Определение риска технологий

РИСК ТЕХНОЛОГИЙ – это риск возникновения прямых или косвенных убытков в результате недоступности ИТ-систем, некорректности настроек и работы алгоритмов, нарушения качества и целостности данных, нарушений в работе подрядчиков и партнеров и ошибок при разработке и обновлении ИТ-систем.

Европейская банковская организация[1]
определяет пять основных категорий риска технологий

Риск ИТ разработки и обновления систем

Риск нарушения качества и целостности данных

Риск кибербезопасности

Риск недоступности ИТ систем

Риск подрядчиков и партнеров

1) European Banking Authority, EBA

Сбой торгового алгоритма Knight

Американская глобальная финансовая фирма, занимающаяся созданием высокочастотных торговых алгоритмов. Knight стал крупнейшим трейдером на американских акциях, с долей рынка 17,3% на NYSE и 16,9% на NASDAQ

1 августа 2012 года на промышленном стенде был обновлен алгоритм HFT- системы (High Frequency Trading). Алгоритм содержал дефект. В результате система в течение 40 минут осуществляла сотни заявок в секунду на покупку и продажу акций.

Суммарный убыток компании составил 440 млн. долларов. Акции упали на 66%, и компания была поглощена другим участником рынка

Количественная оценка риска позволяет эффективно тратить ресурсы команд

СБЕРБАНК

Оценка рисков в измеримых метриках позволяет

- Сравнивать риски между собой и брать в работу те, которые наносят максимальный ущерб в случае из реализации
- Сравнивать задачи рисков технологий с другими задачами бэклога
- Установить лимит на объем риска. Исполнение лимита включить в KPI Product Owner

Риск ИТ разработки и обновления систем

СБЕРБАНК

Риск, связанный с неспособностью организации надлежащим образом управлять и контролировать ИТ изменения (в текущей деятельности/в рамках изменений)

Причины

- Нарушение стандартов при разработке ПО
- Большой накопленный технический долг на АС
- Сложность и связанность релизов в интегрированных АС

Метрики оценки

- Вероятность сбоя после релиза
- Вероятность дефекта после релиза

Как используется оценка?

- Блокировка релизов с высокой вероятностью сбоев/дефектов
- Предоставление командам аналитики о факторах, влияющих на вероятность, для возможности снижения рисков

Обвал сети AT&T

СБЕРБАНК

5 января 1990 года в США около 75 миллионов звонков остались без ответа. Случилась ошибка одного из колл-центров телефонного оператора AT&T, который сперва отключился сам, а затем, после перезагрузки, отключил и оставшиеся 113 центров.

Сбой произошёл во время очередного обновления релиза, из-за одной неверной строчки кода в которой реализовывалась отправка сигнала.

Дефект в коде EDS

СБЕРБАНК

В 2004 году компания EDS разработала систему автоматизированного учёта для Агентства Помощи Детям (CSA) Великобритании.

В результате ошибки кода ПО 1,9 миллиона человек получили повышенные пособия, 700 тысяч — пониженные, часть детей оказалось без пособий вовсе, а несколько десятков тысяч бесследно удалены из базы данных.

Ущерб составил 539 миллионов фунтов

Риск недоступности ИТ систем

СБЕРБАНК

Риск того, что отказ аппаратных или программных компонентов ИТ, недочеты в организации управления ИТ или любое другое событие негативно скажутся на производительности и доступности ИТ систем и/или данных

Причины

- Сбои серверной инфраструктуры
- Сбои сетевого оборудования
- Дефекты прикладного ПО
- Влияние внешних сервисов

Метрики оценки

- Минуты потенциального простоя
- Потерянные операции
- Потери CLTV из-за влияния на клиентов

Как используется оценка?

- Определяем системы с максимальным уровнем ущерба в случае сбоев
- Лимитируем потенциальный простой и ущерб от недоступности – устанавливаем аппетит к риску
- Устраняем и защищаемся от рисков, превышающих аппетит

Сбой аутентификации Google

СБЕРБАНК

14 декабря 2020 года, в течении 47 минут клиентские сервисы Google, требующие доступа Google Oauth, были недоступны.

Основной причиной была проблема в автоматизированной системе управления квотами (дефект при миграции службы идентификаторов), которая уменьшила емкость центральной системы управления идентификацией Google, заставив ее возвращать ошибки по всему миру

В результате инцидента, облачная платформа Google и Google Workspace столкнулись с глобальным отключением всех сервисов, требующих аутентификации учетной записи Google в течении 47 минут.

Риск нарушения качества и целостности данных

СБЕРБАНК

Риск неполноты, неточности или непоследовательности данных, хранящихся и обрабатываемых
в ИТ системах, в результате чего снижается качество предоставления услуг клиентам, предоставления корректной и своевременной финансовой информации

Причины

- Искажение данных при интеграции систем
- Отсутствие контроля над правильностью работы с данными, выполняемых в промышленных средах ИТ-систем.
- Ненадлежащий контроль изменений данных при разработке ИТ-систем

Метрики оценки

- Критичность объекта данных
- Индекс здоровья данных

Как используется оценка?

- Для определения требуемых мер защиты от искажения данных в зависимости от критичности данных

Падение Mars Climate Orbiter

Спутник «Mars Climate Orbiter» 23 сентября 1999 года должен был перейти на круговую орбиту Марса. Через 5 минут MCO запланировано ушел за Марс. Из анализа данных было предположено, что аппарат прошел над поверхностью Марса на высоте 57 км вместо расчетных 110 км и распался в атмосфере.

Компания, которая работала над инженерными задачами, не выполнила преобразования английских единиц измерения в метрическую систему.

Ущерб 125 млн долларов

Риск подрядчиков и партнеров

СБЕРБАНК

Риск того, что привлечение третьей стороны для разработки/ внедрения ИТ систем или связанных с ними услуг, приведет к снижению эффективности деятельности и качества управления рисками

Причины

- Концентрация на одном вендоре
- Отсутствие оценки влияния и проработки мер в случае реализации рисков вендора/аутсорсинга
- Отсутствие мониторинга вендора как контрагента

Метрики оценки

- PD вендора
- Доля контрактов вендора
- Количество ИТ вендоров с негативным новостным фоном
- Количество критичных систем с зависимостью от ИТ вендора

Как используется оценка?

- В закупочных процедурах
- Для постановки критичных подрядчиков на новостной мониторинг

Запуск платформы HealthCare.gov

СБЕРБАНК

HealthCare.gov

Портал государственного страхования в США healthcare.gov. Создавался под реформу Obamacare для продаж полисов обязательного страхования, был запущен в октябре 2013 года. При запуске портала пользователи столкнулись с большим проблем как недоступности портала, так и некорректного его функционирования

Над разработкой платформы работало около 70 подрядных организаций. Каждая из них протестировала свою часть, а полное интеграционное тестирование организовано не было

Репутационный ущерб – инцидент вызвал широкий резонанс. 21 октября 2013 года Президент США Барак Обама лично принес извинения пользователям

Риск кибербезопасности

Риск того, что отсутствие мер защите систем, сетей и программных приложений от цифровых атак, приведет к потере доступа к конфиденциальной информации, ее изменению и уничтожению

Причины

- Отсутствие безопасности данных, новых технологий
- Наличие вредоносного ПО и уязвимостей
- Сложная большая интеграция с другими системами

Метрики оценки

- Доля своевременно устраненных уязвимостей
- Объем данных под риском

Как используется оценка?

- Контроль рисков КБ при запуске новых продуктов/процессов
- Контроль рисков КБ при внедрении новых релизов
- Для постановки задач в части патч менеджмента и работ с уязвимостями

Утечка Estee Lauder

В феврале 2020 года у Транснациональной косметической компании Estee Lauder «Увели» 440 миллионов записей. Все похищенные данные преступники выгрузили на открытых ресурсах интернета.

Причиной инцидента стала не защищенная паролем база данных

В результате инцидента, злоумышленники взяли:

- 440 336 852 записей

– Журналы производства, аудита, ошибок, CMS и промежуточного ПО

- Ссылки на отчеты и другие внутренние документы

- IP-адреса, порты, пути и информация о хранилище

Выводы

СБЕРБАНК

- Количественная оценка рисков технологий возможна и полезна
- Для оценки можно использовать не только денежную оценку
- Лимит на риск дает возможность Product owner управлять своим бэклогом в пределах заданных лимитов

Вопросы?

СБЕРБАНК

Контакты

Лукьянов Михаил Станиславович
Управляющий директор – Начальник центра
Центр управления рисками технологий