Вверх по наклонной за облаками

Банкиры ожидали легализации публичных облаков долгие годы. За это время ИБ-регулирование в финансовой сфере серьезно усилилось по сравнению с сервис-провайдерами. Готовы ли они подняться до требований ЦБ?

Текст
ВАДИМ ФЕРЕНЕЦ,
ОБОЗРЕВАТЕЛЬ **«Б.О»**

В ходе сессии «Аутсорсинг на финансовом рынке: оптимизация расходов или новые риски?» в рамках прошедшего в феврале 2023 года Уральского форума «Кибербезопасность в финансах» в Екатеринбурге стало известно о планируемом изменении подхода к обороту информации и ее защите, что может открыть дорогу IT-аутсорсингу для всего финансового сектора.

Законопроект, разрабатываемый Банком России, вызвал энтузиазм, но также и озабоченность. «Б.О» в этой связи задал нескольким сервис-провайдерам вопросы, касающиеся их отношения к наиболее острым проблемам, в частности к возможному изменению бизнес-моделей для обеспечения информационной безопасности в новых условиях.

Границы ответственности

«Опираясь на практику организации работ в соответствии с другими стандартами, в том числе ЦБ, мы считаем, что ожидать серьезной реорганизации бизнес-моделей не стоит. В случаях предоставления сервисов банковскому сектору в соответствии с актуальными требованиями речь, скорее всего, будет идти о выполнении дополнительных требований в части безопасности и о заключении новых соглашений с банками — заказчиками услуг. Какой-то особенной новизны в моделях совместной ответственности нет — примерно так же работает закон о персональных данных при поручении обработки третьему лицу, включая сервис-провайдеров», — высказал свое мнение **Константин Анисимов,** директор по развитию инфраструктурных продуктов российской

технологической компании Selectel, предоставляющей облачные инфраструктурные сервисы и услуги дата-центров.

Границы ответственности достаточно строго регламентируются стандартами по ИБ. При этом уже сейчас для большинства IT-систем финансовых организаций, размещенных в публичных облаках, ответственность в части информационной безопасности распределена между облачным провайдером-партнером и финансовой организацией.

«Мы видим, что дальше все больше частей (слоев) IT-систем будет передаваться на аутсорсинг. Это общая тенденция во всем мире, и в РФ мы, скорее всего, пойдем таким же путем. Финансовые организации должны фокусироваться на основном для себя бизнесе, а все непрофильное отдавать профессионалам», — считает Константин Анисимов.

Кто и что регулирует в облаках?

Однако список нормативных актов, которые требуется выполнять, выглядит весьма впечатляюще, впрочем, как и перечень регуляторов.

Как можно описать взаимоотношения ИБ-регуляторов и провайдеров? По мнению экспертов «Б.О»: «На базовом уровне облачные провайдеры как субъекты критической информационной инфраструктуры (КИИ) обязаны выполнять законодательство РФ о безопасности КИИ. В этой сфере действуют три основных регулятора: ФСТЭК — в части предъявления требований и их государственного контроля, ФСБ — в части обнаружения, предупреждения и реагирования на компьютерные атаки, а также Минцифры».

При этом обеспечение безопасности КИИ регулируется Федеральным законом № 187-ФЗ от 26.07.2017 «О безопасности критической информационной инфраструктуры Российской Федерации» и другими подзаконными актами.

Минцифры реализует отдельные регулирующие функции в отношении субъектов КИИ, являющихся операторами связи, к которым, как правило, и относятся облачные провайдеры. В этом случае провайдер обязан реализовывать положения Федерального закона № 126-ФЗ от 07.07.2003 «О связи» и подзаконных актов. Кроме того, облачные провайдеры являются субъектами ПДн, в связи с чем они обязаны выполнять соответствующие нормы Закона № 152-ФЗ от 27.07.2006 «О персональных данных».

Помимо этого заказчики могут предъявлять к провайдеру и его облачной инфраструктуре дополнительные требования по информационной безопасности, в частности требования о защите информации, не составляющей государственную тайну, содержащейся в государственных информационных системах, утвержденные Приказом ФСТЭК № 17 от 11.02.2013, а также требования ГОСТ Р 57580.1-2017 «Безопасность финансовых (банковских) операций. Защита информации финансовых организаций. Базовый состав организационных и технических мер».

Эксперты «Б.О» добавили от себя еще несколько возможных требований по ИБ, которые так или иначе дадут о себе знать владельцам облаков. Это требования, содержащиеся в законах № 63-ФЗ от 06.04.2011 «Об электронной подписи» (с правками и дополнениями) и № 536-ФЗ от 19.12.2022 «О внесении изменений в отдельные законодательные акты РФ». Это также требования к подключению кредитной организации к среде Open Banking посредством технической сертификации IT-инфраструктуры банка в качестве участника среды открытых банковских интерфейсов в роли поставщика платежных услуг и к использованию ИБ-протокола ФАПИ.СЕК. Недавний проект банка МКБ в этой сфере «Б.О» описал в материале «Open API: от малого бизнеса до космоса».

Open API: от малого бизнеса до космоса

Одной из инициатив, близкой к трансформации в нормативный акт, является приведение к нынешней реальности законодательства в области архивного дела и переводу его полностью в электронную форму. В частности, по этому поводу на ПМЭФ-2022 ярко выступила **Ольга Скоробогатова,** первый заместитель председателя Банка России.

А еще на подходе цифровой рубль, ЦФА, перезапуск ЕБС, удаленная видеоидентификация и т.д.

Еще раз о бизнес-моделях

Приведенный список требований по ИБ к облачному сервис-провайдеру, очевидно, сможет реализовать далеко не каждый из них. Поэтому в своих ответах опрошенные гораздо чаще, чем ранее, предлагали в дополнение к предложениям **Анатолия Козлачкова,** вице-президента Ассоциации банков России, о разделении ответственности (или вместо них) перейти к практике страхования киберрисков, что выглядит крайне актуально в свете возможного ввода оборотных штрафов за утечки персональных данных.

Все это на одной чаше весов. А что может получить взамен облачный провайдер в качестве поставщика услуг банкирам? Есть ли что предложить им прямо сейчас?

По мнению Константина Анисимова, спешить не следует: «Наиболее интересные решения для компаний enterprise-уровня в финансовой сфере сейчас — это частное облако и аттестованный сегмент ЦОД».

Частное облако — это полностью изолированная от других клиентов виртуальная инфраструктура. Как утверждают в Selectel, существует возможность по требованию клиента привести его в соответствие с любым стандартами, характерными для публичной инфраструктуры: ГИС К1, ИСПДн УЗ-1, PCI DSS и др. Частное (или гибридное) облако более гибкое с точки зрения ресурсов: клиент может не ограничиваться конфигурациями оборудования, как в кластерах у публичного облака.

Аттестованный сегмент ЦОД — это физически и логически изолированный от других клиентов и сетей сегмент, соответствующий всем основным стандартам и требованиям безопасности (152-ФЗ по УЗ-1, ГИС К1, GDPR, PCI DSS и др.). Доступ к нему есть только у клиентов и сертифицированных технических специалистов провайдера. Данный подход позволяет ИБ-специалистам компании-заказчика самим контролировать политики безопасности и управлять ими. Такое решение обеспечивает максимальную защиту биометрических и финансовых данных. Б.О