применить и на других организациях для того, чтобы оценить риски и возможность перехода к облачным сервисам.

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 информационных рисков и экономической эффективности;
4. Изучено использование облачных сервисов;
5. Произведен расчет экономической эффективности рисков на примере страховой компании «МАКС».

Спасибо за внимание!

Москва-2023