

Инфобез в облаке
Риск и возможность

Начальник отдела внедрения средств
защиты ифнормации блока ИБ
Павел Мошкин

Проблемы облака для финансовых организаций

Требования регуляторов

- Требования Банка Росси
- ГОСТ Р 57580
- ГОСТ Р 57580.1-2017
- Требования ФСТЭК России
- Требования ФСБ России

Зоны ответственности

- Разграничение зон ответственности администраторов платформы и заказчика
- Проработанные SLA
- Адаптация под архитектуру банка
- Разграничение доступа к данным

Интеграция СЗИ

- Возможность интеграции BareMetal СЗИ
- Интеграции СЗИ в инфраструктурный слой платформы
- Интеграция NGFW

Возможность построения изолированной инфраструктуры

- Выделение отдельных физических кластеров
- Изоляция узлов хранения и вычисления на уровне L2

Контроль действия администраторов

- Интеграция с PAM и IAM решениями
- Доступ к событиям аудитов безопасности инфраструктуры

Интеграция с SOC

- Получение событий всех уровней
- Интеграция с инфраструктурой платформы

Привлечение технологического партнёра: сервис «Безопасное облако»



1. Платформа Астра (Astra Cloud platform) выступает технологическим слоем, на который опираются остальные сервисы. Безопасное облако предполагает формирование отдельных частных облаков для Заказчика. Такой каркас упрощает масштабирование сервисов и удерживает единые стандарты управления для группы Банка.

2. Интеграция средств защиты информации и источников событий ИБ по умолчанию позволяет видеть весь жизненный цикл инцидента в одной среде. Это снижает разрозненность инструментов и делает управление прозрачным для специалистов по ИБ.

3. Увеличение вычислительных мощностей и хранилищ позволяет без остановки сервисов обеспечивать потребности по масштабированию инфраструктур Заказчиков, а также обеспечивать масштабирование хранилищ событий и средств защиты информации. За счёт этого можно наращивать мощности и покрытие СЗИ.

Концепция «Безопасного облака»

Гибридная инфраструктура под любую нагрузку

Гибридная платформа, комбинирующая облачные технологии и наложенные средства защиты информации

Российская технологическая база

Используется исключительно отечественное оборудование и программное обеспечение — полная независимость от иностранных решений

Безопасность, встроенная в архитектуру

Механизмы защиты информации являются неотъемлемой частью инфраструктуры

Постоянный контроль состояния

Обеспечивается круглосуточный мониторинг доступности всех системных компонентов и резервное копирование данных

Соответствие требованиям регулятора

Инфраструктура облака спроектирована с учётом требований к защите персональных данных и критической информационной инфраструктуры



Сервисы ИБ в «Безопасном облаке»

SOC

VM

WAF

EASM

CLOUD

Iaas

MAIL

Saas

1C

Saas

DISC

Saas



АСТРА | ПСБ

Спасибо за внимание!

