Облака в банках: где проходит граница допустимого риска?

Товстолип Александр,
Ассоциация ФинТех
2026

Ассоциация ФинТех

14 ЧЛЕНЫ АФТ

Банк России
ВТБ
СБЕР
Альфа Банк
ГАЗПРОМБАНК
НСПК
ПСБ
ВСК страховой дом
РСХБ | ЦИФРА
MOEX GROUP
Т БАНК
Райффайзен БАНК
ДОМ РФ
СОВКОМБАНК

24 АССОЦИИРОВАННЫЕ ЧЛЕНЫ

Avito
base alt
Яндекс
МКБ
+|TI
МТС
Кредит Европа Банк
РЕСО гарантия
Ак Барс Банк
DIASOFT всё по-настоящему
БАНК ЦЕНТР-ИНВЕСТ
YADRO
РЕДСОФТ
отпбанк
АЛЬФА СТРАХОВАНИЕ
БПС инновационные решения
ДОХОДЪ управляющая компания
FLEX software systems
синара банк
билайн бизнес
ВБРР
Ростелеком
точка банк для предпринимателей и предприятий
КАПИТАЛ LIFE страхование жизни

Облака – новая инфраструктура финансового сектора

Банки сталкиваются с:

- ростом скорости цифровой трансформации;
- ростом киберугроз;
- требованиями регуляторов;
- ожиданиями клиентов (24/7);
- необходимостью оптимизации затрат.

Облачная инфраструктура помогает решить ряд задач организации.

Облака стали **инфраструктурой цифровой конкуренции.**

Для банков вопрос миграции в облака уже решен рынком!

Какой риск банк готов принять ради скорости и эффективности?

Почему тема критична для банков?

Особенность банковского сектора

- высокая концентрация критичных данных;
- зависимость от непрерывности сервисов;
- строгие требования compliance;
- повышенное внимание регуляторов.

Для банков любой технологический риск становится:

- операционным риском;
- финансовым риском;
- регуляторным риском;
- репутационным риском

Вопрос не в том, безопасно ли облако. Вопрос в том, способен ли банк управлять новыми типами рисков, которые облако приносит.

Основные риски публичных облаков для банков

01. Потеря прямого контроля

- ограниченная видимость;
- зависимость от процессов провайдера;
- сложность независимого аудита.

02. Концентрационный риск

- множество банков используют одних гиперскейлеров;
- сбой провайдера становится системным риском.

03. Риски третьих сторон

- облачный провайдер становится частью критичной инфраструктуры банка.

04. Управление данными

- хранение данных;
- управление ключами;
- доступ к телеметрии.

05. Скорость изменений

- растет скорость изменений
- растет поверхность атаки.

Тепловая карта рисков

		Операционные риски						
R1. Регуляторные риски	**R2. Кредитные риски**	**R3. Риски информационной безопасности**	**R4. Правовые риски**	**R5. Риски информационных систем**	**R6. Системные риски**	**R7. Коммерческие риски**	**R8. Риск аутсорсинга**	**R9. Риски потери деловой репутации**
R1.1 Ограничение законодательства в деятельности кредитных организаций в части передачи и хранения сведений, составляющих банковскую тайну, в облачных сервисах	R2.1 Неисполнение/ некачественное исполнение обязательств Провайдером по причине его плохого финансового положения (в тч банкротство).	R3.1 Риск некорректного разделения зон ответственности и недостаточного контроля уязвимостей в области информационной безопасности	R4.1 Риск неопределённости и ограниченности ответственности сторон при инцидентах в облачной среде.	R5.1 Риск отсутствия экспертизы для работы с новыми технологиями (ИИ и т.п.)	R6.1 Риск концентрации - концентрация пользователей-финансовых организаций у одного Провайдера. В случае возникновения сбоя/нарушения информационной безопасности на стороне Провайдера под угрозой финансовая инфраструктура	R7.1 Появление избыточной стоимости сервисов в облаке	R8.1 Риск ошибок или ненадлежащего исполнения при передаче функций, операций, услуг или процессов третьим лицам.	R9.1 Репутационные риски, возникающие при реализации инцидентов
R1.2 Ограничения законодательства в области НФО в части конфиденциальных сведений может стать барьером для размещения отдельных видов сведений в облачном сервисе.		R3.2 Нарушение целостности или конфиденциальности информации, хранящейся в облаке, по вине Провайдера (Доступ к конфиденциальной информации неуполномоченных лиц, риски цепочки поставок, утечки конфиденциальной информации, модификация/ удаление данных и т.д.)		R5.2 Риск нарушения доступности облачных сервисов по вине Провайдера				
R1.3 Неполная адаптированность текущего нормативного обеспечения к облачной платформе				R5.3 Риск нарушения доступности сервисов из-за сбоев у поставщиков каналов связи				
R1.4 Невыполнение требований регуляторов и стандартов при эксплуатации облачных сервисов								

Уровень риска (экспертная оценка):

- Высокий
- Средний
- Низкий

Облака меняют модель контроля

Облако меняет не только инфраструктуру, оно меняет модель контроля

Традиционная модель	«Облачная» модель
Инфраструктура внутри периметра	Инфраструктура у провайдера
Полный физический контроль	Разделяемая ответственность
Предсказуемые изменения	Постоянные изменения
Локальные зависимости	Экосистемные зависимости

Облако не убирает риски — оно перераспределяет их.

Разделяемая ответственность – кто за что отвечает?

Провайдер отвечает за:

- физическую инфраструктуру;
- базовую доступность;
- часть платформенных сервисов.

Банк отвечает за:

- доступы;
- конфигурации;
- данные;
- мониторинг;
- IAM;
- incident response;
- compliance.

Разделяемая ответственность часто воспринимается как разделяемая подотчетность.
Но ответственность перед клиентом и регулятором остается у банка!

Граница допустимого риска

Где проходит граница допустимого риска?

Граница определяется не технологией, а зрелостью процессов управления рисками.

Вопросы, которые должен задавать банк:

- Что произойдет при отказе облачного провайдера?
- Как быстро восстановится сервис?
- Возможно ли быстрое перемещение workload?
- Кто контролирует ключи шифрования?
- Кто реально видит данные и логи?
- Как проводится независимый аудит?

Критичные зоны контроля CISO

Банк должен сохранять контроль над:

- IAM и привилегированным доступом
- криптографическими ключами
- мониторингом
- управлением инцидентами
- управлением рисками
- политиками доступа к данным

Можно аутсорсить инфраструктуру.

Нельзя аутсорсить ответственность!

CISO – участник бизнес-трансформации.

Задачи CISO раньше

- защита периметра;
- контроль инфраструктуры;
- аудит изменений.

Задачи CISO сейчас

- управление киберриском;
- участие в разработке и тестировании «облачной» архитектуры;
- управление third-party risk;
- взаимодействие с советом директоров;
- обеспечение киберустойчивости.

Сегодня CISO отвечает **за устойчивость цифрового бизнеса.**

Что помогает банкам управлять рисками применения публичных облаков?

Практика зрелых организаций

- единая стратегия безопасности в облаке;
- регулярные штабные учения;
- независимая оценка готовности к облачным киберугрозам;
- постоянный контроль конфигураций;
- сегментация и минимальные привилегии;
- тестирование сценариев восстановления;
- прозрачные SLA и аудит прав.

Выводы

01 Облака уже не эксперимент для банков.

02 Главный риск — не технология,
а отсутствие зрелого процесса управления.

03 Безопасность облака —
это не compliance-проект.

04 Конкурировать будут банки, которые
умеют сочетать скорость, устойчивость,
инновации и управление рисками.

Спасибо за внимание!

Товстолип Александр

Руководитель Управления информационной безопасности

tg: @mydzen

a.tovstolip@fintechru.org

Telegram - канал

Мой контакт в Макс