ЭКСПЕРТНО-АНАЛИТИЧЕСКОЕ ЗАКЛЮЧЕНИЕ ПО ПРАВОВЫМ ОСНОВАМ ОРГАНИЗАЦИИ И ФУНКЦИОНИРОВАНИЯ РЫНКА IT-АУТСОРСИНГА В БАНКОВСКОЙ СФЕРЕ

Москва

2023

ЭКСПЕРТНО-АНАЛИТИЧЕСКОЕ ЗАКЛЮЧЕНИЕ ПО ПРАВОВЫМ ОСНОВАМ ОРГАНИЗАЦИИ И ФУНКЦИОНИРОВАНИЯ РЫНКА IT-АУТСОРСИНГА В БАНКОВСКОЙ СФЕРЕ

Настоящее экспертно-аналитическое заключение (далее – Заключение) подготовлено в связи с обращением Ассоциации банков России (далее – Заказчик) Белицкой Анной Викторовной, доктором юридических наук, профессором кафедры предпринимательского права Юридического факультета МГУ имени М.В. Ломоносова и Лаутс Елизаветой Борисовной, кандидатом юридических наук, доцентом кафедры предпринимательского права Юридического факультета МГУ имени М.В. Ломоносова, руководителем НОЦ «Центр правовых исследований в сфере банковской деятельности» Юридического факультета МГУ имени М.В. Ломоносова.

Цель исследования

Создание комплексной модели правоотношений, возникающих при создании рынка IT-аутсорсинга в банковской сфере Российской Федерации.

Условие построения модели

Построение и описание модели правоотношений базируется на том, что в законодательстве отсутствуют ограничения на передачу персональных данных, а также сведений, защищаемых режимом банковской тайны.

Базовое понятие

Под IT-аутсорсингом понимаются услуги, связанные с хранением, передачей и обработкой информации в соответствующих информационных системах и их компонентах, необходимые для осуществления банковских операций, которые оказываются кредитным организациям специально привлеченными для этих целей третьими лицами. Услуги могут оказываться на условиях как использования облачной архитектуры, так и иными способами.

Задачи исследования

1. Определение общей схемы правоотношений, которые могут возникнуть на рынке IT-аутсорсинга.

1.1. Определение основных субъектов правоотношений на рынке IT- аутсорсинга на основании выделенных IT-функций (Дополнение №1 к Техническому заданию).

1.2. Архитектура правоотношений между основными субъектами рынка IT-аутсорсинга:

1) в зависимости от создания компании IT-аутсорсера, предоставляющей услуги по всем или большинству IT-функций (модель универсального посредника);

2) в зависимости от передачи отдельных IT-функций банка разным лицам (модель множественности аутсорсеров);

1.3. При построении модели необходимо учитывать (и отразить в конструируемой модели):

1) возможную роль страховых компаний в общей архитектуре правоотношений между основными субъектами рынка IT-аутсорсинга;

2) возможное возникновение необходимости осуществления взаимодействия IT-аутсорсера с регулирующими органами вследствие передачи ему от банка соответствующей информации.

2. Рекомендации по определению оптимальной организационно-правовой формы компании-аутсорсера при модели универсального посредника (по результатам анализа по вопросам Таблицы№1 к Техническому заданию), в том числе анализ преимуществ и недостатков для:

1) акционерного общества;
2) общества с ограниченной ответственностью;
3) кооператива;
4) союзов и ассоциаций.

2.1. Рекомендации по оптимальной модели корпоративного управления компании-аутсорсера.

2.2. Предложения по возможным вариантам формирования уставного капитала компании-аутсорсера, в том числе с участием средств:

1) Банка России (например, на момент организации лица с последующей постепенной продажей долей в капитале);
2) кредитных организаций;
3) разработчиков банковского ПО или иных субъектов рынка IT- аутсорсинга;
4) союзов и ассоциаций.

2.3. Определение ограничений на возможную организационно-правовую форму компании, исходя из необходимости получения лицензий и/или прохождения сертификаций, ориентируясь на перечень необходимых IT-функций.

3. Юридическая модель распределения ответственности в сфере IT- безопасности между пользователями информационных услуг, их клиентами и IT-аутсорсером: частно-правовой и публично-правовой аспекты. Указанная модель должна также включать распределение ответственности в сфере банковской деятельности за действия IT-аутсорсера.

4. Описание комплексной целевой модели правоотношений, возникающих при создании рынка IT-аутсорсинга в банковской сфере Российской Федерации, по итогам осуществленного анализа.

В целях исследования были проанализированы:

Иностранные и российские нормативные правовые акты, нормативные акты и программные документы, посвященные вопросам настоящего Заключения; правовая литература, судебная практика.

Краткие выводы

Анализ международной практики показал, что перечень услуг, которые могут быть переданы на аутсорсинг, оставляется регуляторами открытым. В законодательстве могут содержаться ограничения на

передачу существенных услуг на аутсорсинг. Ключевой принцип состоит в том, что банк должен гарантировать, что передача на аутсорсинг услуг не повлияет на его способность выполнять свои обязательства перед клиентами и публично-правовые обязанности.

Между субъектами IT-аутсорсинга могут быть заключены различные соглашения для достижения различных целей (например, договор поставки программного обеспечения и оборудования, договор возмездного оказания услуг для оформления аутсорсинга, договор аренды для использования элементов IT-инфраструктуры, договор на техническое обслуживание информационных и технических систем, договор о защите конфиденциальной информации и др.). В IT-сфере можно выделить транзакции, которые относятся к разовым или краткосрочным контрактам, и отношения, которые относятся к долгосрочным контрактам, договор аутсорсинга относится к последнему виду в отличие от услуг сервиса и поддержки, имеющих разовый, эпизодический характер и ограниченных временными рамками. Кроме того, транзакции могут быть ориентированы на затраты или на результат. Используя опцию затрат, компании закупают ресурсы у поставщиков, но напрямую управляют своей IT-деятельностью, при опции, ориентированной на результат, поставщики услуг самостоятельно управляют реализацией IT-деятельности. Архитектуру правоотношений между основными субъектами рынка IT-аутсорсинга составляют помимо договорной стадии также стадия предварительной комплексной проверки, а также стадии мониторинга и контроля, которые необходимы при передаче услуг на аутсорсинг в банковской сфере.

Действующее российское гражданское право не знает определения договоров аутсорсинга. С юридической точки зрения аутсорсинг представляет собой договор возмездного оказания услуг внешнего исполнителя - специализированной фирмы для выполнения ею определенной деятельности в пользу организации-заказчика, то есть

выполнение каких-либо функций, чаще всего непрофильных для организации. Как показывает международный опыт, важна форма заключения договора IT-аутсорсинга, а также необходимость сообщать о заключении такого договора в уведомительном порядке регулятору или необходимость получать одобрение регулятора на заключение такого договора. Различные страны устанавливают обязательные минимальные требования к условиям соглашений аутсорсинга. Такие требования обычно касаются предмета, срока, размере и порядке вознаграждения аутсорсера (зависимость от результата, абонентская плата и т.д.), условие о конфиденциальности, о том, кому будут принадлежать интеллектуальные права, о порядке пересмотра соглашения, установление срока, в течение которого осуществляется расторжение соглашения после принятия решения о раннем расторжении, чтобы обеспечить плавность передачи осуществления услуг и осуществить непрерывность реализации функции банка или финансовой организации.

Использование правового механизма страхования киберрисков в рамках договорных отношений между кредитной организацией и IT-аусорсером также может способствовать снижению большинства ключевых рисков: риска потери финансовой устойчивости (риск утраты контроля за функцией, системный риск), операционного риска (риск ошибки персонала, риск сбоя информационных систем, риск информационной безопасности), правового риска (комплаенс-риск, риск раскрытия конфиденциальной информации, риск нарушения договора с IT-аутсорсером, риск прекращения договора с IT-аутсорсером), репутационного риска (риск недобросовестных действий IT-аутсорсера). Однако очевидно, что минимизировать указанные риски киберстрахование сможет только при расширении страховых продуктов, предлагаемых страховыми организациями, что возможно в результате решения следующих правовых проблем: появления регулярной аналитики о киберинцидентах, закрепления в нормативных актах Банка

России права страховых организаций на получение обезличенных данных о кибератаках, а также установления единых методик анализа текущих угроз информационной безопасности и операционной надежности кредитной организации и IT-аутсорсера.

При определении основных субъектов на основании IT-функций можно выделить модель универсального аутсорсера и модель множественности аутсорсеров. Представляется, что в законодательстве не должны быть предусмотрены особые статусы субъектов IT-аутсорсинга при множественной модели (поставщики услуг, компании, отвечающие за информационную безопасность, провайдеры (поставщики) инфраструктуры. Модель множественности аутсорсеров понижает риск монополизации функции в руках одного аутсорсера, которого впоследствии будет сложно заменить, однако предполагает увеличение издержек, сложность организации контроля со стороны внутренних ресурсов банка. Недостатком же универсального поставщика является концентрации процессов в руках одной компании, что создает риск утраты контроля над функцией и риск создания конкурента на рынке. Однако при закреплении дополнительных требований к универсальному IT-аутсорсеру, в том числе по его правовому статусу можно минимизировать значительное количество рисков, тем более, что международные подходы требуют, чтобы банк обеспечивал те же стандарты при оказании услуг аутсорсеров, как если бы их оказывал банк.

Для построения оптимальной правовой модели универсального IT-аутсорсера в настоящем исследовании были выявлены гражданско-правовые (договорные), корпоративные (с учетом корпоративных и иных внутренних процедур в IT-аутсорсере и в кредитной организации-клиенте), а также публично-правовые средства минимизации ключевых рисков: риска потери финансовой устойчивости (риск утраты контроля за функцией, системный риск), операционного риска (риск ошибки

персонала, риск сбоя информационных систем, риск информационной безопасности), правового риска (комплаенс-риск, риск раскрытия конфиденциальной информации, риск нарушения договора с IT-аутсорсером, риск прекращения договора с IT-аутсорсером), репутационного риска (риск недобросовестных действий IT-аутсорсера, риск возникновения конфликта интересов), а также риск монополизации рынка (риск злоупотребления доминирующим положением на рынке, риск нарушения законодательства о защите конкуренции в форме недобросовестной конкуренции).

Очевидно, что необходимость осуществления взаимодействия IT-аутсорсера с регулирующими органами возникает в основном вследствие передачи ему от банка соответствующей, в том числе конфиденциальной, информации. Ключевыми рисками в данной сфере являются операционный и правовой, так как в рамках различных нарушений при осуществлении ключевых функций IT-аутсорсера (оказание услуг аутсорсинга ПО, инфраструктурных услуг, а также услуг в области безопасности) через реализацию рисков ошибок персонала, рисков сбоя информационных систем, рисков информационной безопасности может реализоваться риск раскрытия конфиденциальной информации.

Предоставление IT-аутсорсеру сведений, составляющих банковскую тайну, возможно только в случае прямого разрешения такой передачи в банковском законодательстве. При работе IT-аутсорсера с персональными данными необходимо выполнение ряда требований в данной сфере, которые зависят от вида персональных данных, с которыми работает IT-аутсорсер, а также от уровня угрозы им.

При передаче и обработке кредитной организацией информации, IT-аутсорсер должен выполнять требования защиты информации, не ниже, чем это установлено для кредитных организаций или некредитных финансовых организаций, а также лиц, оказывающих профессиональные услуги на финансовом рынке. Однако в отсутствие специального

регулирования в отличие от кредитных организаций IT-аутсорсер будет обязан привлекать организацию, имеющую лицензию на осуществление деятельности по технической защите конфиденциальной информации, для проведения работ и предоставления услуг, предусмотренных Положением о лицензировании деятельности по технической защите конфиденциальной информации.

В части рекомендаций по определению оптимальной организационно-правовой формы компании-аутсорсера при модели универсального посредника, в том числе анализа преимуществ и недостатков для союзов и ассоциаций, кооператива, общества с ограниченной ответственностью и акционерного общества, можно сделать следующие выводы.

Наибольшее количество преимуществ при меньшем количестве недостатков было выявлено применительно к организационно-правовым формам общества с ограниченной ответственностью и акционерного общества, приоритетно публичного акционерного общества (ПАО). При этом нецелесообразно ограничивать возможность создания IT-аутсорсера исключительно организационно-правовой формой акционерного общества, как это сделано, например, в отношении акционерного инвестиционного фонда. Оптимально установление одной из организационно-правовых форм хозяйственных обществ (ООО и АО) с определением публичных требований в законодательстве, минимизирующих риски каждой из организационно-правовых форм. Полагаем, что жесткость требований к аутсорсеру как универсальному посреднику будет компенсироваться эффектом масштаба (соединением большинства функций всего множества посредников).

Полагаем целесообразным придание универсальному IT-аутсорсеру правового статуса лица, оказывающего профессиональные услуги на финансовом рынке путем внесения изменений в главу X.1-1 Закона о Банке России. Установление такого статуса связано с осуществлением IT-

аутсорсером хранения, передачи и обработки информации в соответствующих информационных системах и их компонентах, используемых для осуществления банковских операций банков, что влечет необходимость обеспечения защиты прав их клиентов – физических и юридических лиц.

В отношении корпоративного управления по аналогии с кредитными организациями и с учетом создания IT-аутсорсера как хозяйственного общества, в особенности ПАО, полагаем целесообразным применение близких по смыслу требований к системе внутреннего контроля в IT-аутсорсере. Также при изменении архитектуры рынка IT-аутсорсинга с появлением универсального IT-аутсорсера, функции службы внутреннего контроля (СВК) кредитных организаций также должны быть расширены.

По вопросу о возможных вариантах формирования уставного капитала универсального IT-ауторсера, следует отметить, что структура капитала универсального IT-аутсорсера может стать одним из средств, минимизирующих как риск его финансовой устойчивости, так и его правовой и репутационный риски. С этой целью структуру участников (акционеров) универсального IT-аутсорсера могут составлять кредитные организации-потребители услуг, разработчики банковского ПО или иных субъектов рынка IT- аутсорсинга – поставщики услуг, инфраструктурные организации, в том числе обеспечивающие услуги телекоммуникации и связи, а также представляющие интересы предпринимательского сообщества на соответствующих банковском и технологическом рынках, - ассоциации (союзы) кредитных организаций, а также ассоциации (союзы) субъектов рынка IT-аутсорсинга. Соблюдение такого паритета позволит частично минимизировать риск возникновения конфликта интересов, избежав значительного влияния мажоритарных акционеров (участников) на принимаемых IT-аутсорсером решения.

С учетом того, что IT-аутсорсинг предполагает взаимодействие с кредитными организациями, очевидно, что ПО и услуги соответствующего IT-аутсорсера должны будут соответствовать повышенным требованиям, которые предъявляются Банком России к кредитным организациям в данной сфере. Полагаем, что при отнесении универсального IT-аутсорсера к лицам, оказывающим профессиональные услуги на финансовом рынке, многие проблемы подстройки повышенным банковским стандартам могут быть нивелированы, поскольку на таких субъектов распространяется действие нормативных актов Банка России в рассматриваемой сфере.

При этом в части распределения публично-правовой ответственности между кредитными организациями и универсальным IT-аутсорсером следует отметить, что в случае нарушения требований банковского законодательства, в том числе в части надлежащего уровня управления рисками, кредитная организация вне зависимости от договорных условий с компанией IT-аутсорсером будет нести публично-правовую ответственность перед регулятором. При отнесении универсального IT-аутсорсера к лицам, оказывающим профессиональные услуги на финансовом рынке, помимо всех иных регуляторных требований, которые рассматриваются в настоящем исследовании, он будет включен как субъект финансового рынка также в сферу регуляторного и надзорного воздействия финансового мегарегулятора и, соответственно, за нарушение требований законодательства данная компания также будет нести публично-правовую ответственность перед Банком России, что будет являться существенным фактором минимизации рисков соответствующих нарушений.

Исследовательская часть и выводы

1. Определение общей схемы правоотношений, которые могут возникнуть на рынке IT-аутсорсинга.

В общем виде аутсорсинг (outsourcing - "outside resourse using", англ.) означает использование внешних источников (ресурсов) и конкретизируется в передаче стороннему подрядчику (аутсорсинговой компании) некоторых бизнес-функций или частей бизнес-процессов компании. В процессе аутсорсинга контроль деятельности рассматриваемых подразделений возлагается на поставщика услуг или провайдера, который представляет собой приглашенную со стороны организацию, специализирующуюся в конкретной сфере и способную увеличить рыночную стоимость компании и продуктов, ею выпускаемых, что обычно недостижимо при выполнении различных второстепенных функций компанией, являющейся заказчиком[1].

Концепция аутсорсинга как принципа новой стратегии управления была создана в США в 1963 г. компанией "Elektronic Data System" (ЕДС), специализирующейся на аутсорсинге информационных технологий или IT-аутсорсинге[2]. Научной базой этого направления служили принципы, сформулированные А. Смитом, который предлагал организацию труда разбить на элементарные, простые задания, чтобы каждое из них мог выполнять отдельный рабочий[3]. В настоящее время в мире быстро развивающихся цифровых технологий особую актуальность приобрела дискуссия о правилах аутсорсинга в сфере финансовых услуг. Такой аутсорсинг не является чем-то новым для банковской сферы, но масштабы, которые он приобрел за время пандемии, привлекли внимание регуляторов по всему миру и поставили вопрос о том, насколько такой аутсорсинг несет в себе риск для безопасности и стабильности финансового рынка.

В результате развития новых тенденций на международном рынке **крупный бизнес IT-услуг со значительным количеством клиентов на**

[1] Арабян М.С., Попова Е.В. Таможенный представитель и его место в системе аутсорсинга таможенных услуг // Таможенное дело. 2015. N 2. С. 3 - 5.
[2] Курицкий В.В. Что такое аутсорсинг? Общество и право. 2008. N 1.
[3] Смит А. Исследование о природе и причинах богатства народов. М., 1935.

финансовом рынке может оказаться под прямым надзором со стороны регуляторов финансовых услуг, хотя исторически он всегда считал себя частью технологического сектора. Такой подход обусловлен **необходимостью минимизации рисков на финансовом рынке, в связи со значимостью его стабильности и безопасности для государства и граждан**.

В настоящее время вопросам управления рисками IT-аутсорсинга на финансовом рынке и определению полномочий регуляторов, в том числе в отношении поставщиков IT-услуг, уделяется большое внимание как в России, так и в зарубежных странах. Анализ международных подходов к регулированию IT-аутсорсинга свидетельствует о том, что в Европейском союзе, США, Великобритании, Индии, Канаде, Австралии и многих других странах уже предложены определенные правовые решения данного вопроса. **Создание комплексной правовой модели отношений IT-аутсорсинга в банковской сфере Российской Федерации является сегодня одной из приоритетных задач развития финансового рынка** как с точки зрения реализации потребности в цифровизации, так и с точки зрения необходимости минимизации многочисленных рисков, возникающих в данной сфере.

Аутсорсинг для банков и финансовых организаций имеет **множество преимуществ**, в том числе позволяет значительно сократить финансовые и временные затраты, так как привлечение специалистов различных квалификаций и оплата их услуг определяется объемом проделанной работы и не требует содержания значительного штата сотрудников, что также важно для небольших банков. Привлечение профессионалов различного профиля для точечного решения задач позволяет использовать эффективные клиентоориентированные подходы, обеспечить улучшение сервиса и высокое качество предоставляемых услуг, что следует из возможности банка или финансовой организации в любой момент заменить компанию, работающую на аутсорсинге. Передавая отдельные функции аутсорсерам, банки и финансовые организации получают инновации и передовые технологии, экономя средства на их разработку. К тому же возможность вкладывать

значительные ресурсы в развитие основных средств (а также сопутствующие им технологии и знания) есть не у всех субъектов финансового рынка[4]. Среди основных преимуществ IT-аутсорсинга в банковской сфере можно назвать возможность сфокусироваться на основной деятельности банка или финансовой организации при наличии постоянной консультационной и технической поддержки компетентных специалистов при осуществлении IT-функции, что может означать **получение результата от бизнес-процессов без управления ими**.

При наличии существенных преимуществ IT-аутсорсинга в банковской сфере необходимо указать, что массовое привлечение банками и финансовыми организациями сторонних поставщиков IT-услуг несет в себе значительное число рисков, что требует создания такого регулирования аутсорсинга в банковской сфере, которое бы позволило обеспечить IT-безопасность, стабильность и бесперебойность работы финансового рынка. Необходимо выделить и **ряд недостатков**, которые необходимо принимать во внимание при анализе выбора оптимальной модели аутсорсинга для IT-услуг в банковской сфере. Во-первых, аутсорсинг какой-либо функции приводит к тому, что компания, передающая свои функции, становится частично или полностью зависимой от сервисной организации, что, несомненно, повышает ее уязвимость. Во-вторых, требуется подготовка к разрешению проблемных ситуаций, которые могут возникнуть из-за качества услуг, предоставляемых сторонним поставщиком услуг, особенно с учетом того, что в период перехода на аутсорсинг, как правило, происходит реорганизация - перераспределение, переподготовка или увольнение специалистов определенной отрасли. Необходимо учитывать, что при передаче на аутсорсинг одновременно нескольких важных для компании функций возникает реальный риск утечки информации, что имеет особенное значение в банковской сфере. В-третьих, необходимо отметить такой фактор, как потеря контроля над собственными

[4] Аутсорсинг / С. Ефимова, Т. Пешкова, Н. Коник и др. М.: Журнал "Управление персоналом", 2006. 160 с.

ресурсами. Происходит отрыв руководства от части деятельности компании, вследствие чего возникает риск принятия неадекватных решений. Одним из основных рисков является неожиданное расторжение контракта аутсорсером. Отказ от оказания услуг или банкротство аутсорсера влечет за собой острую необходимость срочного поиска новых партнеров, что должно быть учтено при определении условий контракта, которым оформляется аутсорсинг. Наряду с перечисленными недостатками существует вероятность увеличения издержек при стремлении сосредоточиться на основной деятельности. Передавая второстепенные функции, при недобросовестности аутсорсера предприятие может пострадать из-за снижения качества продукции или услуг[5].

В Российской Федерации в настоящее время отсутствуют нормативные правила в отношении того, как должен осуществляться IT-аутсорсинг в банковской сфере. Вместе с тем **многие зарубежные страны приняли руководящие принципы и правила для IT-аутсорсинга в сфере финансовых услуг.** Для определения общей схемы правоотношений, которые могут возникнуть на рынке IT-аутсорсинга в банковской сфере Российской Федерации, необходимо проанализировать зарубежный опыт регулирования данного вопроса. Основной массив документов, регулирующих IT-аутсорсинг в банковской сфере, был принят в зарубежных странах в последние пять лет. Многие регуляторы систематизировали, обобщили и дополнили уже существующие правила, которые были применимы к аутсорсингу или привлечению третьих лиц к работе с банками и финансовыми организациями, какие-то регуляторы разработали и приняли руководящие принципы с чистого листа.

В 2019 году было выпущено Руководство Европейской Службы по банковскому надзору (EBA) по аутсорсингу от 25.02.2019 № EBA/GL/2019/02

[5] Аутсорсинг / С. Ефимова, Т. Пешкова, Н. Коник и др. М.: Журнал "Управление персоналом", 2006. 160 с.

«Guidelines on outsourcing arrangements»[6] (далее – Руководство EBA по аутсорсингу), которое заменило, в частности Рекомендации Комитета европейского банковского надзора (CEBS) по аутсорсингу, выпущенные в 2006 году и распространявшиеся исключительно на кредитные организации. Цель нового Руководства заключается в том, чтобы создать гармонизированные правила для всех финансовых организаций, находящихся в сфере действия регулирования мандата EBA. Европейский регулятор подчеркивает, что компетентные органы обязаны эффективно контролировать аутсорсинг услуг на финансовом рынке, включая деятельность по выявлению и мониторингу концентрации рисков на отдельных услугах поставщиков и оценку того, может ли такая концентрация представлять риск для стабильности финансовой системы[7]. В данном документе, как и во многих аналогичных документах зарубежных стран, урегулированы вопросы понятия аутсорсинга, надлежащего механизма управления и рисков, связанных с третьими лицами, требований к политикам финансовой организации или платежного учреждения в отношении аутсорсинга, требований к внутреннему аудиту, процессу передачи функций на аутсорсинг, включая анализ, проводимый до заключения соглашения об аутсорсинге, заключение соглашения об аутсорсинге, надзор за функциями, переданными на аутсорсинг, стратегии выхода из соглашения об аутсорсинге.

В США вопросам аутсорсинга на рынке финансовых услуг, в том числе в сфере IT, уделялось значительное внимание последние десять лет. Так, 5 декабря 2013 года Федеральная резервная система США (ФРС США) опубликовала «Руководство по управлению рисками аутсорсинга»[8] с целью оказания помощи финансовым учреждениям в понимании и управлении рисками, связанными с передачей банковской деятельности поставщику

---

[6] https://www.eba.europa.eu/sites/default/documents/files/documents/10180/2551996/38c80601-f5d7-4855-8ba3-702423665479/EBA%20revised%20Guidelines%20on%20outsourcing%20arrangements.pdf?retry=1

[7] EBA Guidelines on outsourcing arrangements EBA/GL/2019/02 25 February 2019. P. 5.

[8] Guidance on Managing Outsourcing Risk (December 2013) https://www.dataguidance.com/legal-research/guidance-managing-outsourcing-risk-december

услуг[9]. ФРС США подчеркнула, что данное Руководство основано на буклете по аутсорсинговым технологическим услугам Федерального экзаменационного совета финансовых учреждений[10] (FFIEC) и дополняет его. Управление денежного контролера США (OCC) в 2013 году выпустило рекомендации по управлению рисками третьих лиц для национальных банков и федеральных сберегательных ассоциаций[11], которые включали в себя документ «Руководящие принципы управления поставщиками технологических услуг и соглашения об аутсорсинге»[12]. Однако, в июне 2023 года данные документы были заменены единым документом «Отношения с третьими лицами: Межведомственное руководство по взаимоотношениям с третьими лицами: управление рисками»[13], выпущенным совместно Управлением денежного контролера (OCC), Федеральной корпорацией по страхованию депозитов (FDIC) и Советом ФРС США (FED). В данном руководстве изложены взгляды OCC, FDIC и FED на разумные принципы управления рисками в банковской сфере, что создает основу для банков и финансовых организаций при разработке и внедрении методов управления рисками на всех этапах жизненного цикла отношений с третьими сторонами[14]. Новое Руководство демонстрирует постоянное стремление к операционной устойчивости поставщиков услуг и будет применяться ко всем банковским и финансовым учреждениям в США, контролируемым названными регуляторами. В связи с растущей зависимостью отрасли от сторонних технологий и программного обеспечения Руководство требует от банков пересмотреть свои отношения с поставщиками программного обеспечения,

[9] USA: Federal Reserve Guidance on Managing Outsourcing Risk https://www.dataguidance.com/opinion/usa-federal-reserve-guidance-managing-outsourcing

[10] Outsourcing Technology Services Booklet (June 2004) https://www.dataguidance.com/legal-research/outsourcing-technology-services-booklet-june

[11] Guidance on Third Party Relationships (OCC 2013-29) https://sharedassessments.org/blog/occ-releases-guidance-third-party-relationships-occ-2013-29/

[12] "Outsourcing by Financial Services Companies: Impact of the OCC and FRB Guidelines" https://www.jdsupra.com/legalnews/outsourcing-by-financial-services-compa-29647/

[13] Interagency Guidance on Third-Party Relationships: Risk Management https://www.fdic.gov/news/financial-institution-letters/2023/fil23029.html

[14] Embracing Escrow: OCC, FDIC, and FED Board releases revised third-party risk management guidelines for US Banks https://www.mynewsdesk.com/nccgroup/news/embracing-escrow-occ-fdic-and-fed-board-releases-revised-third-party-risk-management-guidelines-for-us-banks-468720

внедрив принципы управления рисками третьих лиц (независимые проверки документации и отчетности, надзор, подотчетность и т.д.), а также пересмотреть свои внутренние политики, стандарты и процедуры. Регуляторы выделяют 5 ключевых этапов, на которых необходимо учитывать управление рисками третьих лиц: планирование, комплексная проверка и выбор третьего лица, переговоры по контракту, постоянный мониторинг, прекращение действия контракта.

В Великобритании вопросы, касающиеся аутсорсинга услуг финансовыми организациями, находятся в сфере ведения Управления финансового надзора (FCA) и Управления пруденциального регулирования (PRA) Великобритании. Заявление надзорного органа 2/21 «SS2/21 Аутсорсинг и управление рисками третьих сторон»[15] излагает ожидания Управления пруденциального регулирования (PRA) относительно того, как компании, регулируемые PRA, должны соблюдать нормативные требования, касающиеся аутсорсинга и управления рисками третьих лиц. Данный документ дополняет требования и ожидания в отношении эксплуатационной устойчивости, закрепленные в Своде правил PRA; SS1/21 «Эксплуатационная устойчивость: устойчивость к воздействию важных бизнес-услуг».

Среди новых документов можно назвать, например, Директиву Резервного банка Индии (аутсорсинг услуг в области информационных технологий) 2023 года[16], которая регулирует деятельность банков и других ключевых финансовых организаций, в том числе банков развития в направлении важных аспектов IT-аутсорсинга, нарушения которых может потенциально (a) существенно повлиять на проведение операций такими организациями или (b) в случае любого несанкционированного доступа,

[15] Supervisory Statement | SS2/21 Outsourcing and third party risk management March 2021 https://www.bankofengland.co.uk/-/media/boe/files/prudential-regulation/supervisory-statement/2021/ss221-march-21.pdf

[16] Reserve Bank of India (Outsourcing of Information Technology Services) Directions, 2023 https://rbidocs.rbi.org.in/rdocs/notification/PDFs/102MDITSERVICES56B33FD530B1433187D75CB7C06C8F70.PDF

потери или кражи информации о клиентах оказать существенное влияние на клиентов таких организаций.

В исследовании также были проанализированы непосредственно посвященные IT-аутсорсингу в банковской сфере Уведомление Банка Таиланда № FPG 8/2557 «Положения об аутсорсинге финансовых организаций»[17], Пруденциальный стандарт Австралийской администрации регулирования (APRA)[18], Руководящие принципы «Аутсорсинг бизнес-деятельности, функций и процессов»[19], выпущенные Управлением суперинтенданта финансовых учреждений (OSFI) Канады, Руководящие принципы Банка Танзании[20], Руководящие принципы Банка Маврикия[21], Руководящие принципы регулятора Сингапура[22] и др.

Идея IT-аутсорсинга в банковской сфере заключается в том, что кредитная организация передает сторонним поставщикам услуг выполнение действий, которые не составляют ядро банковской деятельности, являются для нее вспомогательными. Передача вспомогательной деятельности на аутсорсинг позволит банку сосредоточиться на своей основной деятельности. Так, например, Банк Таиланда прямо указывает, что главный принцип аутсорсинга заключается в том, что основные функции, связанные с принятием бизнес-решений, должны выполняться банками и финансовыми организациями, а не поставщиками услуг[23]. Следует отметить, что если раньше прослеживалась тенденция передачи на аутсорсинг

[17] Notification of the Bank of Thailand No. FPG 8/ 2557 Re: Regulations on Outsourcing of Financial Institutions https://www.bot.or.th/content/dam/bot/fipcs/documents/FPG/2558/EngPDF/25580002.pdf

[18] Prudential Standard CPS 231 Outsourcing July 2017 https://www.apra.gov.au/sites/default/files/Prudential-Standard-CPS-231-Outsourcing-%28July-2017%29.pdf

[19] Outsourcing of Business Activities, Functions and Processes https://www.osfi-bsif.gc.ca/Eng/fi-if/rg-ro/gdn-ort/gl-ld/Pages/b10.aspx

[20] Outsourcing guidelines for banks and financial institutions. 2021. Bank of tanzania. https://www.bot.go.tz/Publications/Acts,%20Regulations,%20Circulars,%20Guidelines/Guidelines/en/20210630152241391.pdf

[21] Guidelines on Outsourcing by Financial Institutions. Revised October 2020. Bank of Mauritius. https://www.bom.mu/sites/default/files/guidelines_on_outsourcing_by_financial_institutions_13.10.2020.pdf

[22] Guidelines on Outsourcing. Monetary Authority of Singapore. 27 July 2016. https://www.mas.gov.sg/-/media/mas/regulations-and-financial-stability/regulatory-and-supervisory-framework/risk-management/outsourcing-guidelines_jul-2016-revised-on-5-oct-2018.pdf

[23] Notification of the Bank of Thailand No. FPG 8/ 2557 Re: Regulations on Outsourcing of Financial Institutions https://www.bot.or.th/content/dam/bot/fipcs/documents/FPG/2558/EngPDF/25580002.pdf

обслуживающих или вспомогательных функций, то в настоящее время возрастает количество контрактов по передаче более сложных функций. При переходе на аутсорсинг нужно придерживаться стандартного принципа - прибегать к передаче функций не только с целью экономии средств, а в первую очередь повысить конкурентоспособность компании при минимальных издержках. Важно правильно определить цели и сделать выбор, какие функции необходимо сохранить, а для каких потребуется привлечение сторонних исполнителей[24]. **Главный принцип аутсорсинга - оставляю себе только то, что могу делать лучше других; передаю другому то, что он делает лучше других**[25].

Как указывает Банк России, **в большинстве стран не устанавливается перечень функций, аутсорсинг которых разрешен, а регулирование основано на установлении критериев признания функций существенными**. Анализ зарубежных документов в данной сфере показал, что основным критерием для регулирования IT-аутсорсинга выступает возможность возникновения ситуации, при которой сбой в осуществлении функций банков или финансовых организаций окажет существенное влияние на непрерывность и надежность деятельности участника финансового рынка, соответствие регуляторным требованиям, а также возможность причинения вреда потребителям финансовых услуг[26].

В различных странах предложены разные определения понятия существенности функций или видов деятельности, которые могут быть переданы на аутсорсинг.

Так, APRA регулятор финансового рынка Австралии в п. 14 Пруденциального стандарта[27] определяет существенной вид деятельности как деятельность, нарушение которой потенциально может оказать существенное

[24] Аутсорсинг / С. Ефимова, Т. Пешкова, Н. Коник и др. М.: Журнал "Управление персоналом", 2006. 160 с.
[25] Актуальные новости ("Налоги" (газета), 2009, N 12)
[26] Доклад Банка России для общественных слушаний «Управление рисками аутсорсинга на финансовом рынке». М., 2022. С. 14.
[27] Prudential Standard CPS 231 Outsourcing July 2017 https://www.apra.gov.au/sites/default/files/Prudential-Standard-CPS-231-Outsourcing-%28July-2017%29.pdf

влияние на деловую активность регулируемого учреждения или группы, или ее способность эффективно управлять рисками, принимая во внимание такие факторы, как (a) финансовые и операционные последствия, влияние на репутацию регулируемого учреждения; (b) стоимость соглашения об аутсорсинге в объеме общих затрат; (c) степень сложности, включая время, необходимое для поиска альтернативного поставщика услуг или осуществления деятельности собственными силами; (d) способность учреждения или члена группы, регулируемых APRA, соблюдать нормативные требования в случае возникновения проблем с поставщиком услуг; (e) потенциальные убытки для клиентов учреждения или группы, регулируемых APRA, и других затронутых сторон в случае сбоя работы поставщика услуг; и (f) отношения между учреждением или группой, регулируемой APRA, и поставщиком услуг. Пруденциальный стандарт требует, чтобы все соглашения об аутсорсинге, касающиеся существенных видов деятельности банков и финансовых организаций, находящихся под ее надзором, подлежали соответствующей комплексной проверке, одобрению и постоянному мониторингу. APRA устанавливает, что все риски, возникающие в результате существенных видов деятельности, должны быть надлежащим образом оценены, и гарантировано, что банк или финансовая организация способны выполнять свои финансовые и сервисные обязательства перед вкладчиками и/или страхователями.

В п. 5.3 и 5.4 Заявления надзорного органа 2/21 «SS2/21[28] Великобритании, в своде правил PRA указано, что «существенный аутсорсинг» определяется как аутсорсинг услуг такого рода, слабость исполнения или отказ от которых поставят под серьезное сомнение деятельность регулируемой организации и возможность дальнейшего соблюдения основополагающих правил. Существенность следует понимать

[28] Supervisory Statement | SS2/21 Outsourcing and third party risk management March 2021 https://www.bankofengland.co.uk/-/media/boe/files/prudential-regulation/supervisory-statement/2021/ss221-march-21.pdf

как включение концепции «критического или важного оперативного фактора». В Великобритании термин «существенный аутсорсинг» созвучен европейскому термину «критически важный или существенный».

Согласно п. 29 Руководства Европейской Службы по банковскому надзору[29] функция всегда должна считаться существенной или критической, если сбой в ее осуществлении может нанести значимый ущерб, в частности в аспекте нарушения непрерывного соблюдения условий выданных финансовой организации или платежному учреждению разрешений, нормативных обязательств, ухудшение финансовых результатов или нарушение устойчивого, непрерывного процесса предоставления банковских и платежных услуг и ведения деятельности. Функция всегда должна считаться существенной или критической также, если на аутсорсинг передается операционная часть внутреннего контроля, за исключением случаев, при которых проведенная оценка показывает, что непредоставление или ненадлежащее выполнение этой функции третьей стороной не окажет негативного влияния на общую эффективность внутреннего контроля, и если на аутсорсинг передаются функции, связанные с банковской деятельностью или с предоставлением платежных услуг в объеме, требующем разрешения компетентного органа.

В п. 26 Руководства Европейской Службы по банковскому надзору[30] установлено, что финансовые организации и платежные учреждения должны определить, подпадает ли соглашение с третьей стороной под понятие аутсорсинга. Регулятор рекомендует установить, выполняется ли функция (или ее часть), переданная на аутсорсинг поставщику услуг, на периодической или постоянной основе, а также выявить, могла ли и должна ли была эта финансовая организация или платежное учреждение самостоятельно

[29] EBA Guidelines on outsourcing arrangements EBA/GL/2019/02 25 February 2019 https://www.eba.europa.eu/sites/default/documents/files/documents/10180/2551996/38c80601-f5d7-4855-8ba3-702423665479/EBA%20revised%20Guidelines%20on%20outsourcing%20arrangements.pdf?retry=1

[30] EBA Guidelines on outsourcing arrangements EBA/GL/2019/02 25 February 2019 https://www.eba.europa.eu/sites/default/documents/files/documents/10180/2551996/38c80601-f5d7-4855-8ba3-702423665479/EBA%20revised%20Guidelines%20on%20outsourcing%20arrangements.pdf?retry=1

выполнять переданную третьей стороне функцию (или ее часть), даже если ранее этим не занималась. Регулятор перечисляет виды деятельности, которые, по общему правилу, к аутсорсингу не относятся, в частности, переданные третьим лицам функции, которые по закону должны выполняться поставщиком услуг, например, обязательный аудит; предоставление рыночной информации (например, предоставление данных Bloomberg, Moody's, Standard & Poor's, Fitch); доступ к глобальной инфраструктуре (например, Visa, MasterCard); клиринговые и расчетные соглашения между клиринговыми палатами, центральными контрагентами, расчетными учреждениями и их членами; глобальные инфраструктуры обмена финансовыми сообщениями, которые подлежат надзору со стороны соответствующих органов; корреспондентские банковские услуги; приобретение услуг, которые для финансовой организации или платежного учреждения не являются профильными (например, консультации архитектора, предоставление юридического заключения и т.д.).

В некоторых зарубежных странах законодатель идет по пути классификации различных услуг, которые могут или не могут передаваться на аутсорсинг. Так, в п. 6 Руководящих принципах Банка Танзании[31] виды деятельности банка или финансовой организации разделены на (1) стратегические или (2) нестратегические. Стратегические виды деятельности, по мнению регулятора Танзании, нельзя передавать на аутсорсинг. Такие виды деятельности касаются, например, выполнения функций контроля и управления рисками. Кроме того, в документе прямо названы иные виды деятельности, которые нельзя передавать на аутсорсинг, а также виды деятельности, которые не могут считаться аутсорсингом. Нестратегические, но существенные виды деятельности включают те виды, нарушение которых негативно и существенным образом скажется на способности банка или

[31] Outsourcing guidelines for banks and financial institutions. 2021. Bank of tanzania. https://www.bot.go.tz/Publications/Acts,%20Regulations,%20Circulars,%20Guidelines/Guidelines/en/2021063015241391.pdf

финансовой организации соблюдать требования нормативных актов и вести свой бизнес. В большинстве документов регуляторов не предлагается столь сложной классификации видов деятельности, и речь идет просто о существенных видах деятельности.

Отметим, что встречаются также документы, в которых приведен перечень IT-услуг, которые могут быть переданы на аутсорсинг. Так, Директива Резервного банка Индии[32] (п. IV) содержит список аутсорсинговых IT-услуг, который остается открытым и включает в себя управление IT-инфраструктурой, услуги облачных сервисов, услуги информационной безопасности, услуги управления технологиями, связанными с экосистемой платежных систем и т.д. При этом в Директиве не представлено конкретных параметров, определяющих, какие IT-услуги могут или не могут быть переданы регулируемыми организациями на аутсорсинг сторонним поставщикам услуг. Приложение 3 к Директиве содержит ориентировочный список (a) услуг, которые не подпадают под категорию «аутсорсинга IT-услуг» (например, приложения, предоставляемые финансовыми регуляторами); и (b) поставщики/организации, которые не считаются сторонними поставщиками услуг в соответствии с Директивой (например, поставщики, предоставляющие бизнес-услуги с использованием IT, операторы платежных систем, уполномоченные Резервным банком Индии, и поставщики телекоммуникационных услуг).

Таким образом, в рамках анализа общей схемы правоотношений на рынке IT-аутсорсинга необходимо определить, какие услуги не могут передаваться банками на аутсорсинг. **Как показывает анализ международной практики, перечень услуг, которые могут быть переданы на аутсорсинг, оставляется регуляторами открытым. В законодательстве могут содержаться ограничения на передачу определенных услуг на**

[32] Reserve Bank of India (Outsourcing of Information Technology Services) Directions, 2023 https://rbidocs.rbi.org.in/rdocs/notification/PDFs/102MDITSERVICES56B33FD530B1433187D75CB7C06C8F70.PDF

аутсорсинг финансовыми организациями, а также для передачи определенного вида услуг могут быть установлены дополнительные требования.

Согласно Докладу Банка России, в отечественной интерпретации под IT-услугами понимается привлечение поставщиков информационных технологий и облачных сервисов для резервного копирования, обработки и хранения данных; разработки и сопровождения программного обеспечения; технического обслуживания программно-аппаратных средств; сопровождения сетевой инфраструктуры[33]. При этом в соответствии с Проектом Федерального закона «О внесении изменений в отдельные законодательные акты Российской Федерации» (далее – Законопроект об IT-аутсорсинге) ст. 2 Федерального закона от 27.07.2006 № 149-ФЗ «Об информации, информационных технологиях и о защите информации»[34] (далее – Закон об информации) дополняется пунктом 23, согласно которому поставщик услуг аутсорсинга информационных технологий и облачных услуг – это лицо, являющееся владельцем информационных систем и их компонентов, в частности облачных и файловых хранилищ, серверов, иных устройств и систем сбора, хранения и обработки информации, предоставляющее услуги по размещению, хранению и иной обработке сведений в соответствующих информационных системах и их компонентах. **Представляется, что в основе выделения IT-аутсорсинга должен находиться критерий существенности функций и видов деятельности, передаваемых на аутсорсинг, а также соблюдение принципа о том, что кредитная организация не передает сторонним поставщикам услуг выполнение действий, которые составляют ядро их деятельности.**

Ключевой основополагающий принцип рекомендаций регуляторов заключается в том, что банк или финансовая организация должны

[33] Доклад Банка России для общественных слушаний «Управление рисками аутсорсинга на финансовом рынке». М., 2022. С. 7.
[34] СЗ РФ. 2006, N 31 (1 ч.), ст. 3448.

гарантировать, что соглашения об аутсорсинге не уменьшают их способность выполнять свои обязательства перед своими клиентами и регулятором. Как отмечает Европейский регулятор EBA, аутсорсинг не должен привести к ситуации, в которой учреждение становится «пустой оболочкой», которой не хватает содержания, чтобы оставаться авторизованным[35]. Кроме того, **кредитная организация должна гарантировать, что соглашения об аутсорсинге не препятствуют эффективному надзору со стороны регулятора**. В этой связи банки должны принять меры для обеспечения того, чтобы поставщик услуг исходил из тех же стандартов при оказании услуг, из которых исходит сам банк, если бы такая деятельность не была передана на аутсорсинг и осуществлялась самим банком. Кроме того, **ответственность за соблюдения требований законодательства и регулятора возлагается на кредитные организации, в том числе и в случае, когда они передали свои функции или отдельные виды деятельности сторонним поставщикам услуг по соглашению аутсорсинга**. Так, в Руководящих принципах OSFI Канады[36] установлено, что банк или финансовая организация сохраняют полную ответственность за всю деятельность, переданную на аутсорсинг. Более того, надзорные полномочия OSFI не должны быть ограничены, независимо от того, осуществляется ли деятельность собственными силами банка или финансовой организации, передается ли она на IT-аутсорсинг или иным образом делегируется для исполнения сторонним поставщикам услуг. В Тайланде регулятор установил, что при аутсорсинге любой функции банки и финансовые организации должны нести ответственность перед клиентами, как если бы они сами выполняли эти функции[37]. Директива Резервного банка Индии[38] прямо

[35] EBA Guidelines on outsourcing arrangements EBA/GL/2019/02 25 February 2019 https://www.eba.europa.eu/sites/default/documents/files/documents/10180/2551996/38c80601-f5d7-4855-8ba3-702423665479/EBA%20revised%20Guidelines%20on%20outsourcing%20arrangements.pdf?retry=1

[36] Outsourcing of Business Activities, Functions and Processes https://www.osfi-bsif.gc.ca/Eng/fi-if/rg-ro/gdn-ort/gl-ld/Pages/b10.aspx

[37] Notification of the Bank of Thailand No. FPG 8/ 2557 Re: Regulations on Outsourcing of Financial Institutions https://www.bot.or.th/content/dam/bot/fipcs/documents/FPG/2558/EngPDF/25580002.pdf

[38] Outsourcing of IT Services by Banks and Financial Institutions - Overview of the Regulatory Regime and the Key Takeaways May 12 2023 https://www.lexology.com/library/detail.aspx?g=ac19aa69-3751-4814-b5ad-98f1837dfa13

возлагает на регулируемые организации ответственность перед своими клиентами за исполнение аутсорсинговых услуг. Резервный банк Индии указывает, что банк или финансовая организация должны принять меры для обеспечения того, чтобы поставщик услуг применял такие же высокие стандарты качества при оказании услуг, которые применялись бы самим банком или финансовой организацией, если бы та же деятельность не была передана на аутсорсинг. Не должны привлекаться поставщики услуг, чья деятельность может привести к компрометации или ослаблению репутации банка или финансовой организации (п. 4 Директивы[39]).

Банк России отмечает, что анализ международных подходов к регулированию аутсорсинга свидетельствует о том, что вопросам управления рисками аутсорсинга и определению полномочий регуляторов, в том числе в отношении поставщиков услуг, уделяется большое внимание»[40]. Как было отмечено, Руководство Европейской Службы по банковскому надзору (EBA) также выпустило Руководство по аутсорсингу EBA от 25.02.2019 № EBA/GL/2019/02 «Guidelines on outsourcing arrangements»[41] (далее – Руководство EBA по аутсорсингу), которое соблюдается в настоящее время большинством стран Европейского союза[42]. Примечательно, что Руководство EBA по аутсорсингу обязывало финансовые организации внести изменения с учетом ряда требований в действующие соглашения об аутсорсинге до 31.12.2021, в противном случае уведомить регулятора, указав какие меры финансовая организация будет предпринимать для приведения соглашений в соответствие с требованиями Руководства EBA по аутсорсингу.

Если обобщить ключевые риски, которые выделяются для аутсорсинга в Руководстве EBA, то к ним можно отнести:

---

[39] Reserve Bank of India (Outsourcing of Information Technology Services) Directions, 2023 https://rbidocs.rbi.org.in/rdocs/notification/PDFs/102MDITSERVICES56B33FD530B1433187D75CB7C06C8F70.PDF

[40] Доклад Банка России для общественных слушаний «Управление рисками аутсорсинга на финансовом рынке». М., 2022. С. 2. // https://cbr.ru/Content/Document/File/142481/Consultation_Paper_06122022.pdf

[41] https://www.eba.europa.eu/sites/default/documents/files/documents/10180/2551996/38c80601-f5d7-4855-8ba3-702423665479/EBA%20revised%20Guidelines%20on%20outsourcing%20arrangements.pdf?retry=1

[42] https://www.eba.europa.eu/sites/default/documents/files/document_library//875334/EBA%20GL%202019%2002%20-%20CT%20GLs%20on%20outsourcing%20arrangements%20%281%29.pdf?retry=1

- риск потери финансовой устойчивости;

- операционные риски;

- репутационные риски.

Немецкие исследователи также отмечают, что основные проблемы интеграции в сфере IT-аутсорсинга состоят, в том числе в высокой сложности этих процессов, а также в IT-безопасности, конфиденциальности, несовместимых интерфейсах[43].

Банк России в Докладе «Управление рисками аутсорсинга на финансовом рынке» (далее – Доклад Банка России), в том числе на основе анализа зарубежного опыта выделяет риски утраты контроля за отдельными функциями, операционные риски, комплаенс-риски, репутационные риски, а также риск монополизации рынка.

Таким образом, **для построения оптимальной правовой модели универсального IT-аутсорсера необходимо выявить и систематизировать гражданско-правовые (договорные), корпоративные (с учетом корпоративных и иных внутренних процедур в IT-аутсорсере и в кредитной организации-клиенте), а также публично-правовые средства минимизации ключевых рисков: риска потери финансовой устойчивости (риск утраты контроля за функцией, системный риск), операционного риска (риск ошибки персонала, риск сбоя информационных систем, риск информационной безопасности), правового риска (комплаенс-риск, риск раскрытия конфиденциальной информации, риск нарушения договора с IT-аутсорсером, риск прекращения договора с IT-аутсорсером) репутационного риска (риск недобросовестных действий IT-аутсорсера, риск возникновения конфликта интересов), а также риска монополизации рынка (риск злоупотребления доминирующим положением на рынке, риск нарушения законодательства о защите конкуренции в форме недобросовестной конкуренции).**

---

[43] Rederer Tomas «Finanzdienstleistungssektor setzt verstärkt auf Outsourcing» // https://www.pwc.de/de/finanzdienstleistungen/outsourcing-in-der-finanzindustrie.html

Все указанные средства применительно к минимизации обозначенных рисков рассматриваются в настоящем исследовании в соответствующих разделах для их систематизации в заключительной части.

1.1. Определение основных субъектов правоотношений на рынке IT- аутсорсинга на основании выделенных IT-функций (Дополнение №1 к Техническому заданию).

Для определения основных субъектов правоотношений на рынке IT-аутсорсинга необходимо рассмотреть использование облачных сервисов.

В рамках настоящего исследования мы рассматриваем такие IT-функции, как банковская Core-система; Back-office (электронный архив; бухгалтерия; финансовый мониторинг; налоговый учет; расчетный центр; инкассация; кредиты; депозиты; карты; залоги; депозитарные ячейки (сейфовые ячейки); валютно-денежный рынок; международные переводы; фондовый рынок; МСФО 9; исполнительное производство; РКО; хозяйственная деятельность); Front-office (процессинг; дистанционное банковское обслуживание; контакт-центр; система принятия решений (скоринг); CRM-система; работа с партнерами (PRM); система управления бизнес-процессами (BPM)); отчетность и аналитика; информационная безопасность; разработка и тестирование программного обеспечения (ПО); аутстаффинг IT-персонала; сервисы биометрии; серверное оборудование; облачные сервисы. Перечень видов деятельности в области информационных технологий перечислен в Приказе Минцифры России от 11.05.2023 № 449 «Об утверждении перечня видов деятельности в области информационных технологий»[44].

В законодательстве не предусмотрены особые статусы в отношении субъектов правоотношений на рынке IT- аутсорсинга.

[44] http://publication.pravo.gov.ru/document/0001202308150009?ysclid=lmqjayc9b1342636418&index=2

На практике **поставщик услуг аутсорсинга программного обеспечения** занимается **созданием/адаптацией/развитием/ сопровождением прикладного программного обеспечения автоматизированной банковской системы** (АБС), **поставкой общесистемного программного обеспечения** (операционные системы, системы управления базами данных, программное обеспечение серверов приложений и т.д.), предоставлением эксплуатирующего IT-персонала (**аутстаффинг**), организацией технической поддержки программного обеспечения.

По договору поставки поставщик-продавец, осуществляющий предпринимательскую деятельность, обязуется передать в обусловленный срок или сроки производимые или закупаемые им товары покупателю для использования в предпринимательской деятельности или в иных целях, не связанных с личным, семейным, домашним и иным подобным использованием (ст. 506 ГК РФ). Договор поставки не является договором, который оформляет отношения аутсорсинга, но может служить вспомогательным договором, который определяет отношения между основными субъектами на рынке IT-аутсорсинга. Представляется, что аутсорсер может закупать необходимое оборудование и программное обеспечение, и тогда он будет выступать посредником на основании гражданско-правовых договоров агентирования, комиссии или поручения. Так как согласно ст. 509 ГК РФ поставка товаров осуществляется поставщиком путем отгрузки (передачи) товаров покупателю, являющемуся стороной договора поставки, или лицу, указанному в договоре в качестве получателя, можно обойтись и без заключения посреднического договора, так как покупателем может являться банк, а передача товара может производиться аутсорсеру.

При создании прикладного программного обеспечения автоматизированной банковской системы необходимо определиться с тем, кому будут принадлежать исключительные права на результаты интеллектуальной деятельности. Согласно п. 1 ст. 1233 ГК РФ,

правообладатель может распорядиться принадлежащим ему исключительным правом на результат интеллектуальной деятельности или на средство индивидуализации любым не противоречащим закону и существу такого исключительного права способом, в том числе путем его отчуждения по договору другому лицу (договор об отчуждении исключительного права) или предоставления другому лицу права использования соответствующих результата интеллектуальной деятельности или средства индивидуализации в установленных договором пределах (лицензионный договор). Следовательно, в зависимости от того, кому будут принадлежать исключительные права на результаты интеллектуальной деятельности и от того, хочет ли банк обладать ими на постоянной или временной основе, необходимо заключить лицензионный договор или и договор об отчуждении исключительного права для использования той или другой стороной результатов интеллектуальной деятельности. **Адаптация, развитие и сопровождение прикладного программного обеспечения автоматизированной банковской системы, а также организация технической поддержки программного обеспечения будут осуществляться по договору о возмездном оказании услуг**, о котором речь пойдет подробно далее.

Предоставление эксплуатирующего IT-персонала может осуществляться по договору аутстаффинга. Понятие аутстаффинга законодательно нигде не определено. Договор о предоставлении труда работников (персонала) - это соглашение, по которому одна сторона (исполнитель) временно направляет своих работников с их согласия к другой стороне (заказчику) для выполнения данными работниками трудовых функций, установленных в их трудовых договорах с исполнителем, в интересах, под управлением и контролем заказчика. Другая сторона (заказчик) обязуется оплатить услуги по предоставлению труда работников (персонала) и использовать труд работников в соответствии с их трудовыми функциями (п. 2 ст. 18.1 Закона РФ от 19.04.1991 № 1032-1 «О занятости населения в

Российской Федерации»[45]). К таким субъектам были отнесены, во-первых, частные агентства занятости - специализированные юридические лица, подлежащие аккредитации, для которых предоставление персонала является основной деятельностью, а во-вторых, иные юридические лица, право на предоставление персонала у которых возникает только в прямо установленных законом случаях[46]. Согласно действующему российскому законодательству, аутстаффинг подпадает под понятие заемный труд, который по общему правилу согласно ст. 56.1 ТК РФ запрещен. С момента введения запрета на аутстаффинг у компаний возникали правовые и финансовые риски, в том числе в отношении уплаты страховых взносов и налогов вследствие переквалификации гражданского договора и установления трудовых правоотношений в отношении лиц, занятых по схеме аутстаффинга. То есть заемный труд влечет не только риски в части трудового права, но и налоговые риски. При закреплении отношений по схеме аутстаффинга правовые и финансовые риски возникают не только у компаний, но и у физических лиц - работников. **Таким образом, использование заемного труда по схеме аутстаффинга при наличии прямого законодательного запрета на такой труд может повлечь негативные последствия как для компаний, так и для работников**[47]. **Преимуществом аутсорсинга перед аутстаффингом** является то, что под аутсорсингом понимается передача организацией специализированному внешнему подрядчику определенных видов или бизнес-процессов, то есть функций производственной предпринимательской деятельности на основании договора подряда или услуг. В рамках договора подряда/услуг компания-провайдер сама организует производство, руководит своими работниками и отвечает за результаты их деятельности перед заказчиком, тогда как классический аутстаффинг предполагал ответственность провайдера таких услуг только за «качество»

[45] СЗ РФ. 1996, ст. 1915.
[46] Саурин С.А. Перспективы дальнейшего совершенствования законодательства о предоставлении персонала // Закон. 2022. N 10. С. 93 - 103.
[47] Хлебников П. Аутстаффинг. Риски современности // Трудовое право. 2022. N 5. С. 13 - 20.

предоставляемого персонала и соблюдение сроков, но не за результаты работы этого персонала, поскольку контроль за производственной деятельностью был в руках заказчика[48].

Провайдеры инфраструктуры IT занимаются предоставлением вычислительных мощностей (процессоры и оперативная память), предоставлением систем хранения данных, предоставлением услуг телекоммуникационной связи. В последнее время в данном контексте широкое распространение подучила такая **модель, как Software as a service (SaaS) («Программное обеспечение как услуга»), которая предполагает запуск приложения на технической площадке провайдера через браузер, исключая необходимость капитальных вложений в собственную IT-инфраструктуру**. Заказчик лишь организует доступ в Интернет и покупает подписку на сервисы, необходимые ему для ведения бизнеса. Использование данной концепции позволяет небольшим компаниям получать услуги на высоком техническом уровне, ранее доступном только крупным корпорациям, и дает возможность сконцентрировать свое внимание не на развитии и поддержании собственной IT-инфраструктуры: покупке программного обеспечения, оборудования, найме высокооплачиваемых IT-специалистов, а только на своем бизнесе[49]. В теории максимальное преимущество от замены собственной инфраструктуры на услуги внешних провайдеров достигается, когда арендуется все IT, включая вычислительные мощности, программную платформу и бизнес-приложения. В этом случае не нужно платить за оборудование, которое устаревает и за лицензии на программное обеспечение[50].

Как правило, регулирование отношений организации-клиента с ASP-провайдером (Application Service Providing, ASP) осуществляется **в рамках соглашения об уровне (качестве) обслуживания** (Service Level Agreement,

[48] Гулякина В., Звагольская О., Платонов В., Попова О., Рейзман Е. Аутсорсинг как форма аутстаффинга - о чем говорит практика // Трудовое право. 2023. N 4. С. 79 - 102.
[49] Смолянов М. Эффективность в аренду. Недорого // Консультант. 2010. N 11. С. 82 - 85.
[50] Костылев И. Все в ауте // Банковское обозрение. 2011. N 11. С. 120 - 122.

SLA), в котором оговариваются ответственность ASP-провайдера и возможности клиента. Такое соглашение является одним из видов соглашения (контракта) об аутсорсинге. Однако зачастую услуги, оказываемые ASP-провайдерами, представляют собой **использование элементов IT-инфраструктуры на условиях аренды (фиксированной ежемесячной платы), особенно когда речь идет о предоставлении систем хранения данных.** Начиная с услуг дата-центров, удаленное использование IT-ресурсов аутсорсера приобретало все большую популярность. ASP-провайдеры размещают на своей территории серверы и сетевое оборудование, устанавливают различные программные средства (прикладное программное обеспечение, системы мониторинга и управления и др.) и предоставляют своим клиентам доступ к этим средствам. В структуре услуг аутсорсинга ASP рассматривается полный или частичный IT-аутсорсинг, в зависимости от комплексности поддержки IT-сервиса, предоставляемой поставщиком услуг. Взаимодействие клиента с ASP-провайдером осуществляется следующим образом. ASP-провайдер (одна или несколько компаний) развертывают на своем (или арендуемом) оборудовании приложения (обычно разработки третьих фирм) и специализированные сервисы, предназначенные для сдачи в аренду. Клиент подписывает договор об аренде и получает право удаленного доступа к приложениям или сервисам. Такая модель снимает с клиента проблемы и затраты, связанные с развитием приложений и технической базы. Клиентам не надо заботиться об администрировании серверов приложений и баз данных (и тем более приобретать их). Все эти ресурсы находятся у ASP-провайдера. Доступ к арендуемым приложениям осуществляется через Интернет (только для приложений, имеющих интернет-клиента) или виртуальную частную сеть.

Среди основных участников ASP-рынка можно выделить независимых разработчиков программного обеспечения, обладающих правом собственности на приложения, сдаваемые в аренду; ASP-провайдеров, являющихся владельцами аппаратно-программных средств и сдающих

приложения и сервисы в аренду; NSP-провайдеров (network service provider), которые представляют собой организация, поставляющие услуги связи и передачи данных (физическая связь, маршрутизация, управление трафиком), центра обработки данных и IP-ресурсы (виртуальные собственные сети, межсетевые экраны, кеширование); клиентов. ASP-провайдеры сдают в аренду следующие основные типы приложений: - персональные - офисные пакеты (наподобие MS-Office), игры, обучающие программы и др.; групповое программное обеспечение; приложения для электронного бизнеса (электронные торговые места, магазины, порталы и др.); приложения для предприятий - управление ресурсами предприятия (ERP), взаимодействие с клиентами (CRM), управление цепями поставок (SCM); специфические отраслевые приложения для различных вертикальных рынков (здравоохранение, госслужба, коммунальные службы и др.); аналитические приложения, системы управления персоналом. Различают следующие основные типы ASP-провайдеров: 1) сервис-интеграторы (service integrators) - Full-service ASP или Solution Provider - компании, непосредственно работающие с конечными пользователями, которые предоставляют на условиях аренды полное автоматизированное решение (IT-инфраструктуру, хостинг и управление доступом к пакетным приложениям, программные сервисы через глобальную сеть из центра обработки данных); 2) провайдеры доступа - компании, предоставляющие пользователям доступ в Сеть (провайдеры «последней мили»), в том числе операторы мобильной связи, предоставляющие доступ к беспроводным приложениям; 3) операторы инфраструктуры (infrastructure operators) - телекоммуникационные компании, предоставляющие международные каналы, хостинг и выделенные линии; 4) сервис-провайдеры инфраструктуры (infrastructure service providers) или провайдеры прикладной инфраструктуры (application infrastructure provider, AIP), которые предлагают полный набор инфраструктурных IT-услуг для хостинга онлайн-приложений, а также сервисы управления различными системами (например, биллинговыми и платежными) и сетями и др., благодаря

которым конечные пользователи получают доступ к приложениям, содержимому, системам хранения данных (потребителями этих услуг могут быть и другие ASP-провайдеры); 5) MSP-провайдеры (management service providers) - провайдеры, специализирующиеся на удаленном управлении IT-системами клиентов на основе подписки. Фактически MSP - это эволюционное развитие аутсорсинга, они осуществляют мониторинг приложений, которые передаются в аренду; 6) ASP-агрегаторы, которые помогают IT-менеджерам предприятий интегрировать работу разных ASP-провайдеров в одном месте. В результате менеджеры организации-клиента могут арендовать все ASP-сервисы в одном месте, обеспечить централизованный доступ к этим службам через Интернет и снять с себя заботы о контроле за их работой. ASP-агрегаторы предлагают свои услуги через партнеров (системных интеграторов, консалтинговые компании и интернет-провайдеров) и ориентируются в первую очередь на предприятия малого и среднего бизнеса[51].

Что же касается предоставления услуг телекоммуникационной связи, то обычно речь идет о договорной конструкции абонентского обслуживания. На территории РФ услуги связи оказываются операторами связи пользователям услугами связи на основании договора об оказании услуг связи, заключенного в соответствии с гражданским законодательством и правилами оказания услуг связи (п. 1 ст. 44 Федерального закона от 07.07.2003 № 126-ФЗ «О связи»[52]). По смыслу ст. ст. 2, 12, 44 Закона о связи предоставление доступа к информационно-телекоммуникационной сети Интернет относится к услугам электросвязи. Договоры, скрываемые под маской абонентского договора, - это прежде всего договоры по оказанию услуг и договоры по выполнению работ. Деловая практика к таким договорам относит договоры на оказание услуг телефонной связи, услуг по трансляции кабельного телевидения, услуг доступа к информационным ресурсам сети

[51] Аникин Б.А., Рудая И.Л. Аутсорсинг и аутстаффинг: высокие технологии менеджмента: учебное пособие. 4-е изд., испр. и доп. Москва: ИНФРА-М, 2022. 313 с.
[52] СЗ РФ. 2003, N 28, ст. 2895.

Интернет, услуг на обслуживание сайта, на оказание комплекса спортивно-оздоровительных услуг, договоры по оказанию юридической помощи, консультативной помощи, договоры подряда по техническому обслуживанию бытовой техники, автомобилей и др.[53]. Как отмечается в научной литературе, абонентский договор – это договорная конструкция, в которую можно облечь, по сути, почти любой возмездный поименованный или непоименованный договор. Абонентская договорная конструкция отличается от обычного способа оформления договорного правоотношения двумя ключевыми признаками. Во-первых, в рамках такого договора одна из сторон (абонент) получает право в течение срока действия договора требовать от другой стороны исполнения в тот момент, в который ей это будет нужно, и в том объеме, который ей будет нужен. Во-вторых, специфика абонентского договора, отличающая его от договора с исполнением по заявкам (вроде договора кредитной линии или договора поставки товара по заявкам), проявляется в порядке фиксации цены. В рамках абонентского договора абонент платит фиксированную плату (обычно в виде периодических платежей), не зависящую от объема затребованного и осуществленного в соответствующий период исполнения[54].

Компании, отвечающие за безопасность, занимаются средствами защиты информации от воздействия вредоносного кода (СЗИ от ВВК), средствами защиты от несанкционированного доступа (СЗИ от НСД), средствами криптографической защиты информации (СКЗИ), например, ЭЦП, средствами организационной защиты информации (пропускной режим и т.д.), средствами инженерно-технической защиты информации (система контроля и управления доступом (СКУД), например, карточки на проход в кабинет, телевизионная система наблюдения и регистрации (ТСНР), видеокамеры. **Для**

[53] Малеина М.Н. Абонентский договор. Комментарий к статье 429.4 Гражданского кодекса РФ // Гражданское право. 2020. N 5. С. 3 - 7.

[54] Договорное право (общая часть): постатейный комментарий к статьям 420 - 453 Гражданского кодекса Российской Федерации / А.К. Байрамкулов, О.А. Беляева, А.А. Громов и др.; отв. ред. А.Г. Карапетов. Москва: М-Логос, 2020. 1425 с.

обеспечения безопасности может заключаться договор на техническое обслуживание информационных и технических систем, используемых для обеспечения безопасности, в том числе сигнализации и видеонаблюдения. Данный договор также по своему виду относится к договору возмездного оказания услуг.

Таким образом, при определении основных субъектов правоотношений на рынке IT-аутсорсинга на основании выделенных IT-функций можно предположить, что данные функции могут осуществляться единым поставщиком услуг на основании договора аутсорсинга или множеством компаний, которые привлекаются на основании различных гражданско-правовых договоров.

Отдельно **необходимо рассмотреть вопрос относительно возможностей использования облачных сервисов.** «Облачные» сервисы представляют собой сложные программно-аппаратные системы (платформы), которые включают несколько структурных элементов: дата-центры (центры обработки данных, облачные хранилища данных) с сетевым и серверным оборудованием, интернет-каналами связи; распределенные файловые системы с использованием аппаратных и виртуальных средств, средств шифрования и защиты; виртуальные операционные системы, ресурсы и приложения, а также веб-сервис с идентификатором (веб-адресом)[55]. В рамках «облачных» сервисов обслуживание может происходить в различных формах, наиболее распространенными среди которых являются следующие: 1) предоставление клиенту программного обеспечения в качестве услуги (Software-as-a-Service Concept); предоставление в качестве услуги клиенту ресурса-платформы с созданной инфраструктурой для дальнейшей ее адаптации и улучшения со стороны клиента (Platform-as-a-Service Concept); предоставление в качестве услуги клиенту ресурсов в виде вычислительных мощностей, возможностей по хранению информации для строительства собственной сетевой "облачной"

[55] Карцхия А.А. Облачные технологии: правовой аспект // Российский юридический журнал. 2018. N 6. С. 162 - 172.

инфраструктуры, аналогичной физической (hardware) структуре (Infrastructure-as-a-Service Concept). Все вышеперечисленные услуги, предоставляемые пользователям, также предполагают осуществление со стороны провайдера поддержки функционирования IT-инфраструктуры, ее обновления и актуализации[56]. Как и при использовании любой технологии, у «облачных» вычислений есть свои минусы, они несут новые риски. Во-первых, пользователь не является владельцем и не имеет доступа к внутренней «облачной» инфраструктуре. Сохранность пользовательских данных сильно зависит от компании провайдера. Во-вторых, отсутствуют общепринятые стандарты в направлении безопасности «облачных» технологий. В-третьих, нет однозначного ответа об ответственности лица, предоставляющего услугу перед заказчиком. В-четвертых, не все договорные формы могут использоваться для заключения договора на использование результатов интеллектуальной деятельности с заказчиком. К преимуществам использования облачных сервисов можно отнести отсутствие необходимости дополнительных инвестиций в IT-инфраструктуру собственной компании, т.к. компания платит «облачному» провайдеру только за использованные «облачные» ресурсы; ответственность за работу программно-аппаратных средств возлагается на «облачного» провайдера; сокращаются расходы на приобретение программных и аппаратных средств и их обновление[57]. Использование «облачных» сервисов позволяет также избавиться от финансовых рисков, связанных с эксплуатацией собственной IT-инфраструктуры: если какой-либо проект организации, связанный с обширным использованием вычислительных мощностей, окажется провальным, то неутилизируемое оборудование не повиснет на балансе

[56] Васильев А.О. Налоговый фокус "облачных" сервисов // Налоги. 2018. N 4. С. 3 - 7.
[57] Жарова А.К., Демьянец М.В., Елин В.М. Предпринимательская деятельность в сети Интернет: монография. М.: ЮРКОМПАНИ, 2014. 440 с.

организации мертвым грузом, такие вычислительные мощности динамически перераспределятся и вернутся в общий пул ресурсов провайдера[58].

Некоторые зарубежные регуляторы установили требования к использованию облачных сервисов. Пункт 12 Руководства Европейской Службы по банковскому надзору (EBA) по аутсорсингу[59] определяет облачные сервисы как сервисы, предоставляемые с использованием облачных вычислительных ресурсов, обеспечивая таким образом повсеместный, удобный сетевой доступ к общему пулу конфигурируемых вычислительных ресурсов (например, к сетевому и серверному оборудованию, системам хранения данных, приложениям и услугам), которые могут быть быстро предоставлены с минимальными усилиями или с минимальным вмешательством со стороны поставщиков услуг. В Руководстве публичный облачный сервис понимается как облачная инфраструктура, доступная для использования неопределенным кругом клиентов, частный облачный сервис как облачная инфраструктура, доступная только одной организации или платежному учреждению, общественный облачный сервис как облачная инфраструктура, доступная для определенной группы организаций или платежных учреждений, в том числе нескольких связанных между собой учреждений, гибридные облачные сервисы представляют собой облачную инфраструктуру, состоящую из двух или более различных облачных инфраструктур. В п. 2.1 Руководящих принципов Банка Маврикия[60] облачные услуги относятся к ресурсам, предоставляемым по требованию через Интернет на основе оплаты за использование. Предложены такие модели, как: а) программное обеспечение как услуга (SaaS), что представляет собой использование общего программного обеспечения или специальных бизнес-приложений, работающих на компьютерах в облаке, но принадлежащих и

[58] Савельев А.И. Правовая природа "облачных" сервисов: свобода договора, авторское право и высокие технологии // Вестник гражданского права. 2015. N 5. С. 62 - 99.

[59] EBA Guidelines on outsourcing arrangements EBA/GL/2019/02 25 February 2019 https://www.eba.europa.eu/sites/default/documents/files/documents/10180/2551996/38c80601-f5d7-4855-8ba3-702423665479/EBA%20revised%20Guidelines%20on%20outsourcing%20arrangements.pdf?retry=1

[60] Guidelines on Outsourcing by Financial Institutions. Revised October 2020. Bank of Mauritius. https://www.bom.mu/sites/default/files/guidelines_on_outsourcing_by_financial_institutions_13.10.2020.pdf

управляемых поставщиками облачных услуг; б) платформа как услуга (PaaS), где предоставляется полноценная цифровая среда для создания и доставки веб-приложений, в то время как покупка, управление и хостинг базового оборудования осуществляется поставщиком облачных услуг; в) инфраструктура как услуга (IaaS), где компаниям предоставляются вычислительные ресурсы, включая серверы, сети, хранилища и пространство центра обработки данных. «Облачные» услуги могут предоставляться через публичные, частные или гибридные облака: публичное облако, в котором услуги и инфраструктура принадлежат и управляются поставщиками услуг и предоставляются за пределами площадки через общедоступную сеть; частное облако, в котором услуги и инфраструктура эксплуатируются исключительно одной организацией, независимо от того, управляются ли они изнутри или третьей стороной и размещаются в частной сети; гибридное облако, построенное на основе частного облака со стратегическим сочетанием общедоступных облачных сервисов. Частное облако - достаточно удобная и эффективная инфраструктура, которая обладает большей гибкостью, чем обычный внутренний сервер. Также частное облако позволяет сократить бюджет и произвести его прогнозирование на будущее. Использование такой облачной технологии служит базой для создания гибкого и безопасного гибридного облака, которое использует лучшие качества публичного и частного облака при решении поставленной задачи. Часто такой тип применяется, когда организация имеет сезонные периоды активности, как только внутренняя IT-инфраструктура не справляется с текущими задачами, часть мощностей перебрасывается на публичное облако (например, большие объемы статистической информации), а также для предоставления пользователям доступа к ресурсам предприятия через публичное облако[61]. Интерес в Руководящих принципах Банка Маврикия[62] также представляет

[61] Берестова В.И. Перспективы использования облачных технологий в электронном документообороте // Делопроизводство. 2015. N 3. С. 39 - 44.

[62] Guidelines on Outsourcing by Financial Institutions. Revised October 2020. Bank of Mauritius. https://www.bom.mu/sites/default/files/guidelines_on_outsourcing_by_financial_institutions_13.10.2020.pdf

выделение облачных услуг как формы аутсорсинга, которая разрешена для повышения эффективности деятельности и обслуживания клиентов. Согласно позиции регулятора Маврикия, использование облачных сервисов финансовыми учреждениями должно быть ограничено только непрофильной деятельностью. **Облачные услуги подвержены тем же рискам, что и другие формы аутсорсинга, то есть они должны подлежать такой же комплексной проверке управлению рисками при подписке**. В документе установлены специальные требования к использованию банком или финансовой организацией облачных сервисов[63]. Отметим, что, например, в Австралии выпущен специальный аналитический документ в отношении использования облачных сервисов в банковской сфере[64].

По российскому праву возникают вопросы, касающиеся природы договора, в соответствии с которым пользователь получает доступ к инфраструктуре оператора облачного сервиса. Речь идет о договоре возмездного оказания услуг, обладающего всеми соответствующими признаками[65]. Следует подчеркнуть, что базовая версия облачного сервиса может представлять собой и безвозмездный договор[66]. Договор доступа к инфраструктуре может быть заключен по конструкции абонентского договора. Отметим, что оговоры аутсорсинга могут быть абонентскими, когда исполнитель (подрядчик) оказывает услуги (выполняет работы) по требованию заказчика.

1.2. Архитектура правоотношений между основными субъектами рынка IT-аутсорсинга:

[63] Guidelines on Outsourcing by Financial Institutions. Revised October 2020. Bank of Mauritius. https://www.bom.mu/sites/default/files/guidelines_on_outsourcing_by_financial_institutions_13.10.2020.pdf

[64] Outsourcing involving cloud computing services. 24 September 2018. https://www.apra.gov.au/sites/default/files/information_paper_-_outsourcing_involving_cloud_computing_services_0.pdf

[65] Карцхия А.А. Облачные технологии: правовой аспект // Российский юридический журнал. 2018. N 6. С. 162 - 172.

[66] Чурилов А.Ю. Правовое регулирование облачного гейминга // Актуальные проблемы российского права. 2022. N 8. С. 83 - 92.

1) в зависимости от создания компании IT-аутсорсера, предоставляющей услуги по всем или большинству IT-функций (модель универсального посредника);

2) в зависимости от передачи отдельных IT-функций банка разным лицам (модель множественности аутсорсеров).

В контексте аутсорсинга IT-услуг в банковской сфере можно выделить две основные модели взаимодействия: модель универсального посредника и модель аутсорсинга с участием нескольких организаций.

Универсальные модели аутсорсинга предполагают передачу IT-услуг провайдеру или вендору. Этот подход прост и прозрачен, так как предлагает централизованное управление, но он может предполагать ограничения с точки зрения гибкости и специализации. Встречаются две распространенные универсальные модели аутсорсинга. **Первая модель – это полный IT-аутсорсинг**, в рамках которого банк или финансовая организация передает все свои IT-функции и услуги единому стороннему поставщику (например, управление инфраструктурой, разработку приложений, службы поддержки и т.д.), при этом сторонний поставщик берет на себя полную ответственность за IT-операции банка. **Вторая модель – это модель управляемых услуг**, в рамках которой банк или финансовая организация передает лишь определенные IT-функции или компоненты одному поставщику управляемых услуг. Например, банк может заключить контракт с поставщиком на управление операциями своего центра обработки данных, сохраняя при этом контроль над другими аспектами IT. Данная классификация **созвучна классификации аутсорсинга в зависимости от разделения ответственности и рисков**, в рамках которой **выделяется полный и частичный (выборочный) аутсорсинг**[67]. Полный аутсорсинг предполагает такие действия, как выполнение сбытовых операций в сети Интернет с разработкой веб-сайта, его пополнение и поддержание, передача внешним

[67] Арабян М.С., Попова Е.В. Таможенный представитель и его место в системе аутсорсинга таможенных услуг // Таможенное дело. 2015. N 2. С. 3 - 5.

исполнителям полномочий по набору сотрудников для определенной компании, полный цикл обучения персонала, управление финансами, недвижимостью, отдельными подразделениями фирмы, выполнение административных функций, документооборот, логистика и т.п. Частичный аутсорсинг предполагает, что предприятие передает часть своих специфических задач, например, программирование веб-сайта, а выработка всей стратегии, ее внедрение в практику остается за самой компанией[68]. Решение о вынесении функции на полный или частичный аутсорсинг должно предусматривать делегирование ответственности за результаты осуществления функции в полной мере или в части[69], при этом банк или финансовая организация будет нести ответственность перед регулятором в любом случае, что будет обосновано далее.

Модели аутсорсинга с участием нескольких организаций предполагают аутсорсинг различных IT-услуг нескольким провайдерам или вендорам. Такой подход позволяет банкам выбирать специализированных поставщиков для выполнения конкретных функций, что потенциально приводит к большей гибкости и экспертному потенциалу. Этот вариант также имеет свои риски, в том числе сложность в координации различных поставщиков, распределение обязанностей между ними, особенно когда переданные на аутсорсинг процессы взаимозависимы[70].

Существуют две распространенные модели множественности аутсорсеров: мультисорсинг и гибридная модель. В **модели мультисорсинга** банк или финансовая организация выбирают нескольких поставщиков для управления различными аспектами своих IT-операций, например, один поставщик может предоставлять услуги облачного хостинга, а другой специализироваться на кибербезопасности. Банк или финансовая организация

[68] Курицкий В.В. Что такое аутсорсинг? Общество и право. 2008. N 1.
[69] Вопрос-ответ // Росимущество: официальный сайт. 2016. URL: http://www.rosim.ru (дата обращения: 25.10.2016).
[70] Reyes Gonzalez, Juan Llopis, Jose Gasco Information technology outsourcing in financial services file:///C:/Users/BelitskayaAV/Downloads/Information_technology_outsourcing_in_fi.pdf

управляют отношениями с этими многочисленными поставщиками услуг и координируют их деятельность. **Гибридная модель** сочетает в себе элементы универсального аутсорсинга и аутсорсинга с участием нескольких организаций и предполагает передачу некоторых IT-функций одному поставщику (универсальный аутсорсинг) и заключение контрактов с другими специализированными поставщиками на предоставление конкретных услуг (аутсорсинг нескольких организаций). Банк сохраняет контроль над существенными функциями, одновременно получая выгоду от специализированного опыта сторонних поставщиков услуг.

Выбор между универсальной моделью аутсорсинга и моделью множественности аутсорсеров зависит от различных факторов, включая направленность IT-стратегии банка, бюджет, толерантность к риску и требуемые конкретные услуги, при этом проводится тщательный процесс оценки, чтобы определить, какая модель аутсорсинга или комбинация моделей лучше всего соответствует потребностям и целям банка. Среди недостатков универсального поставщика услуг можно выделить опасение излишней концентрации значимых процессов в руках одной компании. Организация стремится заключить договор аутсорсинга с несколькими компаниями одновременно, несмотря на то, что такой подход ведет к увеличению издержек, однако он понижает уровень зависимости и снижает риск выращивания конкурента[71].

Анализ международного опыта регулирования IT-аутсорсинга в банковской сфере не позволил выделить страны, которые предпочитают исключительно ту или иную модель аутсорсинга. Вместе с тем можно сделать вывод о том, что в США исторически использовали полный IT-аутсорсинг со стороны крупных игроков в IT сфере. Многие европейские банки также приняли модели универсального аутсорсинга для повышения своей эффективности и конкурентоспособности. В Индии банки и финансовые

[71] Аутсорсинг / С. Ефимова, Т. Пешкова, Н. Коник и др. М.: Журнал "Управление персоналом", 2006. 160 с.

организации часто заключают контракты с несколькими поставщиками услуг, чтобы получить доступ к специализированным навыкам. В банковском секторе Великобритании банки зачастую используют гибридные модели, сочетая внутренние IT-функции с аутсорсинговыми услугами, включая специализированные услуги, такие, как кибербезопасность.

Существуют различные классификации аутсорсинга, в том числе по критерию того, в какой стране находятся компании, которые оказывают аутсорсинговые услуги. Наряду с внутригосударственным аутсорсингом, когда покупатель и продавец соответствующего блага действуют в одном государстве, можно выделить так называемый офшорный (иностранный) аутсорсинг, в котором поставщик услуг аутсорсинга действует в другом государстве, чем их покупатель[72]. Встречается деление аутсорсинга на производственный аутсорсинг, когда продаваемое аутсорсером благо представляет собой материальный объект (вещь), и аутсорсинг услуг (функций) - так называемый аутсорсинг сервиса, при котором соответствующим благом является нематериальный объект (функция, услуга)[73].

Эксперты предлагают и другие классификации, в частности классификацию, основанную на стиле транзакций и принципе закупок.

Согласно первому параметру можно выделить транзакции, которые относятся к разовым или краткосрочным контрактам, и отношения, которые относятся к долгосрочным контрактам. Договоры аутсорсинга заключаются, как правило, с целью краткосрочного привлечения непрофильных специалистов для реализации отдельных корпоративных программ или долгосрочного сотрудничества по ряду услуг или выполнению работ без увеличения штата собственных работников[74], при этом для

[72] Kedia B., Mukherjee D. Understanding Ottshoring: A Research Framework Based on Disintegration, Location and Externalisation Advantages // Journal of World Business, 2009. Vol. 44. P. 250. N 2.
[73] Mclvor R. Global Services Outsourcing - Cambridge, 2010. P. 7, 11, 12 и др.
[74] Хорват О., Севастьянова Ю. Аутсорсинг и аутстаффинг в банке - экономический эффект или социальные и налоговые риски? // СПС КонсультантПлюс. 2014.

краткосрочного сотрудничества может подойти модель множественности аутсорсеров, тогда как для долгосрочных отношений подходит универсальная модель или гибридная модель. В отличие от услуг сервиса и поддержки, имеющих разовый, эпизодический характер и ограниченных временными рамками, на аутсорсинг обычно передаются функции по профессиональной поддержке бесперебойной работоспособности отдельных систем и инфраструктуры на основе длительного контракта (не менее 1 года)[75], аутсорсер осуществляет не некоторое разовое исполнение или несколько отдельных таких исполнений, а постоянно участвует в текущей деятельности покупателя (заказчика)[76]. В отличие от субподряда, аутсорсинг - это стратегия на перспективу, которая влечет за собой серьезную перестройку внутри компании[77]. Как указывают эксперты, долгосрочный IT-аутсорсинг следует рассматривать не просто как контракт, но и как отношения, в которых клиент и поставщик(и) связаны через отдельных менеджеров в течение всего срока взаимодействия. Критериями долгосрочного успеха IT-аутсорсинга являются набор реалистичных, измеримых и открытых для обеих сторон контракта ожиданий. До момента заключения контракта обе стороны должны проявить должную осмотрительность, чтобы обеспечить хорошее соответствие спроса и предложения[78].

Параметр принципа закупок может быть ориентирован на затраты или на результат. Используя опцию затрат, компании закупают ресурсы у поставщиков, но напрямую управляют своей IT-деятельностью. В соответствии с концепцией альтернативной стоимости затраты по проекту, передаваемому фирмой-заказчиком в аутсорсинг, всегда должны сравниваться со стоимостью реализации проекта своими силами либо через совместное

[75] Райзберг Б.А., Лазовский Л.Ш., Старадубцева Е.Б. Современный экономический словарь. 5-е изд., перераб. и доп. М.: ИНФРА-М, 2007. С. 15.
[76] Ковалевский А.М. Определение и экономико-юридический смысл аутсорсинга // Социальное и пенсионное право. 2015. N 4. С. 3 - 10; 2016. N 1. С. 3 - 8.
[77] Актуальные новости ("Налоги" (газета), 2009, N 12)
[78] Dr. Ming Luong, Dr. Jeff Stevens A Multi-Stage Maturity Model for Long-Term IT Outsourcing Relationship Success https://files.eric.ed.gov/fulltext/EJ1141766.pdf

предприятие[79]. При опции, ориентированной на результат, поставщики услуг самостоятельно управляют реализацией IT-деятельности.

В результате сопоставления выделенных параметров можно выявить **четыре различных вида контракта**: «покупай» (Buy-in), предпочтительный поставщик, «нанимай» (Contract-out), предпочтительный подрядчик. **Ориентированными на результат являются контракты «нанимай» и предпочтительный подрядчик, именно они рассматриваются как аутсорсинговые контракты**. **В стратегии контракта «нанимай» вендор несет ответственность за полученные результаты IT-деятельности**. Успех этой стратегии часто зависит от надежного контракта, который определяет полный набор обязанностей для вендора. Из-за своего краткосрочного характера стратегия «нанимай» иногда сводится к оппортунистическим действиям в поведении вендора. **Стратегия предпочтительного подрядчика предполагает, что организация заключает долгосрочный контракт с поставщиком услуг, чтобы снизить риск оппортунистического поведения**. Поставщик несет ответственность за управление и реализацию IT-деятельности. Этот вариант отличается от предыдущего тем, что договор имеет долгосрочный характер. **Стратегия «покупай»** эффективна тогда, когда организации прибегают к помощи внешних консультантов для удовлетворения временной потребности, например, на определенной стадии осуществления проекта. **Стратегия предпочтительного поставщика** основана на подходе «покупай», при этом организация-пользователь сторонних услуг стремится разработать долгосрочное взаимодействие с поставщиком, чтобы получить доступ к его ресурсам для осуществления текущей IT-деятельности. Как в стратегии «покупай», так и в стратегии предпочтительного поставщика организация-клиент нанимает ресурсы, но она, привлеченная компания не является в полном смысле поставщиком услуг,

[79] Аутсорсинг / С. Ефимова, Т. Пешкова, Н. Коник и др. М.: Журнал "Управление персоналом", 2006. 160 с.

не несет ответственность за управление этими ресурсами для достижения требуемых результатов[80].

Рассматривая схемы аутсорсинга, отечественные ученые отмечают, что постоянная приверженность заказчика только одной из основных схем кооперации (организации) разделенной деятельности при меняющихся экономических условиях может не обеспечить экономическую эффективность данной деятельности (труда). Подобное обстоятельство предполагает, что, кроме чистых схем координации на практике должны существовать и использоваться в целях обеспечения непрерывности, устойчивости и экономической эффективности деятельности (труда) в целом некие смешанные (переходные) схемы кооперации (организации) применительно к аутсорсингу[81].

Архитектуру правоотношений между основными субъектами рынка IT-аутсорсинга составляют помимо договорной стадии так же стадия предварительной проверки, а также стадии мониторинга и контроля, которые необходимы при передаче услуг на аутсорсинг, особенно в банковской сфере. Так, в Пруденциальном стандарте австралийского регулятора APRA[82] установлено, что все соглашения об аутсорсинге, касающиеся существенных видов деятельности банков и финансовых организаций, находящихся под надзором APRA, должны пройти соответствующую комплексную проверку, быть одобрены со стороны APRA и подлежать постоянному мониторингу. APRA устанавливает, что все риски, возникающие в результате существенных видов деятельности, должны быть надлежащим образом оценены, и гарантировано, что банк или финансовая организация способны выполнять свои финансовые и сервисные обязательства перед вкладчиками и/или страхователями. Ключевые требования Пруденциального стандарта

[80] Maddalena Sorrentino The Outsourcing of IT Services in Banking: Beyond the Transaction Cost Framework https://www.academia.edu/28336047/The_Outsourcing_of_IT_Services_in_Banking_Beyond_the_Transaction_Cost_Framework

[81] Ковалевский А.М. Правовая природа договора аутсорсинга в аспекте разрешения социально-экономических проблем // Социальное и пенсионное право. 2017. N 4. С. 3 - 9; 2018. N 1. С. 10 - 17; N 2. С. 3 - 7.

[82] Prudential Standard CPS 231 Outsourcing July 2017 https://www.apra.gov.au/sites/default/files/Prudential-Standard-CPS-231-Outsourcing-%28July-2017%29.pdf

заключаются, в том числе в том, чтобы проконсультироваться с APRA перед заключением соглашений о передаче услуг на аутсорсинг поставщикам услуг, которые ведут свою деятельность за пределами Австралии и уведомлять APRA в течение 20 дней после заключения соглашений о передаче осуществления существенных видов деятельности на аутсорсинг. Соглашение об аутсорсинге должно включать пункт, разрешающий APRA доступ к документации и информации, связанными с соглашением об аутсорсинге, при этом сами банк или финансовая организация должны проводить мониторинг и аудит того, что происходит в рамках аутсорсинга[83].

Рассмотрим каждую стадию.

На преддоговорной стадии должна быть проведена комплексная проверка как самого поставщика услуг, так и деятельности, которую он осуществляет. Банк или финансовая организация, которые передают IT деятельность на аутсорсинг, должны иметь комплексную внутреннюю политику, позволяющую оценить, может ли эта деятельность быть передана на аутсорсинг, и если да, то каким образом. Банк или финансовая организация должны разработать комплексную систему управления рисками аутсорсинга, которая позволит как управлять рисками, связанными с самой деятельностью, так и рисками, связанными с поставщиками услуг. Финансовая служба должна гарантировать, что соглашения об аутсорсинге не уменьшают ее способность выполнять свои обязательства перед клиентами и регуляторами и не препятствуют эффективному надзору со стороны регуляторов за деятельностью банков и финансовых организаций. Кроме того, финансовая служба должна провести соответствующую комплексную проверку при выборе сторонних поставщиков услуг[84]. Прежде чем заключить контракт, необходимо определиться с предметом взаимодействия и теми услугами, которые передаются на аутсорсинг, с количеством поставщиков

[83] Prudential Standard CPS 231 Outsourcing July 2017 https://www.apra.gov.au/sites/default/files/Prudential-Standard-CPS-231-Outsourcing-%28July-2017%29.pdf

[84] Данные требования установлены почти во всех руководящих принципах регулятора, например, п. 5.3, 5.4 руководящих принципов Сингапура

услуг, финансовыми договоренностями в отношении цены и порядка оплаты услуг, сроком контракта, правом собственности на оборудование[85].

Стадии мониторинга и контроля будут подробно описаны далее, отметим лишь, что **мониторинг деятельности в рамках аутсорсинга должен проводиться прежде всего самим банком или финансовой организацией с определенной регулярностью, и лишь в некоторых случаях проверки должны осуществляться также со стороны регулятора, выполняющего в основном контрольно-надзорные функции.**

Что же касается договорных правоотношений между основными субъектами рынка IT-аутсорсинга, то большое разнообразие юридических конструкций, которые опосредуют отношения по аутсорсингу, является одним из свидетельств того, что значительное число бизнес-процессов (в широком смысле), имеющих место в организациях и связанных с управлением, производством, снабжением и пр. - от самых элементарных до самых сложных, могут являться предметом аутсорсинга[86]. Отношения IT-аутсорсинга, как правило, должны регулироваться письменными договорами, в которых четко описывается каждый существенный аспект отношений аутсорсинга, включая права, обязанности и ожидания сторон. Банк или финансовая организация вместе со своими поставщиками услуг должны создать и поддерживать планы действий в чрезвычайных ситуациях, включая план аварийного восстановления работы системы и периодического тестирования резервных объектов. Необходимо обеспечить также конфиденциальность информации, с которой работают сторонние поставщики IT-услуг[87].

---

[85] Reyes Gonzalez, Juan Llopis, Jose Gasco Information technology outsourcing in financial services file:///C:/Users/BelitskayaAV/Downloads/Information_technology_outsourcing_in_fi.pdf

[86] Ковалевский А.М. Определение и экономико-юридический смысл аутсорсинга // Социальное и пенсионное право. 2015. N 4. С. 3 - 10; 2016. N 1. С. 3 - 8.

[87] Reyes Gonzalez, Juan Llopis, Jose Gasco Information technology outsourcing in financial services file:///C:/Users/BelitskayaAV/Downloads/Information_technology_outsourcing_in_fi.pdf

Действующее российское гражданское право не знает определения договоров аутсорсинга[88]. **С юридической точки зрения аутсорсинг представляет собой договор возмездного оказания услуг** внешнего исполнителя - специализированной фирмы для выполнения ею определенной деятельности в пользу организации-заказчика, то есть выполнение каких-либо функций, чаще всего непрофильных для организации[89]. По договору возмездного оказания услуг исполнитель обязуется по заданию заказчика оказать услуги (совершить определенные действия или осуществить определенную деятельность), а заказчик обязуется оплатить эти услуги (ч. 1 ст. 779 ГК РФ). В научной литературе информационная услуга определяется как действия с информацией (поиск, обработка, хранение и (или) передача), направленные на удовлетворение информационных потребностей услугополучателя[90].

В международной практике встречаются следующие виды контрактов, которые в различных правопорядках регулируются по-разному.

Во-первых, необходимо назвать **генеральное соглашение об оказании услуг**, которое представляет собой **основополагающий документ, содержащий общие положения и условия аутсорсинговых отношений**. Он охватывает аспекты высокого уровня, такие, как объем услуг, структура ценообразования, права интеллектуальной собственности, ответственность, разрешение споров и положения о прекращении действия соглашения. Данный контракт часто служит рамочным соглашением, которое применяется к нескольким проектам или услугам. Генеральное соглашение об оказании услуг подходит для универсальных моделей аутсорсинга, хотя может быть в целом применен и в моделях множественности аутсорсеров.

---

[88] Витко В.С., Цатурян Е.А. Юридическая природа договоров аутсорсинга и аутстаффинга. М.: Статут, 2012. 128 с.

[89] Арабян М.С., Попова Е.В. Таможенный представитель и его место в системе аутсорсинга таможенных услуг // Таможенное дело. 2015. N 2. С. 3 - 5.

[90] Дорохова Н.А. Договоры об оказании информационных услуг: монография. Москва: Проспект, 2022. 176 с.

Во-вторых, это соглашение об уровне обслуживания, которое представляет собой подробный контракт, определяющий **конкретные показатели производительности и уровни обслуживания, которым должен соответствовать аутсорсинговый поставщик**. Эти показатели могут включать время отклика, доступность системы, частоту ошибок и стандарты качества. Соглашения об уровне обслуживания часто предусматривают штрафы или поощрения в зависимости от результатов работы согласно отчетам. Представляется, что данный вид контракта больше подходит для моделей множественности аутсорсеров, хотя может быть применен и в универсальных моделях.

В-третьих, это соглашение об обработке данных, которое имеет решающее значение, когда аутсорсинг предполагает обработку личных или конфиденциальных данных, таких как финансовая информация клиентов. В нем **описывается, как данные будут обрабатываться, защищаться и обеспечиваться в соответствии с правилами защиты данных и конфиденциальности**. Данный контракт обычно касается доступа к данным, их хранению, уведомлениям о нарушениях. Представляется, что данный контракт специфичен и подходит для моделей множественности аутсорсеров, где обязанности распределены между различными поставщиками услуг, иначе данные вопросы можно было бы урегулировать в генеральном соглашении об оказании услуг или соглашении об уровне обслуживания.

В-четвертых, в рамках правоотношений между основными субъектами рынка IT-аутсорсинга может заключаться **соглашение о неразглашении информации**, которое используется для защиты конфиденциальной информации и коммерческой тайны, передаваемой во время переговоров по контракту или в рамках аутсорсинговых отношений. Контракт запрещает несанкционированное раскрытие конфиденциальных данных и устанавливает обязательства обеих сторон в отношении конфиденциальности. Вопросы конфиденциальности можно урегулировать также в генеральном соглашении об оказании услуг или соглашении об уровне обслуживания.

Наряду с вышеперечисленными договорами можно также заключить **соглашение об аудите и соблюдении требований**, которое предоставляет банку право проводить аудит и оценку деятельности аутсорсингового провайдера, мер безопасности и соблюдения договорных и нормативных требований. Возможно также подписать протоколы управления изменениями, которые определяют процедуры внесения изменений в соглашение об аутсорсинге. Они охватывают изменения в услугах, соглашениях об уровне обслуживания, ценах или объеме работ. В соглашениях о расторжении описываются условия и процессы прекращения аутсорсинговых отношений. Можно заключить соглашение о плане обеспечения непрерывности бизнеса и аварийного восстановления, соглашение о механизме разрешения споров, соглашение о соответствии нормативным требованиям. **Все перечисленные соглашения могут войти в качестве разделов в генеральное соглашение об оказании услуг или соглашение об уровне обслуживания.**

Важным вопросом в отношении архитектуры правоотношений между основными субъектами рынка IT-аутсорсинга **является форма заключения договора IT-аутсорсинга, а также необходимость сообщать о заключении такого договора в уведомительном порядке регулятору или необходимость получать одобрение регулятора на заключение такого договора.**

В большинстве юрисдикций установлены **требования к письменной форме заключения соглашения об IT-аутсорсинге**. Так, в Заявлении надзорного органа Великобритании[91] установлено требование письменной формы договора аутсорсинга вне зависимости от того, находятся ли поставщики услуг внутри группы с банком или финансовой организации или являются сторонними поставщиками услуг. В Руководящих принципах

[91] Supervisory Statement | SS2/21 Outsourcing and third party risk management March 2021 https://www.bankofengland.co.uk/-/media/boe/files/prudential-regulation/supervisory-statement/2021/ss221-march-21.pdf

регулятора Танзании[92] установлено, что все соглашения об аутсорсинге должны оформляться письменным договором, который должен быть согласован регулятором до его заключения в письменной форме. По мнению регулятора Таиланда, нестратегические существенные функции могут быть переданы на аутсорсинг с предварительного одобрения Банка Таиланда, несущественные функции могут быть переданы на аутсорсинг без предварительного одобрения[93]. В Пруденциальном стандарте австралийского регулятора APRA[94] прописано, что необходимо уведомлять APRA в течение 20 дней после заключения соглашений о передаче осуществления существенных видов деятельности на аутсорсинг, а также предварительно консультироваться в заключении соглашений о передаче услуг на аутсорсинг поставщикам услуг, которые ведут свою деятельность за пределами Австралии.

Основной проблемой контрактов по разработке и реализации аутсорсинговых проектов становится проблема разделения рисков и вознаграждения, а также учет интересов заказчика и исполнителя аутсорсингового проекта, которые непосредственно связаны с оценкой эффективности данного проекта[95]. **Различные страны устанавливают минимальные требования к условиям соглашений аутсорсинга, которые могут отличаться друг от друга.**

Так, в Пруденциальном стандарте Австралии[96] (п. 29) установлено, что в соглашении, как минимум, должны быть урегулированы вопросы предмета соглашения и перечня предоставляемых услуг, срока соглашения, положения о пересмотре соглашения, цены и порядка оплаты услуг, уровней

---

[92] Outsourcing guidelines for banks and financial institutions. 2021. Bank of tanzania. https://www.bot.go.tz/Publications/Acts,%20Regulations,%20Circulars,%20Guidelines/Guidelines/en/20210630152 41391.pdf

[93] Notification of the Bank of Thailand No. FPG 8/ 2557 Re: Regulations on Outsourcing of Financial Institutions https://www.bot.or.th/content/dam/bot/fipcs/documents/FPG/2558/EngPDF/25580002.pdf

[94] Prudential Standard CPS 231 Outsourcing July 2017 https://www.apra.gov.au/sites/default/files/Prudential-Standard-CPS-231-Outsourcing-%28July-2017%29.pdf

[95] Аутсорсинг / С. Ефимова, Т. Пешкова, Н. Коник и др. М.: Журнал "Управление персоналом", 2006. 160 с.

[96] Prudential Standard CPS 231 Outsourcing July 2017 https://www.apra.gov.au/sites/default/files/Prudential-Standard-CPS-231-Outsourcing-%28July-2017%29.pdf

обслуживания и требований к производительности, формы, в которой должны храниться данные, положений, определяющих владение и контроль данных, требований к отчетности, включая содержание и частоту отчетности, процедуры аудита и мониторинга, управления непрерывностью бизнеса, конфиденциальности и безопасности информации, соглашения о невыполнении обязательств и положения о прекращении действия, механизмов разрешения споров, ответственности и возмещения ущерба, субподряда, страхования, работ с оффшорами. В Руководящих принципах по аутсорсингу, выпущенных Валютным управлением Сингапура[97] (п. 5.5.2), закреплено, что должны быть также установлены стандарты производительности, операционной деятельности, внутреннего контроля и управления рисками, должны быть указаны случаи и обстоятельства, при которых поставщик услуг обязан сообщить о происшествии регулятору, установлен срок, в течение которого осуществляется расторжение соглашения после принятии решения о раннем расторжении, чтобы обеспечить плавность передачи осуществления услуг. В Руководящих принципах Канады[98] (п. 7.2.1) также встречаются интересные минимальные требования к условиям соглашения об аутсорсинге. В частности, ожидается, что в соглашении об аутсорсинге будет указан тип и частота информации, которую банк или финансовая организация будут получать от поставщика услуг, включая отчеты, которые позволят оценить, соблюдаются ли показатели эффективности, а также любую другую информацию, необходимую для мониторинга. Кроме того, ожидается, что соглашение об аутсорсинге будет включать процедуры и требования к поставщику услуг в отношении оповещения банка или финансовой организации о событиях, которые могут иметь потенциальную возможность существенно повлиять на предоставление

[97] Guidelines on Outsourcing. Monetary Authority of Singapore. 27 July 2016. https://www.mas.gov.sg/-/media/mas/regulations-and-financial-stability/regulatory-and-supervisory-framework/risk-management/outsourcing-guidelines_jul-2016-revised-on-5-oct-2018.pdf

[98] Outsourcing of Business Activities, Functions and Processes https://www.osfi-bsif.gc.ca/Eng/fi-if/rg-ro/gdn-ort/gl-ld/Pages/b10.aspx#toc7.2.1

услуги. Кроме того, согласно требованиям канадского регулятора, в соглашении должна быть четко установлена идентификация в отношении прав собственности на все активы (интеллектуальные и физические), связанные с соглашением об аутсорсинге, включая активы, созданные или приобретенные в соответствии с соглашением об аутсорсинге. В контракте или соглашении об аутсорсинге должно быть также указано, имеет ли поставщик услуг право использовать активы банка или финансовой организации, и каким образом (например, данные, аппаратное и программное обеспечение, системную документацию или интеллектуальную собственность), а также право банка или финансовой организации на доступ к этим активам. В минимальных требованиях, которые установлены в Руководящих принципах Банка Танзании[99] (п. 17), среди прочего содержится требование об установлении запрета уступки договора третьему лицу без согласия банка или предварительного согласия финансовой организации. Кроме того, регулятором Танзании в качестве обязательных минимальных требований указано на определение ответственности и возмещения в случае невыполнения, задержки или ошибочных транзакций, обработанных поставщиком аутсорсинговых услуг, закрепление права банка на физический доступ в любое время к помещениям или оборудованию, положение о признании права банка инициировать проверку поставщика услуг, его документов и счетов. Согласно Руководящим принципам регулятора Сингапура[100], договор аутсорсинга должен содержать пункты, устанавливающие правила и ограничения на субподряд, в том числе право требовать, чтобы поставщик услуг нес договорную ответственность за производительность и риски своего субподрядчика. В Руководящих

[99] Outsourcing guidelines for banks and financial institutions, 2021 https://www.bot.go.tz/Publications/Acts,%20Regulations,%20Circulars,%20Guidelines/Guidelines/en/20210630152241391.pdf

[100] Guidelines on Outsourcing. Monetary Authority of Singapore. 27 July 2016. https://www.mas.gov.sg/-/media/mas/regulations-and-financial-stability/regulatory-and-supervisory-framework/risk-management/outsourcing-guidelines_jul-2016-revised-on-5-oct-2018.pdf

принципах Банка Маврикия[101] (п. 3.5.2) закреплено, что соглашение не должно содержать положений, которые препятствовали бы регулятору осуществлять свои надзорные полномочия. Банк Маврикия должен иметь такое же право доступа к информации в отношении поставщика услуг, как и в отношении финансовых организаций, которые привлекают по аутсорсингу. Контракт должен прямо предусматривать выезды на места и беспрепятственные проверки переданной на аутсорсинг деятельности со стороны финансовых учреждений и регулятора. Контракт должен содержать пункт о получении предварительного одобрения регулятора в случае субподряда на выполнение существенных видов деятельности, которая была передана финансовым учреждением на аутсорсинг любой другой организации. Согласно требованиям Директивы Резервного банка Индии[102] соглашение об аутсорсинге должно отвечать параметру обеспечения его эффективной принудительной реализации и соблюдения применимого законодательства. Директива определяет, какие условия должны содержаться в договоре. Среди таких условий названы четкая идентификация и описание аутсорсинговых услуг, включая стандарты деятельности для поставщика услуг и субподрядчиков, обеспечение доступа регулируемых организаций к данным и документам поставщика услуг, права регулируемых лиц на мониторинг и аудит в отношении деятельности компаний, оказывающих услуги по аутсорсингу, обязательство поставщиков услуг сообщать о любых существенных неблагоприятных инцидентах (таких, как утечка данных, недоступность или перебои в предоставлении услуг), право регулируемых организаций вмешиваться в деятельность компаний, оказывающих услуги по аутсорсингу, и принимать соответствующие меры для обеспечения соблюдения законодательных и нормативных требований; право регулируемых организаций совершать иные действия, такие, как назначение

[101] Guidelines on Outsourcing by Financial Institutions. Revised October 2020. Bank of Mauritius. https://www.bom.mu/sites/default/files/guidelines_on_outsourcing_by_financial_institutions_13.10.2020.pdf
[102] Outsourcing of IT Services by Banks and Financial Institutions - Overview of the Regulatory Regime and the Key Takeaways May 12 2023 https://www.lexology.com/library/detail.aspx?g=ac19aa69-3751-4814-b5ad-98f1837dfa13

субподрядчиков поставщиков услуг для всей или части переданной на аутсорсинг деятельности и право на прекращение аутсорсинговой деятельности, в том числе право регулируемой организации передать другому поставщику услуг переданную на аутсорсинг деятельность.

Существенными условиями договора признаются условия, без согласования которых договор не будет считаться заключенным. Существенными условиями договора являются: условие о его предмете, условия, существенные для договоров данного вида в силу закона или иных правовых актов, а также все те условия, относительно которых по заявлению одной из сторон должно быть достигнуто соглашение. **Существенными условиями договора возмездного оказания услуг по ГК РФ признается предмет, иногда также в судебной практике срок и цена, что должно быть отражено в договоре аутсорсинга.** Важно отметить, что согласно п. 1 ст. 422 ГК РФ, договор должен соответствовать обязательным для сторон правилам, установленным законом и иными правовыми актами (императивным нормам), действующим в момент его заключения. То есть **в случае, если регулятор установит необходимость включения в договор аутсорсинга определенных условий, стороны такого договора будут обязаны соблюдать данное требование.** Помимо необходимости определения существенных условий и выполнения требований регулятора, установленных в правовых актах, необходимо отметить, что стороны свободны в заключении договора и определении его условий. Так, в Постановлении Пленума Высшего Арбитражного Суда Российской Федерации от 14.03.2014 N 16 «О свободе договора и ее пределах» разъяснено, что в соответствии с п. 2 ст. 1 и ст. 421 ГК РФ граждане и юридические лица свободны в установлении своих прав и обязанностей на основе договора и в определении любых не противоречащих законодательству условий договора.

В научной литературе отмечается, что для договоров об оказании информационных услуг единственным существенным условием является условие о предмете. Предмет договора по поиску, обработке, хранению и (или)

передаче информации составляют информация и действия с ней (поиск, обработка, хранение и/или передача)[103]. **Предмет соглашения должен включать в себя перечень и описание предоставляемых услуг, которые передаются на аутсорсинг (четкая идентификация и описание аутсорсинговых услуг)**. По российскому праву договор возмездного оказания услуг может считаться заключенным, если в нем **перечислены определенные действия, которые обязан совершить исполнитель, либо указана определенная деятельность, которую он обязан осуществить**. В том случае, когда предмет договора обозначен указанием на конкретную деятельность, круг возможных действий исполнителя может быть определен на основании предшествующих заключению договора переговоров и переписки, практики, установившейся во взаимных отношениях сторон, обычаев делового оборота, последующего поведения сторон и т.п. (ст. 431 ГК РФ). Поскольку стороны в силу ст. 421 ГК РФ вправе определять условия договора по своему усмотрению, обязанности исполнителя могут включать в себя не только совершение определенных действий (деятельности), но и представление заказчику результата действий исполнителя[104]. Определяя исчерпывающим образом такое существенное условие договора, как его предмет, федеральный законодатель не включил в понятие предмета договора возмездного оказания услуг достижение результата, ради которого он заключается. Выделение в качестве предмета данного договора совершения определенных действий или осуществления определенной деятельности обусловлено тем, что даже в рамках одного вида услуг результат, ради которого заключается договор, в каждом конкретном случае не всегда достижим, в том числе в силу объективных причин. Следовательно, заключая договор возмездного оказания услуг, стороны, будучи свободны в определении цены договора, сроков его

[103] Дорохова Н.А. Договоры об оказании информационных услуг: монография. Москва: Проспект, 2022. 176 с.

[104] П. 1 Информационного письма Президиума ВАС РФ от 29.09.1999 N 48 «О некоторых вопросах судебной практики, возникающих при рассмотрении споров, связанных с договорами на оказание правовых услуг»

исполнения, порядка и размера оплаты, вместе с тем не вправе изменять императивное требование закона о предмете данного договора[105].

По вопросу о том, является ли **условие о сроке оказания услуг** существенным для договора возмездного оказания услуг, существует две противоположные позиции судов[106]. В п. 8. Информационного письма Президиума ВАС РФ от 25.02.2014 N 165 отмечено, что отсутствие согласованного сторонами условия о сроках оказания услуг само по себе не влечет признания договора возмездного оказания услуг незаключенным. Вместе с тем **срок оказания услуг имеет важное значение для передачи IT-услуг на аутсорсинг и должен быть отражен в договоре об IT-аутсорсинге.** Большинство зарубежных сран указывает определение срока в качестве одного из минимально необходимых условий, которые должны быть отражены в таком договоре.

Согласно п. 1 ст. 781 ГК РФ, заказчик **обязан оплатить оказанные ему услуги в сроки и в порядке, которые указаны в договоре возмездного оказания услуг** (в судебной практике существуют противоположные позиции о том, считается ли цена существенным условием[107]). Исходя из положений ст.ст. 779, 781 ГК РФ, стоимость услуг, не являющаяся существенным условием договора оказания услуг, не является его невосполнимым условием: тот факт, что по цене услуг отсутствует прямо выраженное в письменной форме волеизъявление сторон, не является основанием для отказа во

---

[105] П. 3.1 Постановления Конституционного Суда РФ от 23.01.2007 N 1-П "По делу о проверке конституционности положений пункта 1 статьи 779 и пункта 1 статьи 781 Гражданского кодекса Российской Федерации в связи с жалобами общества с ограниченной ответственностью "Агентство корпоративной безопасности" и гражданина В.В. Макеева"

[106] Не является (Постановление Арбитражного суда Дальневосточного округа от 21.01.2021 N Ф03-5806/2020 по делу N А04-1849/2020, Определение ВАС РФ от 23.12.2011 N ВАС-16329/11 по делу N А46-14757/2010; Определение ВАС РФ от 17.02.2011 N ВАС-967/11 по делу N А40-26577/10-134-194; Постановление Арбитражного суда Волго-Вятского округа от 18.07.2017 N Ф01-2678/2017 по делу N А43-26462/2016 и др.), является (Постановление ФАС Уральского округа от 19.01.2011 N Ф09-11412/10-С3 по делу N А76-9405/2010-61-368; Постановление ФАС Дальневосточного округа от 22.08.2011 N Ф03-3755/2011 по делу N А16-48/2011 и др.).

[107] В отдельных решениях судебной практики цена считается существенным условием, и договор считается незаключенным (Постановление Арбитражного суда Дальневосточного округа от 21.06.2022 N Ф03-2294/2022 по делу N А24-478/2021; Постановление Арбитражного суда Московского округа от 01.12.2016 N Ф05-12111/2016 по делу N А40-185818/2014). В других представлена противоположная позиция Постановление Арбитражного суда Северо-Западного округа от 13.02.2020 N Ф07-699/2020 по делу N А52-4251/2018; Определением Верховного Суда РФ от 26.05.2020 N 307-ЭС20-6822.

взыскании стоимости услуг, так как к соответствующим отношениям сторон могут быть применены общие положения ГК РФ о гражданско-правовых договорах и обязательствах, в частности п. 3 ст. 424 ГК РФ, согласно которому в случаях, когда в возмездном договоре цена не предусмотрена и не может быть определена исходя из условий договора, исполнение договора должно быть оплачено по цене, которая при сравнимых обстоятельствах обычно взимается за аналогичные услуги[108]. Зачастую оплата услуг исполнителя в договоре ставится в зависимость от действия или решения государственного органа или третьих лиц (так называемый гонорар успеха) либо от достижения иного результата. Аналогично может быть поставлен под условие срок выплаты вознаграждения. На практике возникает вопрос о правомерности оплаты услуг под таким условием, но обычно речь идет о гонораре успеха адвокатов. Представляется, что оплата услуг аутсорсера может быть поставлена в зависимость от того результата, которого они достигли, особенно, когда речь идет о модели универсального аутсорсера, который в целом должен отвечать за результат осуществления IT-функции. **Стороны вправе включить в договор условие о том, что размер вознаграждения исполнителя зависит от достижения им определенного результата**, если он не обусловлен действиями и решениями органов государственной власти либо такое условие не противоречит публичному порядку РФ[109]. Это касается, например, **требований (стандартов) к производительности стороннего поставщика услуг**, которые называются зарубежными регуляторами, как было отмечено выше, одним из минимально необходимых условий, по которым должны договориться стороны договора аутсорсинга. Отметим, что исходя из судебной практики, заказчик не обязан оплачивать частично

[108] Постановление Арбитражного суда Северо-Западного округа от 13.02.2020 N Ф07-699/2020 по делу N А52-4251/2018; Определением Верховного Суда РФ от 26.05.2020 N 307-ЭС20-6822

[109] Постановление Арбитражного суда Волго-Вятского округа от 22.09.2021 N Ф01-5026/2021 по делу N А79-9011/2020; Постановление ФАС Московского округа от 09.06.2012 по делу N А40-81010/11-120-655; Постановление Арбитражного суда Поволжского округа от 30.11.2017 N Ф06-26787/2017 по делу N А12-4175/2016

оказанные услуги, если поэтапная оплата в договоре не предусмотрена и определенный в нем результат не достигнут[110].

Вместе с тем существует и иная **модель оплаты услуг на основе абонентской платы, которая также может быть применена к договорам аутсорсинга, причем как в универсальной модели, так и в модели со множественностью аутсорсеров**. Условие об абонентской плате формулируется в договоре как обязанность заказчика ежемесячно вносить одинаковую плату, если в этом месяце заказчик не отказывался от потребления услуг. В силу п. 1 и 2 ст. 429.4 ГК РФ плата по абонентскому договору может как устанавливаться в виде фиксированного платежа, в том числе периодического, так и заключаться в ином предоставлении (например, отгрузка товара), которое не зависит от объема запрошенного от другой стороны (исполнителя) исполнения[111]. Условие об абонентской плате содержится в договорах с неограниченным объемом потребления услуг, а также в договорах, по которым из установленного перечня услуги оказываются по мере. В такой модели договора заказчик обязан вносить абонентскую плату независимо от объема оказанных услуг[112], что в некоторых случаях подходит для договора аутсорсинга, когда поставщик услуг оказывает техническую поддержку и при необходимости консультационные услуги или услуги по починке оборудования и т.д.

В минимальных требованиях зачастую значится **условие договора аутсорсинга о порядке пересмотра соглашения.** Так, по российскому праву, в договоре можно установить запрет на его изменение в связи с существенным изменением обстоятельств (п. 1 ст. 451 ГК РФ), если стороны хотят придать договорным отношениям стабильность и неизменность. Если в договоре не указано, что стороны не вправе требовать изменения договора в связи

---

[110] Постановление ФАС Западно-Сибирского округа от 03.09.2009 N Ф04-4384/2009(10956-А75-11) по делу N А75-506/2009/;

[111] П. 33 Постановления Пленума Верховного Суда РФ от 25.12.2018 N 49

[112] Постановление Арбитражного суда Северо-Западного округа от 12.01.2022 N Ф07-17808/2021 по делу N А13-18074/2020; Постановление Арбитражного суда Дальневосточного округа от 24.06.2019 N Ф03-2187/2019 по делу N А04-3893/2018; Постановление Арбитражного суда Западно-Сибирского округа от 18.04.2019 N Ф04-1232/2019 по делу N А45-10587/2018

существенным изменением обстоятельств, заинтересованная сторона вправе обратиться в суд с таким требованием (пп. 2 п. 1 ст. 450, п. п. 1, 4 ст. 451 ГК РФ). Существенность изменения обстоятельств будет определяться судом[113].

В качестве одного из минимально необходимых для закрепления в договоре аутсорсинга условий зарубежными регуляторами называется **установление срока, в течение которого осуществляется расторжение соглашения после принятия решения о раннем расторжении, чтобы обеспечить плавность передачи осуществления услуг**. Согласно ст. 782 ГК РФ, заказчик вправе отказаться от исполнения договора возмездного оказания услуг при условии оплаты исполнителю фактически понесенных им расходов. Исполнитель вправе отказаться от исполнения обязательств по договору возмездного оказания услуг лишь при условии полного возмещения заказчику убытков. Условие договора возмездного оказания услуг, запрещающее односторонний отказ от исполнения такого договора, может признаваться недействительным[114]. При этом **по вопросу о том, вправе ли стороны включить в договор возмездного оказания услуг условия о необходимости предупредить исполнителя об одностороннем отказе от исполнения договора за определенный срок** и (или) об ответственности заказчика за неисполнение данного условия, существует две позиции судов. Одна позиция заключается в том, что отказ заказчика от исполнения договора возможен в любое время: как до начала исполнения услуги, так и в процессе оказания услуги, а значит, поскольку право сторон (как исполнителя, так и заказчика) на односторонний отказ от исполнения договора возмездного оказания услуг императивно установлено ст. 782 ГК РФ, оно не может быть ограничено соглашением сторон[115], в том числе и в отношении срока такого расторжения. Вместе с тем существует и позиция судов о том, что стороны вправе включить в договор возмездного оказания услуг условия о необходимости предупредить

[113] Путеводитель по договорной работе. Возмездное оказание услуг. Рекомендации по заключению договора
[114] Постановление Президиума ВАС РФ от 07.09.2010 N 2715/10 по делу N А64-7196/08-23
[115] Постановление Арбитражного суда Восточно-Сибирского округа от 28.04.2021 N Ф02-1905/2021 по делу N А69-2481/2020: Определение ВАС РФ от 21.05.2013 N ВАС-5767/13 по делу N А40-60948/2012-144-295

исполнителя об одностороннем отказе от исполнения договора за определенный срок и (или) об ответственности заказчика за неисполнение данного условия. Так, суды приходили к выводу, что условие договора о необходимости уведомления другой стороны при досрочном его расторжении в определенный срок не ограничивает право на односторонний отказ от него и являлось волей сторон, не противоречащей действующему законодательству (статьи 421, 422 ГК РФ)[116]. Положения ст. 782 ГК РФ, дающие каждой из сторон договора возмездного оказания услуг право на немотивированный односторонний отказ от исполнения договора, не исключают возможность согласования сторонами договора установления порядка осуществления права на отказ от исполнения договора возмездного оказания услуг, например, предусмотрев специальный порядок уведомления об отказе от договора[117].

В договоре должно быть предусмотрено **обеспечение доступа банка к данным и документам поставщика услуг,** которые его касаются, а также **право на мониторинг и аудит** в отношении деятельности аутсорсера, в том числе **требований к отчетности, включая содержание и частоту отчетности.** Могут быть установлены требования в отношении отчетов, которые позволяют оценить, соблюдаются ли показатели эффективности, а также любую другую информацию, необходимую для мониторинга. Процедуры аудита и мониторинга, управления непрерывностью бизнеса, конфиденциальности и безопасности информации могут быть закреплены как в самом договоре об аутсорсинге (возмездном оказании услуг), так и в самостоятельных соглашениях. Могут быть отдельно приняты стандарты операционной деятельности, внутреннего контроля и управления рисками в отношении IT-аутсорсинга внутри банка или финансовой организации, которые будут рассмотрены далее.

[116] Постановление ФАС Поволжского округа от 12.05.2010 по делу N А57-20634/2009
[117] Постановление Арбитражного суда Московского округа от 09.11.2020 N Ф05-13976/2020 по делу N А40-7026/2020

Например, **предметом соглашений о конфиденциальности** является определение порядка открытия доступа к информации, составляющей коммерческую тайну, условия и цели ее использования, а также ответственность за нарушение данного обязательства[118]. Для обеспечения конфиденциальности информации важно прописать в соглашении, как стороны взаимодействуют при ее передаче и работе с ней, в том числе могут быть предусмотрены **формы, в которых должны храниться данные, положений, определяющих владение и контроль данных**, что значится среди минимальных для закрепления условий договора аутсорсинга в требованиях зарубежных регуляторов. В ряде соглашений о конфиденциальности информация ограниченного доступа определена абстрактно либо в узком смысле слова, перечень лиц, имеющих доступ к такой информации, не закреплен вовсе либо определяется через оценочные понятия[119]. Такого быть не должно. Отметим, что согласно ст. 783.1 ГК РФ, уточнено, что договором, в силу которого исполнитель обязуется совершить действия по предоставлению определенной информации заказчику (договор об оказании услуг по предоставлению информации), может быть предусмотрена обязанность одной из сторон или обеих сторон не совершать в течение определенного периода действий, в результате которых информация может быть раскрыта третьим лицам.

Как отмечается в научной литературе, ключевая проблема ст. 783.1 ГК РФ заключается в рассмотрении исключительно относительных правоотношений, складывающихся между субъектами соответствующего договора, в то время как при рассмотрении информации и массивов данных в качестве объектов гражданского оборота прежде всего необходимо урегулировать положения, касающиеся абсолютных прав, т.е.

---

[118] Бычков А. Режим коммерческой тайны в организации // Юридический справочник руководителя. 2021. N 6. С. 69 - 81.

[119] Подузова Е.Б. Пользовательское соглашение, соглашение о конфиденциальности: особенности содержания в контексте использования технологий искусственного интеллекта // Актуальные проблемы российского права. 2023. N 2. С. 71 - 78.

неприкосновенности прав обладателя информации и запрета несанкционированного доступа к данным неопределенному кругу лиц[120].

Одним из наиболее логичных кандидатов на квалификацию массива данных в качестве объекта гражданских прав выступает такая их разновидность, как охраняемые результаты интеллектуальной деятельности. Как известно, российское законодательство об интеллектуальной собственности исходит из закрытого перечня объектов интеллектуальной собственности, которым предоставляется охрана. Соответствующий перечень содержится в ст. 1225 ГК РФ. Как отмечается, законодатель исключил предоставление такой охраны иным объектам, в этом списке, т.е. в законе не названным[121]. Поэтому при оценке применимости данного варианта квалификации следует исходить из тех видов объектов интеллектуальной собственности, которые поименованы в данной статье. Из всего их многообразия наиболее релевантными по отношению к массиву данных являются такие объекты, как база данных и ноу-хау[122].

Так как поставщик услуг аутсорсинга программного обеспечения занимается созданием/адаптацией/развитием/сопровождением прикладного программного обеспечения автоматизированной банковской системы, в процессе своей деятельности он может создавать результаты интеллектуальной деятельности, в связи с чем необходимо определить, кому будут принадлежать исключительные права на них. В ст. 1295 ГК РФ предусмотрены правила в отношении служебных произведений, но так как создание результатов интеллектуальной деятельности может быть передано на аутсорсинг, нормы о служебном произведении в данном случае применяться не будут. **В договоре аутсорсинга могут быть предусмотрены положения о том, кому будут**

[120] Савельев А.И. Гражданско-правовые аспекты регулирования оборота данных в условиях попыток формирования цифровой экономики // Вестник гражданского права. 2020. N 1. С. 60 - 92.
[121] Маковский А.Л. О кодификации гражданского права (1922 - 2006). М.: Статут, 2010. С. 621.
[122] Савельев А.И. Гражданско-правовые аспекты регулирования оборота данных в условиях попыток формирования цифровой экономики // Вестник гражданского права. 2020. N 1. С. 60 - 92.

принадлежать исключительные права на результаты интеллектуальной деятельности. Если такие права будут принадлежать аутсорсеру, то будет необходимо заключить лицензионный договор на использование таких прав с заключившими ними договор аутсорсинга банком или финансовой организацией.

Согласно требованиям некоторых зарубежных регуляторов, **в договоре аутсорсинга должны быть четко установлены права собственности на все активы (интеллектуальные и физические), которые используются в рамках аутсорсинга, включая активы, созданные или приобретенные в соответствии с договором или по иным соглашениям, например, купли-продажи или аренды оборудования**.

В договоре об аутсорсинге должно быть установлено, **имеет ли поставщик услуг право использовать активы банка или финансовой организации и каким образом** (например, данные, аппаратное и программное обеспечение, системную документацию или интеллектуальную собственность), а также право банка или финансовой организации на доступ к этим активам. **В данном случае могут быть заключены дополнительные соглашения, например, лицензионные. Вопросы поставки оборудования или программного обеспечения могут быть урегулированы в договорах поставки.**

Кроме того, в договоре аутсорсинга должно быть установлено, что **регулятор должен иметь такое же право доступа к информации в отношении аутсорсера**, как и в отношении финансовых организаций, которые привлекают по аутсорсингу сторонних поставщиков услуг. В договоре должно быть закреплено **обязательство поставщиков услуг сообщать о любых существенных неблагоприятных инцидентах** (таких, как утечка данных, недоступность или перебои в предоставлении услуг), которые могут иметь потенциальную возможность существенно повлиять на предоставление услуги банку или финансовой организации. В договоре также должно быть установлено **право банка вмешиваться в деятельность**

компаний, оказывающих услуги по аутсорсингу, и принимать соответствующие меры для обеспечения соблюдения законодательных и нормативных требований. В договоре могут быть указаны случаи и обстоятельства, при которых поставщик услуг обязан сообщить о происшествии регулятору.

В договоре должен быть установлен **механизм разрешения споров. Может быть также предусмотрено положение о непрерывности бизнеса.** Поддержание в актуальном состоянии планов непрерывности бизнеса и управления инцидентами вместе со стратегией непрерывности - достаточно сложный процесс, который называется процессом управления непрерывностью бизнеса. Он включает регулярное тестирование планов, в том числе тестирование взаимодействия с третьими сторонами в случае чрезвычайной ситуации, обучение новых сотрудников, строжайший контроль за изменениями сопутствующей документации, непрерывное улучшение процесса на базе регулярного внутреннего аудита, вовлечение высшего руководства и т.д. Стандарт подробно описывает, что должна иметь компания, чтобы незамедлительно привести планы в исполнение в случае реализации угрозы[123]. Комплексность подхода к обеспечению непрерывности бизнеса заключается в разработке максимально полного перечня видов и характера возможных рисков и угроз непрерывности деятельности, определении вероятности их наступления, значимости последствий, установлении взаимосвязей внутренних и внешних факторов, а также выявлении наиболее критичных бизнес-операций и их зависимости от ресурсов (сторонних организаций, персонала, информационных систем, офисных ресурсов и т.п.), требуемых для восстановления в случае прерывания деятельности[124].

В договоре должно быть установлено, возможно ли в принципе и каким образом осуществляется **привлечение субисполнителей** по договору

[123] Авакян А. Система управления непрерывностью бизнеса // Финансовая газета. 2009. N 31.
[124] Козлов Д.Н. Обеспечение непрерывности деятельности кредитной организации - контроль исполнения // Внутренний контроль в кредитной организации. 2014. N 2. С. 58 - 70.

возмездного оказания услуг, **так как регулятор должен осуществлять контрольно-надзорные функции в отношении всех лиц, которые задействованы в IT-аутсорсинге в банковской сфере.**

Согласно ч. 2 ст. 779 ГК РФ, если иное не предусмотрено договором возмездного оказания услуг, исполнитель обязан оказать услуги лично. **Некоторые регуляторы специально устанавливают правила для субконтрактов в рамках аутсорсинга**. Так, в Заявлении надзорного органа Великобритании[125] указывается важность того, чтобы поставщики услуг оценили соответствующие риски субаутсорсинга, прежде чем заключать договор. Важно при этом, чтобы поставщики услуг осознавали всю цепочку взаимодействия между субъектами в данном вопросе. Поставщики услуг должны также оценить, соответствует ли субаутсорсинг критериям существенности видов деятельности. Договор можно заключить, только если субаутсорсинг не приведет к возникновению неоправданного операционного риска для первоначального поставщика услуг, субаутсорсинговые поставщики услуг обязуются соблюдать все применимые законы, нормативные требования и договорные обязательства и предоставить первоначальному поставщику услуг, банку и регулятору договорные права доступа, аудита и информации, эквивалентные тем, которые предоставлены первоначальному поставщику услуг. В Руководящих принципах OSFI Канады[126] закреплено, что в соглашении об аутсорсинге должны быть установлены любые правила или ограничения на субподряд со стороны поставщика услуг. В частности, стандарты безопасности и конфиденциальности должны применяться к соглашениям о субподряде или аутсорсинге со стороны основного поставщика услуг также, как и к первоначальному поставщику услуг. В соответствии с принципами данного Руководства права регулятора на проведение аудита и

[125] Supervisory Statement | SS2/21 Outsourcing and third party risk management March 2021 https://www.bankofengland.co.uk/-/media/boe/files/prudential-regulation/supervisory-statement/2021/ss221-march-21.pdf

[126] Outsourcing of Business Activities, Functions and Processes https://www.osfi-bsif.gc.ca/Eng/fi-if/rg-ro/gdn-ort/gl-ld/Pages/b10.aspx

инспекций будут распространятся на все значимые субподрядные соглашения. В Руководящих принципах регулятора Сингапура[127] установлено, что поставщик услуг должен сохранять возможность отслеживать и контролировать деятельность, которая передана на аутсорсинг, если он нанимает субподрядчика. Для субподрядчика соблюдение положений договора с поставщиком услуг, а также Руководящих принципов является обязательным, когда речь идет о существенных видах деятельности. Кроме того, привлечение поставщиком услуг субподрядчика должно быть предварительно одобрено банком или финансовой организацией.

Исполнитель считается надлежаще исполнившим свои обязательства после того, как совершит действия (осуществит деятельность), указанные в договоре возмездного оказания услуг[128]. В российском праве рассматривается **вопрос об ответственности исполнителя за ненадлежащее оказание услуг**. Согласно п. 1 ст. 15 ГК РФ лицо, право которого нарушено, может требовать полного возмещения причиненных ему убытков, если законом или договором не предусмотрено возмещение убытков в меньшем размере. На практике возникают споры об основаниях для освобождения исполнителя от ответственности и о действительности условия договора возмездного оказания услуг об установлении ограниченной ответственности исполнителя за ненадлежащее оказание услуг. Если исполнитель не оказал услугу, заказчик вправе взыскать с него убытки в размере разницы между суммой, уплаченной третьему лицу за аналогичные услуги, и стоимостью услуг исполнителя. В соответствии с п. 1 ст. 393.1 ГК РФ, если неисполнение или ненадлежащее исполнение должником договора повлекло его досрочное прекращение и кредитор заключил взамен него аналогичный договор, кредитор вправе потребовать от должника возмещения убытков в виде разницы между ценой,

---

[127] Guidelines on Outsourcing. Monetary Authority of Singapore. 27 July 2016. https://www.mas.gov.sg/-/media/mas/regulations-and-financial-stability/regulatory-and-supervisory-framework/risk-management/outsourcing-guidelines_jul-2016-revised-on-5-oct-2018.pdf

[128] Информационное письмо Президиума ВАС РФ от 29.09.1999 N 48 "О некоторых вопросах судебной практики, возникающих при рассмотрении споров, связанных с договорами на оказание правовых услуг"

установленной в прекращенном договоре, и ценой на сопоставимые товары, работы или услуги, которая предусмотрена в договоре, заключенном взамен прекращенного. Условие договора об освобождении исполнителя от ответственности за ненадлежащее оказание охранных услуг в случае, если заказчик не исполняет обязанность по их своевременной оплате, является ничтожным[129].

В зарубежных правопорядках в качестве обязательных минимальных требований может быть указано на определение ответственности и возмещения в случае невыполнения, задержки или ошибочных транзакций, обработанных поставщиком аутсорсинговых услуг. Некоторые регуляторы требуют, чтобы было установлено право требовать, чтобы поставщик услуг нес договорную ответственность за производительность и риски своего субподрядчика.

Таким образом, **предлагается, избрав для отношений аутсорсинга письменную форму договора возмездного оказания услуг, предусмотреть требования регулятора Банка России в отношении того, что должно быть закреплено в качестве условий такого договора (данные условия не будут считаться существенными с точки зрения гражданского законодательства, но будут отвечать требованиям, установленным регулятором). Договор может считаться дополнительным инструментом распределения ответственности во взаимоотношениях по IT-аутсорсингу в банковской сфере.**

В архитектуре правоотношений между основными субъектами рынка IT-аутсорсинга необходимо обратить внимание на **особенности в отношении поставщиков услуг, которые аффилированы с банком или финансовой организацией и привлекаются ими для IT-аутсорсинга**. В Заявлении надзорного органа Великобритании[130] (п. 3.3, 3.4) установлено, что

[129] Постановление ФАС Волго-Вятского округа от 24.03.2014 по делу N А79-12984/2012

[130] Supervisory Statement | SS2/21 Outsourcing and third party risk management March 2021 https://www.bankofengland.co.uk/-/media/boe/files/prudential-regulation/supervisory-statement/2021/ss221-march-21.pdf

внутригрупповой аутсорсинг подчиняется **тем же требованиям и ожиданиям, что и аутсорсинг поставщиков услуг, не входящих в группу**, и их не следует рассматривать как менее рискованные по своей сути. В зависимости от уровня контроля и влияния в отношении внутригруппового аутсорсинга компания может, например, использовать общие политики или проводить не такую детальную комплексную проверку при принятии решения об аутсорсинге, если информация о деятельности компании у нее имеется. Специальные требования для внутригруппового аутсорсинга установлены, например, в Циркуляре Государственного банка Пакистана[131]. Данный вопрос рассматривается также в Пруденциальном стандарте Австралии[132].

Таким образом, для правового оформления отношений IT-аутсорсинга принципиальное значение имеет не столько вид договора, который закрепляет такие отношения, сколько его форма. Договор должен быть заключен в письменной форме, кроме того, представляется необходимым уведомлять Банк России о заключении такого договора и направлять ему его копию.

В Российской Федерации наиболее подходящей правовой формой для отношений IT-аутсорсинга является договор возмездного оказания услуг, однако наряду с ним могут быть использованы договоры поставки, аренды, передачи исключительных прав на результаты интеллектуальной деятельности, лицензионный договор и договорная конструкция абонентского обслуживания, договор о защите конфиденциальной информации. Представляется, что Банком России должны быть предусмотрены требования по отношению к минимальному набору необходимых условий договора, оформляющего отношения IT-аутсорсинга. Среди таких условий должны быть предмет, срок, стоимость услуг и порядок их оплаты, условие о порядке пересмотра договора, срок,

[131] Framework for Risk Management in Outsourcing Arrangements by Financial Institutions BPRD Circular No. 06 of 2019 https://www.sbp.org.pk/bprd/2019/C6-Annex-II.pdf

[132] Prudential Standard CPS 231 Outsourcing July 2017 https://www.apra.gov.au/sites/default/files/Prudential-Standard-CPS-231-Outsourcing-%28July-2017%29.pdf

в течение которого осуществляется расторжение соглашения после принятия решения о раннем расторжении, условие о праве доступа банка или финансовой организации к данным и документам поставщика IT-услуг, которые его касаются, праве на мониторинг и аудит в отношении деятельности IT-аутсорсера в том числе, требований к отчетности, включая содержание и частоту отчетности, условие о работе с конфиденциальной информацией, условие о распределении прав на результаты интеллектуальной деятельности.

Кроме того, Банком России должны быть закреплены требования проводить предварительную комплексную проверку, а также мониторинг и контроль, которые необходимы при передаче услуг на аутсорсинг в банковской сфере.

Банку России рекомендуется в своем акте установить, что кредитные организации должны гарантировать, что заключение и исполнение договора IT-аутсорсинга не влияет на их способность выполнять свои обязательства перед клиентами и требования регулятора, а также принять меры для обеспечения того, чтобы поставщик услуг IT-аутсорсинга исходил из тех же стандартов при оказании услуг, из которых исходит сам банк. Ответственность за соблюдения требований законодательства и регулятора в рамках IT-аутсорсинга предлагается в акте Банка России возложить на кредитные организации в том числе и в случае, когда они передали свои функции или отдельные виды деятельности сторонним поставщикам услуг по соглашению IT-аутсорсинга.

Кроме того, регулятору необходимо установить, какие услуги не могут передаваться на аутсорсинг кредитными организациями, и для каких услуг передача требует соблюдения дополнительных требований. Предлагаем в качестве таких требований установить требования к минимальному набору условий, который должны быть отражены в договоре, оформляющем отношения IT-аутсорсинга. Услугами, передача

которых требует соблюдения дополнительных требований, предлагаем считать существенные услуги, к которым предлагаем отнести деятельность, нарушение которой потенциально может оказать существенное влияние на деловую активность кредитной организации и/или ее способность эффективно управлять рисками, принимая во внимание такие факторы, как финансовые и операционные последствия, влияние на репутацию кредитной организации, стоимость соглашения об аутсорсинге в объеме общих затрат кредитной организации, время, необходимое для поиска альтернативного поставщика услуг или организации деятельности собственными силами, способность кредитной организации соблюдать нормативные требования в случае возникновения проблем с поставщиком услуг, потенциальные убытки для клиентов в случае сбоя работы поставщика услуг.

Банку России рекомендуется в своем акте установить, что кредитные организации, которые передают IT-деятельность на аутсорсинг, должны иметь комплексную внутреннюю политику, позволяющую оценить, может ли такая деятельность быть передана на аутсорсинг и если да, то каким образом.

1.3. При построении модели необходимо учитывать (и отразить в конструируемой модели):

1) возможную роль страховых компаний в общей архитектуре правоотношений между основными субъектами рынка IT-аутсорсинга.

Очевидно, что часть рисков, возникающих в рамках договорных отношений между кредитными организациями и IT-компаниями по поводу указания аутсорсинговых услуг в сфере IT, может быть помимо традиционных видов страхования также минимизирована при помощи страхования киберрисков.

В федеральном законодательстве отсутствует понятие киберриска. Однако в нормативных актах и иных документах Банка России понятие киберриска раскрывается. Согласно п. 7.2 Положения Банка России от

08.04.2020 № 716-П «О требованиях к системе управления операционным риском в кредитной организации и банковской группе»[133] **киберриск** относится к риску информационной безопасности и **представляет собой риск преднамеренных действий со стороны работников кредитной организации и (или) третьих лиц с использованием программных и (или) программно-аппаратных средств, направленных на объекты информационной инфраструктуры кредитной организации (головной кредитной организации банковской группы) в целях нарушения и (или) прекращения их функционирования и (или) создания угрозы безопасности информации, подготавливаемой, обрабатываемой и хранимой такими объектами, а также в целях несанкционированного присвоения, хищения, изменения, удаления данных и иной информации (структуры данных, параметров и характеристик систем, программного кода) и нарушения режима доступа.**

Очевидно, что с точки зрения выделяемых Банком России рисков информационной безопасности **в целях настоящего исследования необходим анализ страхования именно киберрисков, поскольку другие виды риска информационной безопасности связаны с обработкой (хранением, уничтожением) информации без использования объектов информационной инфраструктуры и с небольшой долей вероятности могут возникнуть при взаимодействии кредитной организации и IT-аутсорсера** (например, социальная инженерия, фишинг, хищения, связанные с заменой SIM-карт, хищения в случае несанкционированного физического доступа третьих лиц к банковской карте или мобильному устройству клиента)[134].

В экспертной литературе выделяются различные киберриски: риск утечки конфиденциальной информации; риск потери или недоступности

[133] Вестник Банка России. 2020. № 51.

[134] См., например: Письмо Банка России от 11.11.2020 N 716-Р-2020/11 // https://cbr.ru/faq_ufr/dbrnfaq/doc/?UniDbQuery.Posted=True&UniDbQuery.SHrase=716-P-2020%2F11&UniDbQuery.number=716-П

важных данных; риск использования неполной или искаженной информации; риск неправомочной скрытой эксплуатации информационно-вычислительных ресурсов (например, при создании бот-сети); риск распространения во внешней среде информации, угрожающей репутации организации.

В общем понимании страхового риска именно страх перед **риском как вероятностью наступления неблагоприятных для лица событий** побуждает лицо обеспечить защиту своих имущественных интересов. При этом страховой случай представляет собой воплощенный в реальность страховой риск, т.е. предполагаемое нежелательное для лица событие, обладающее признаками вероятности и одновременно случайности его наступления.

Как известно, в имущественном страховании выделяются три крупные подотрасли: страхование имущества, страхование предпринимательских рисков и страхование ответственности.

Для страхования киберрисков очевидно в большей степени подходят страхование предпринимательских рисков и страхование ответственности.

Страхование предпринимательского риска предполагает страхование предпринимателем риска убытков от осуществляемой им деятельности из-за нарушения своих обязательств контрагентами предпринимателя или изменения условий этой деятельности по независящим от предпринимателя обстоятельствам, в том числе риска неполучения ожидаемых доходов. Особенностью данного вида имущественного страхования является также то, что согласно требованиям ГК РФ предприниматель может застраховать только свой предпринимательский риск и только в свою пользу, ведь зачастую степень риска может во многом зависеть от самого предпринимателя (в то время как по данному виду страхования покрываются не только реальный ущерб предпринимателя, но и упущенная выгода). Соответственно, **такой вид страхования не является распространенным вследствие сложности доказывания. Тем более, вряд ли можно говорить о распространении данного вида страхования в сфере минимизации киберрисков ввиду**

сложности объективной оценки убытков банка, в том числе неполучения ожидаемых доходов из-за нарушения договорных условий со стороны IT-аутсорсера.

На страховом рынке в рассматриваемой сфере более распространенным видом страхования является такая разновидность страхования гражданской ответственности как страхование ответственности за причинение вреда (ст. 931 ГК РФ), поскольку страхование ответственности по договору (ст. 932 ГК РФ) возможно только в случаях, предусмотренных законом.

По договору страхования риска ответственности по обязательствам, возникающим вследствие причинения вреда жизни, здоровью или имуществу других лиц, может быть застрахован риск ответственности самого страхователя. Может быть застрахована ответственность и иного лица, но только того, на которое такая ответственность может быть возложена. Договор страхования риска ответственности за причинение вреда считается в любых случаях заключенным в пользу лиц, которым может быть причинен вред (выгодоприобретателей). При этом выгодоприобретатель по договору обязательного страхования риска ответственности за причинение вреда вправе обратиться непосредственно к страховщику с требованием о выплате страхового возмещения в целях покрытия причиненного ему вреда в пределах страховой суммы. Указанный вид страхования достаточно распространен в предпринимательской деятельности, ведь он позволяет предпринимателю заранее обезопасить себя от необходимости за счет собственных средств в полном объеме возмещать вред, причиненный третьим лицам.

Специалисты страховой отрасли считают, что часть киберрисков можно застраховать, например, таргетированные компьютерные атаки, внедрение вредоносных компьютерных программ, технические сбои, а также непреднамеренные ошибки персонала[135].

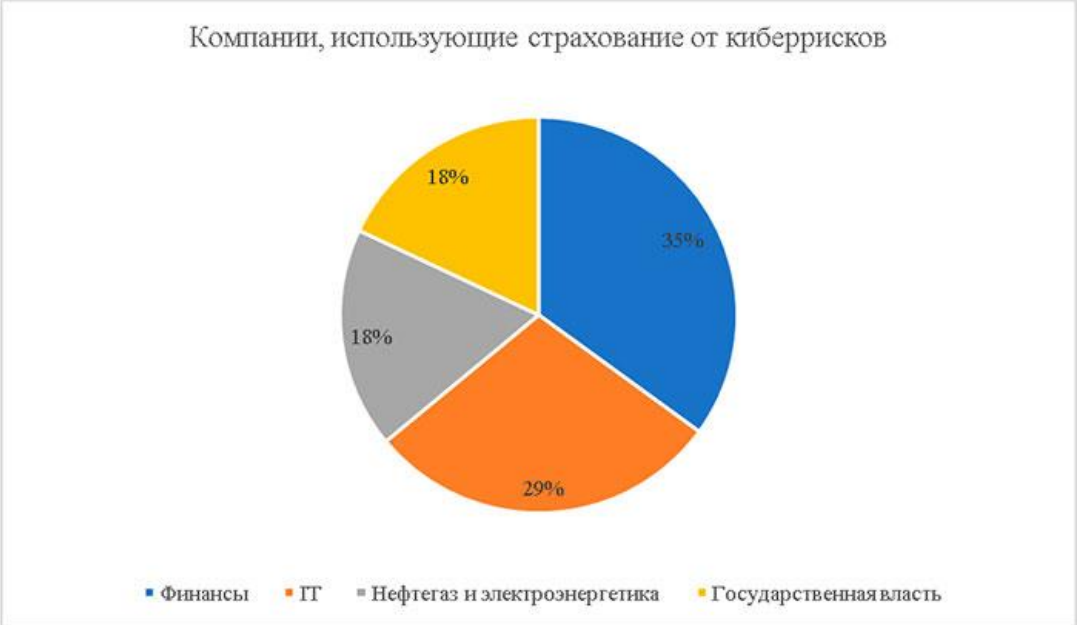
Однако на практике страхования киберрисков сводится в основном к

[135] HTTPS://BOSFERA.RU/BO/KIBERSTRAHOVANIE-NE-DLYA-BANKA-DLYA-KLIENTA

страхованию ответственности кредитных организаций в части публичных санкций (штрафов) вследствие нарушения законодательства, вызванного несоблюдением требований к обеспечению защиты конфиденциальной информации. Как отмечается экспертами, «в рамках киберстрахования сейчас представлен достаточно узкий спектр услуг, связанных в основном с тем, чтобы компенсировать штрафы, которые накладывают регуляторы в случаях утечки персональных данных»[136]. Вопрос о расширении данного вида страхования на компенсацию ущерба, причиненного вследствие реализации киберриска клиентам банка, является важным и одновременно сложным, так как требует большей информированности страховых организаций и определения единых методик оценки.

Исходя из статистических данных, наибольшая доля компаний, которые в настоящее время страхуют кибберриски, являются финансовыми организациями, что подтверждает необходимость создания благоприятных, в том числе с правовой точки зрения условий для развития данного сегмента рынка, особенно в связи с перспективой урегулирования рынка финансового IT-аутсорсинга со всеми многочисленными рисками, возникающими при взаимодействии его участников.

[136] Интервью с А. Шейкиным «Киберриски страхуют единицы» // https://bosfera.ru/bo/kiberriski-strahuyut-edinicy?ysclid=lmdf0mmxvx633075761



[137]

Следует отметить, что с точки зрения развития рынка страхования на уровне Стратегии Правительства РФ предполагается, что в ближайшие годы отдельное внимание будет уделено созданию условий для развития новых для российского рынка страховых продуктов, учитывая все более широкую цифровизацию экономических и общественных отношений, в том числе применение искусственного интеллекта, а также повышение значимости киберрисков[138].

Однако для повышения доли страхования киберрисков на страховом рынке, что, как было отмечено, для рынка финансового IT-аутсорсинга является крайне важным, необходимо обозначить ряд проблем и предложить пути их решения в правовом поле.

1. В экспертной литературе отмечается проблема, связанная со сложностью актуарных расчетов в сфере киберстрахования, в том числе вследствие практически полного отсутствия статистических данных по страховым случаям[139].

[137] Источник: «Ростелеком Солар», опрос 400 компаний в 2022 году.
[138] Распоряжение Правительства РФ от 29.12.2022 N 4355-р «Об утверждении Стратегии развития финансового рынка РФ до 2030 года» // СЗ РФ. 2023, N 1 (часть III), ст. 476.
[139] HTTPS://BOSFERA.RU/BO/KIBERSTRAHOVANIE-NE-DLYA-BANKA-DLYA-KLIENTA

В настоящее время одним из ключевых источников получения статистических данных о случаях реализации киберрисков является аналитические данные ФинЦЕРТ (Центр взаимодействия и реагирования Департамента информационной безопасности, специальное структурное подразделение Банка России). На базе ФинЦЕРТ создана система информационного обмена между участниками финансового рынка, правоохранительными органами, провайдерами и операторами связи, системными интеграторами, разработчиками антивирусного программного обеспечения и другими компаниями, работающими в сфере информационной безопасности, всего более 1000 участниками[140].

ФинЦЕРТ собирает с финансовых организаций информацию о кибератаках, осуществляет их анализ и на его основе информирует их об актуальных угрозах кибербезопасности, разрабатывает рекомендации по отражению хакерских атак, взаимодействует с правоохранительными органами и оперативными службами ФСБ. Оперативный обмен информацией о компьютерных атаках с финансовыми организациями ведется, в том числе с помощью автоматизированной системы обработки инцидентов (АСОИ).

Хотя ФинЦЕРТ достаточно регулярно публикует различные аналитические документы о различных киберугрозах на финансовом рынке[141], тем не менее, для развития киберстрахования аналитическая работа о киберинцидентах должна быть поставлена на регулярную основу. Кроме того, возможно закрепить в нормативных актах Банка России право страховых организаций на получение обезличенных данных о кибератаках.

2. Также эксперты страхового рынка отмечают проблему отсутствия для страховщиков стандартов по формированию такого страхового продукта, как страхование киберрисков[142].

---

[140] https://cbr.ru/information_security/fincert/#highlight=финцерт

[141] См., например: «Основные типы компьютерных атак в кредитно-финансовой сфере в 2019-2020 годах» // https://cbr.ru/Collection/Collection/File/32122/Attack_2019-2020.pdf;

[142] HTTPS://BOSFERA.RU/BO/KIBERSTRAHOVANIE-NE-DLYA-BANKA-DLYA-KLIENTA

Для страховых компаний использование единых методик анализа текущих угроз информационной безопасности и операционной надежности кредитной организации и IT-аутсорсера является крайне актуальным и важным фактором для развития киберстрахования. Поэтому, как будет проанализировано далее в связи с рассмотрением вопросов взаимодействия IT-аутсорсера с регулятором, полагаем целесообразным распространить на соответствующие компании IT-аутсорсинга действие стандартов Банка России, связанные с обеспечением информационной безопасности и управлением инцидентами, связанными с реализацией информационных угроз, и инцидентами операционной надежности, а также определить рекомендации для страховых организаций использования таких единых методик оценки рисков.

3. Наконец, участники страхового рынка отмечают сложности при оценке киберрисков. В особенности, как было отмечено, данная проблема возникает при страховании не столько публичной ответственности банка-клиента IT-аутсорсера, сколько ущерба, нанесенного клиенту банка как 3-му лицу при реализации страхового случая. Как отмечают эксперты, «помимо сложного андеррайтинга для защиты от киберрисков страховым компаниям требуется определенная инфраструктура: она нужна для расследования инцидента и минимизации его последствий»[143]. Полагаем, что данная проблема во многом лежит вне правового поля, тем не менее, может быть отчасти решена после устранения рассмотренных выше первого (статистические данные) и второго (единые стандарты и методология) препятствий.

Одним из факторов для развития киберстрахования может стать принятие закона об оборотном штрафе для компаний за утечку персональных данных, поскольку, с одной стороны, будет способствовать большей заинтересованности участников финансового рынка в страховании

[143] HTTPS://BOSFERA.RU/BO/KIBERSTRAHOVANIE-NE-DLYA-BANKA-DLYA-KLIENTA

ответственности за причинение вреда вследствие реализации киберриска, а с другой стороны, позволит упросить оценку такого ущерба. В рамках готовящегося законопроекта предполагается реализовать механизм путем внесения изменений в КоАП[144]. Рассматривается также возможность создания специального фонда по аналогии с Агентством по страхованию вкладов, в который будут перечислять собранные штрафы и из которого станут выплачивать компенсации гражданам, пострадавшим от утечек[145].

Полагаем, что использование правового механизма страхования киберрисков может способствовать в рамках договорных отношений между кредитной организацией и IT-аусорсером снижению большинства ключевых рисков, рассматриваемых в настоящем исследовании: риска потери финансовой устойчивости (риск утраты контроля за функцией, системный риск), операционного риска (риск ошибки персонала, риск сбоя информационных систем, риск информационной безопасности), правового риска (комплаенс-риск, риск раскрытия конфиденциальной информации, риск нарушения договора с IT-аутсорсером, риск прекращения договора с IT-аутсорсером), репутационного риска (риск недобросовестных действий IT-аутсорсера). Однако очевидно, что минимизировать указанные риски киберстрахование сможет только при расширении страховых продуктов, предлагаемых страховыми организациями, что возможно в результате решения проанализированных правовых проблем: появления регулярной аналитики о киберинцидентах, закрепления в нормативных актах Банка России права страховых организаций на получение обезличенных данных о кибератаках, а также установления единых методик анализа

[144] Вероятность принятия данного законопроекта велика, так как Президент РФ еще в январе 2023 поручил Правительству РФ рассмотреть вопросы об установлении оборотных штрафов в отношении компаний, допускающих утечку персональных данных, усилении ответственности за их незаконный оборот и иные нарушения законодательства в области персональных данных и представить предложения по внесению соответствующих изменений в законодательство Российской Федерации // Перечень поручений по итогам заседания Совета по развитию гражданского общества и правам человека (утв. Президентом РФ 12.01.2023 N Пр-19). http://kremlin.ru

[145] Подробнее см: https://www.rbc.ru/technology_and_media/27/07/2023/64c15e069a79474102dac8b0

текущих угроз информационной безопасности и операционной надежности кредитной организации и IT-аутсорсера.

2) возможное возникновение необходимости осуществления взаимодействия IT-аутсорсера с регулирующими органами вследствие передачи ему от банка соответствующей информации.

Вопрос о взаимодействии IT-аутсорсера с регулирующими органами в связи с передачей ему банком-клиентом информации, в том числе конфиденциальной, с учетом понимания самого IT-аутсорсинга, является по существу системообразующим для построения всей правовой модели соответствующего рынка.

Очевидно, что необходимость осуществления взаимодействия IT-аутсорсера с регулирующими органами возникает в основном вследствие передачи ему от банка соответствующей, в том числе конфиденциальной информации. **Ключевыми рисками в данной сфере являются операционный и правовой, так как в рамках различных нарушений при осуществлении ключевых функций IT-аутсорсера (оказание услуг аутсорсинга ПО, инфраструктурных услуг, а также услуг в области безопасности) через реализацию рисков ошибок персонала, рисков сбоя информационных систем, рисков информационной безопасности может реализоваться риск раскрытия конфиденциальной информации**.

Банк России ориентирует кредитные организации на то, что в ряде случаев ущерб от реализации рисков нарушения информационной безопасности не может быть компенсирован поставщиком услуг в рамках договорных отношений. В связи с этим кредитные организации при привлечении для аутсорсинга поставщиков услуг должны обеспечить реализацию механизмов управления и контроля риска нарушения информационной безопасности, создающую основу для обеспечения соответствия уровня риска нарушения информационной безопасности при передаче бизнес-функций на аутсорсинг уровню риска, принятому

самостоятельно кредитной организацией[146]. **Таким образом, помимо установления требований к IT-аутсорсеру по работе с конфиденциальной информацией на уровне, не ниже, чем предъявляется к кредитным организациям или некредитным финансовым организациям, а также лицам, оказывающим профессиональные услуги на финансовом рынке, сами банки также будут оставаться ответственными за реализацию указанных выше рисков.** Также возможно предъявление самостоятельных требований к соответствующим системам, используемым IT-аутсорсерами. Так, Законопроектом об IT-аутсорсинге предлагается внести в Федеральный закон от 10.07.2002 № 86-ФЗ «О Центральном банке Российской Федерации (Банке России)»[147] (далее – Закон о Банке России) ст. 57.5-2, согласно которой Банк России будет устанавливать обязательные для кредитных организаций требования к порядку взаимодействия с поставщиками услуг аутсорсинга информационных технологий и облачных услуг, а также требования к предоставляемым или информационным системам, в том числе в целях обеспечения защиты информации и операционной надежности банковских услуг.

Банковская тайна

Предоставление IT-аутсорсеру сведений, составляющих банковскую тайну, возможно только в случае прямого разрешения такой передачи в банковском законодательстве.

Согласно статье 857 ГК РФ банк гарантирует тайну банковского счета и банковского вклада, операций по счету и сведений о клиенте. В соответствии со статьей 26 Федерального закона от 02.12.1990 № 395-1 «О банках и банковской деятельности» (далее – Закон о банках) кредитная организация гарантирует тайну об операциях, о счетах и вкладах своих клиентов и

[146] Стандарт Банка России "Обеспечение информационной безопасности организаций банковской системы Российской Федерации. Управление риском нарушения информационной безопасности при аутсорсинге" СТО БР ИББС-1.4-2018 (принят и введен в действие Приказом Банка России от 06.03.2018 N ОД-568) // Вестник Банка России. 2018. № 27.

[147] Собрание законодательства РФ. 15.07.2002, N 28, ст. 2790.

корреспондентов. Сведения, составляющие банковскую тайну, могут быть предоставлены только самим клиентам или их представителям, а также представлены в бюро кредитных историй на основаниях и в порядке, которые предусмотрены законом. Государственным органам и их должностным лицам, а также иным лицам такие сведения могут быть предоставлены исключительно в случаях и порядке, которые предусмотрены законом[148]. Порядок предоставления сведений, составляющих банковскую тайну, иным лицам определен в статье 26 Закона о банках. Таким образом, для того, чтобы IT-аутсорсер мог получать и обрабатывать информацию, составляющую банковскую тайну, должны быть внесены изменения непосредственно в ст. 26 Закона о банках.

Согласно Законопроекту об IT-аутсорсинге Закон о банках предлагается дополнить ст. 25.3 «Взаимодействие между кредитной организацией и поставщиком услуг аутсорсинга информационных технологий и облачных услуг», согласно которой кредитная организация сможет поручить поставщикам услуг аутсорсинга информационных технологий и облачных услуг (далее также – IT-аутсорсер) осуществление размещения, хранения и иной обработки сведений, устанавливаемых и собираемых в рамках своей деятельности кредитной организацией, за исключением сведений, отнесенных к государственной тайне, без получения согласия лиц, к которым относятся указанные сведения, с использованием принадлежащих IT-аутсорсерам, в частности облачных и файловых хранилищ, серверов, иных устройств и систем сбора, хранения и обработки информации, на основании заключенных с IT-аутсорсерами договоров. IT-аутсорсеры и их должностные лица будут не вправе разглашать полученные от кредитной организации сведения под

[148] В частности, Федеральная антимонопольная служба не признается органом, имеющим право на получение сведений, составляющих банковскую тайну, поскольку статья 26 Закона о банках не перечисляет ФАС в перечне органов и лиц, имеющих право на ее получение. Статья 25 Закона о защите конкуренции во взаимосвязи с положениями части 6 статьи 44 данного Закона и статьи 26 Закона о банках не содержит положений, обязывающих банк представлять в антимонопольный орган по его мотивированному требованию документы и сведения, составляющие банковскую тайну. См., например, Постановление Арбитражного суда Северо-Западного округа от 12.03.2020 № Ф07-1619/2020 по делу № А56-74329/2019 и Определение Судебной коллегии по экономическим спорам Верховного Суда РФ от 01.02.2019 № 305-АД18-18535 по делу № А40-199212/2017. Документы опубликованы не были. СПС «КонсультантПлюс».

угрозой ответственности за такое разглашение в соответствии с законодательством и договором. На IT-аутсорсеров и их должностных лиц предлагается также возложить обязанность соблюдать установленные законодательством режимы защиты, режимы обработки информации, которую они получают и в отношении которой установлено требование об обеспечении ее конфиденциальности, и порядок ее использования также с возложением на них ответственности за нарушения.

Законопроектом об IT-аутсорсинге также предлагается дополнить ст. 26 Закона о банках правом кредитных организаций осуществлять размещение, хранение и иную обработку сведений, составляющих банковскую тайну, с использованием принадлежащих IT-аутсорсерам информационных систем и их компонентов, в частности облачных и файловых хранилищ, серверов, иных устройств и систем сбора, хранения и обработки информации на основании договоров. Специально устанавливается обязанность IT-аутсорсеров и их должностных лиц хранить тайну об операциях, о счетах и вкладах клиентов и корреспондентов кредитных организаций, за разглашение которой предусматривается ответственность, включая возмещение понесенного ущерба в порядке, предусмотренном законодательством и договором. Взаимодействие с регулирующими и судебными органами в рамках норм о защите банковской тайны возможно на этапе привлечения IT-аутсорсера к гражданско-правовой, его должностных лиц к административной и иной публичной ответственности. Данный вопрос с учетом необходимости распределения бремени данной ответственности между IT-аутсорсером и кредитными организациями будет рассмотрен далее в самостоятельном разделе.

Персональные данные

При работе IT-аутсорсера с персональными данными необходимо выполнение ряда требований в данной сфере, которые зависят от вида персональных данных, с которыми работает IT-аутсорсер, а также от уровня угрозы им.

Согласно п. 5 ст. 19 Федерального закона от 27.07.2006 № 152-ФЗ «О персональных данных»[149] федеральные органы исполнительной власти, осуществляющие функции по выработке государственной политики и нормативно-правовому регулированию в установленной сфере деятельности, органы государственной власти субъектов Российской Федерации, Банк России, органы государственных внебюджетных фондов, иные государственные органы в пределах своих полномочий принимают нормативные правовые акты, в которых определяют угрозы безопасности персональных данных, актуальные при обработке персональных данных в информационных системах персональных данных, эксплуатируемых при осуществлении соответствующих видов деятельности, с учетом содержания персональных данных, характера и способов их обработки[150].

Следует отметить, что кредитные организации должны выполнять требования к уровню защищенности информации, в том числе при работе с персональными данными. Согласно ст. 57.4. Закона о Банке России, ЦБ РФ по согласованию с федеральным органом исполнительной власти, уполномоченным в области обеспечения безопасности, и федеральным органом исполнительной власти, уполномоченным в области противодействия техническим разведкам и технической защиты информации, устанавливает обязательные для кредитных организаций требования к обеспечению защиты информации при осуществлении банковской деятельности в целях противодействия осуществлению переводов денежных средств без согласия клиента, за исключением требований к обеспечению защиты информации, установленных федеральными законами и принятыми в соответствии с ними нормативными правовыми актами.

---

[149] СЗ РФ. 2006, N 31 (1 ч.), ст. 3451.

[150] См.: Постановление Правительства РФ от 01.11.2012 N 1119 «Об утверждении требований к защите персональных данных при их обработке в информационных системах персональных данных» // СЗ РФ. 2012, N 45, ст. 6257; Приказ ФСБ России от 10.07.2014 N 378 «Об утверждении Состава и содержания организационных и технических мер по обеспечению безопасности персональных данных при их обработке в информационных системах персональных данных с использованием средств криптографической защиты информации, необходимых для выполнения установленных Правительством Российской Федерации требований к защите персональных данных для каждого из уровней защищенности» // "Российская газета", N 211, 17.09.2014 и др.

В настоящее время оценка выполнения требований к обеспечению защиты информации проводится кредитными организациями в соответствии со следующими требованиями нормативных актов Банка России:

- пункт 9 Положения Банка России от 17.04.2019 № 683-П «Об установлении обязательных для кредитных организаций требований к обеспечению защиты информации при осуществлении банковской деятельности в целях противодействия осуществлению переводов денежных средств без согласия клиента»[151] (далее – Положение Банка России № 683-П);
- пункт 1.1 Положения Банка России от 04.06.2020 № 719-П «О требованиях к обеспечению защиты информации при осуществлении переводов денежных средств и о порядке осуществления Банком России контроля за соблюдением требований к обеспечению защиты информации при осуществлении переводов денежных средств»[152] (далее - Положение Банка России № 719-П);
- пункт 20 Положения Банка России от 25.07.2022 № 802-П «О требованиях к защите информации в платежной системе Банка России» [153] (далее - Положение Банка России № 802-П).

Сведения о результатах проведения оценки выполнения требований к обеспечению защиты информации представляются в Банк России кредитными организациями в рамках отчетности по форме 0409071 «Сведения об оценке выполнения кредитными организациями требований к обеспечению защиты информации» (далее - отчетность по форме 0409071).

Информация, представляемая согласно разделам 1, 2 отчетности по форме 0409071, отражает степень выполнения установленных указанными

[151] Вестник Банка России. 2019. № 33.
[152] Вестник Банка России. 2020. № 83
[153] Вестник Банка России. 2022. № 60.

нормативными актами Банка России требований к обеспечению защиты информации, применяемых с использованием технологических мер защиты информации, и требований, применяемых в отношении прикладного программного обеспечения автоматизированных систем и приложений (далее - оценка выполнения требований).

При проведении оценки выполнения требований Банком России банки руководствуются Методическими рекомендациями Банка России по расчету значений показателей оценки выполнения требований к технологическим мерам защиты информации и прикладному программному обеспечению автоматизированных систем и приложений в целях составления отчетности об оценке выполнения требований к обеспечению защиты информации от 02.11.2022 № 12-МР.

Оценка выполнения требований может осуществляться кредитной организацией самостоятельно. Информация, представляемая согласно разделам 3, 4 отчетности по форме 0409071, отражает информацию об оценке выполнения требований к обеспечению защиты информации, проведенной в соответствии с национальным стандартом Российской Федерации ГОСТ Р 57580.2-2018 «Безопасность финансовых (банковских) операций. Защита информации финансовых организаций. Методика оценки соответствия».

Согласно Положению Банка России № 802-П требования к защите информации распространяются на автоматизированные системы, программное обеспечение, средства вычислительной техники, телекоммуникационное оборудование (далее при совместном упоминании - объекты информационной инфраструктуры), применяемые для формирования (подготовки), обработки, передачи и хранения защищаемой информации, в частности о конфигурации, определяющей параметры работы объектов информационной инфраструктуры, а также о конфигурации, определяющей параметры работы технических средств защиты информации[154].

[154] п. 2.2 Положения Банка России № 719-П.

Соответственно, при работе с такой информацией для объектов информационной инфраструктуры участники должны применять меры защиты информации, посредством выполнения которых обеспечивается реализация стандартного уровня (уровня 2) защиты информации. Стандартом «Защита информации финансовых организаций»[155] кредитным организациям для обеспечения выполнения требований к защите персональных данных при их обработке в информационных системах персональных данных (ИСПДн) рекомендуется реализовывать требования к содержанию базового состава мер защиты информации для соответствующих уровней защиты информации, установленных данным стандартом.

Требования к обеспечению защиты информации применительно к некредитным финансовым организациям, а также лицам, оказывающим профессиональные услуги на финансовом рынке, закреплены в отдельных нормативных актах Банка России[156].

Очевидно, что **при передаче и обработке кредитной организацией такой информации IT-аутсорсер должен выполнять требования защиты информации, не ниже, чем это установлено для кредитных организаций или некредитных финансовых организаций, а также лиц, оказывающих профессиональные услуги на финансовом рынке. Однако в отсутствие специального регулирования в отличие от кредитных организаций IT-аутсорсер будет обязан привлекать организацию, имеющую лицензию на осуществление деятельности по технической защите конфиденциальной**

[155] ГОСТ Р 57580.1-2017. Национальный стандарт Российской Федерации. Безопасность финансовых (банковских) операций. Защита информации финансовых организаций. Базовый состав организационных и технических мер (утв. и введен в действие Приказом Росстандарта от 08.08.2017 N 822-ст).

[156] Положение Банка России от 17.10.2022 № 808-П «О требованиях к обеспечению защиты информации при осуществлении деятельности в сфере оказания профессиональных услуг на финансовом рынке в целях противодействия осуществлению незаконных финансовых операций, обязательных для лиц, оказывающих профессиональные услуги на финансовом рынке, к обеспечению бюро кредитных историй защиты информации, указанной в статье 4 Федерального закона "О кредитных историях", при ее обработке, хранении и передаче сертифицированными средствами защиты, а также к сохранности информации, полученной в процессе деятельности кредитного рейтингового агентства» // Вестник Банка России. 2022. № 62.; Положение Банка России от 20.04.2021 № 757-П «Об установлении обязательных для некредитных финансовых организаций требований к обеспечению защиты информации при осуществлении деятельности в сфере финансовых рынков в целях противодействия осуществлению незаконных финансовых операций» // Вестник Банка России. 2021. № 42.

информации, для проведения работ и предоставления услуг, предусмотренных подпунктами "б", "д" или "е" пункта 4 Положения о лицензировании деятельности по технической защите конфиденциальной информации[157].

Следует отметить, что в данной сфере Банком России также принято Указание от 10.12.2015 № 3889-У «Об определении угроз безопасности персональных данных, актуальных при обработке персональных данных в информационных системах персональных данных»[158].

При выполнении функций поставщика услуг аутсорсинга ПО в рамках сервисов биометрии IT-аутсорсер также может ориентироваться на перечень соответствующих угроз безопасности в рамках Указания Банка России от 16.12.2021 № 6017-У «О перечне угроз безопасности, актуальных при обработке биометрических персональных данных, их проверке и передаче информации о степени их соответствия предоставленным биометрическим персональным данным физического лица, при взаимодействии организаций финансового рынка с единой биометрической системой»[159].

В свете анализа вопросов взаимодействия с регуляторами при работе с соответствующей информацией необходимо проанализировать вопросы потенциального взаимодействия IT-аутсорсера с ФиНЦЕРТ. Как было отмечено в предыдущем разделе, соглашения о взаимодействии с ФинЦЕРТ по вопросу предупреждения и противодействия компьютерным атакам могут быть заключены разными участниками рынка, в том числе и IT-компаниями. За последние годы количество активных участников информационного обмена ФинЦЕРТ, регулярно передающих информацию о выявленных угрозах и уязвимостях, увеличилось[160]. Данное обстоятельство связано с активной реализацией поднадзорными организациями принятого в 2018 году Стандарта

---

[157] утв. постановлением Правительства Российской Федерации от 03.02.2012 N 79.
[158] Вестник Банка России. 2016. № 35.
[159] Вестник Банка России. 2022. № 11.
[160] См.: Отчет Центра мониторинга и реагирования на компьютерные атаки в кредитно-финансовой сфере Департамента информационной безопасности Банка России. М. 2019. С. 15 // https://cbr.ru/Collection/Collection/File/32087/FINCERT_report_20191010.PDF

Банка России СТО БР БФБО-1.5-2018[161]. В настоящее время взаимодействие с участниками информационного обмена осуществляется согласно Стандарту Банка России «Безопасность финансовых (банковских) операций. Управление инцидентами, связанными с реализацией информационных угроз, и инцидентами операционной надежности. О формах и сроках взаимодействия Банка России с кредитными организациями, некредитными финансовыми организациями и субъектами национальной платежной системы при выявлении инцидентов, связанных с реализацией информационных угроз, и инцидентов операционной надежности» СТО БР БФБО-1.5-2023[162]. Область действия данного Стандарта определяется требованиями законодательства Российской Федерации, в том числе нормативных актов Банка России, которыми предусмотрены обязанности участников информационного обмена по информированию Банка России. Так, согласно ст. 75.5 Закона о Банке России ЦБ РФ устанавливает обязательные для кредитных организаций требования к операционной надежности при осуществлении банковской деятельности в целях обеспечения непрерывности оказания банковских услуг. Согласно п. 6.4. Положения Банка России от 12.01.2022 № 787-П «Об обязательных для кредитных организаций требованиях к операционной надежности при осуществлении банковской деятельности в целях обеспечения непрерывности оказания банковских услуг»[163] кредитные организации должны обеспечивать выполнение следующих требований к взаимодействию с поставщиками услуг в сфере информационных технологий:

- нейтрализация информационных угроз, связанных с привлечением поставщиков услуг в сфере информационных технологий, в том числе защита объектов информационной инфраструктуры от возможной реализации информационных

[161] Стандарт утратил силу.
[162] Стандарт принят и введен в действие приказом Банка России от 08.02.2023 N ОД-215 // https://cbr.ru/crosscut/lawacts/file/6150
[163] Вестник Банка России. 2022. № 25.

угроз со стороны поставщиков услуг в сфере информационных технологий;

- нейтрализация информационных угроз, обусловленных технологической зависимостью функционирования объектов информационной инфраструктуры кредитной организации от поставщиков услуг в сфере информационных технологий.

При этом согласно п. 6.3 Положения Банка России № 787-П **кредитные организации должны** обеспечивать выполнение ряда требований к выявлению, регистрации инцидентов операционной надежности и реагированию на них, а также восстановлению выполнения технологических процессов и функционирования объектов информационной инфраструктуры после реализации таких инцидентов, в том числе **организовать взаимодействие между подразделениями кредитной организации, а также между кредитной организацией и Банком России, иными участниками технологического процесса в рамках реагирования на инциденты операционной надежности и восстановления выполнения технологических процессов и функционирования объектов информационной инфраструктуры после реализации инцидентов операционной надежности**.

Таким образом, банки должны обеспечить взаимодействие с Банком России об инцидентах операционной надежности о событиях операционного риска или серии связанных событий операционного риска, вызванных информационными угрозами и (или) сбоями объектов информационной инфраструктуры, которые привели к неоказанию или ненадлежащему оказанию банковских или финансовых услуг, то есть событиях операционного риска, связанных с нарушением операционной надежности.

Также в рамках Стандарта банки должны обеспечить взаимодействие с Банком России об инцидентах с реализацией информационных угроз, в свете настоящего раздела, к ним относятся инциденты защиты информации, в том числе незаконное раскрытие банковской тайны, персональных данных и (или)

иных данных клиентов или работников участника информационного обмена, компьютерные инциденты, компьютерные атаки и уязвимости информационной безопасности, которые могут привести к инциденту защиты информации или компьютерному инциденту.

Таким образом, с точки зрения осуществления взаимодействия IT-аутсорсера с регулирующими органами вследствие передачи ему от банка соответствующей информации, следует отметить, что передача IT-аутсорсеру информации от кредитных организаций, в том числе персональных данных и сведений, охраняемых режимом банковской тайны, неизбежно повлечет такое взаимодействие. При этом для того, чтобы кредитные организации могли взаимодействовать с IT-аутсорсером, и поскольку они остаются ответственными за обеспечение надлежащего уровня защиты конфиденциальной информации, очевидна необходимость распространения на IT-аутсорсера стандартов обеспечения защиты, в том числе конфиденциальной информации, не ниже, чем для кредитных организаций или некредитных финансовых организаций, а также лиц, оказывающих профессиональные услуги на финансовом рынке, в том числе рассмотренных стандартов, устанавливающих общие подходы к управлению инцидентами, связанными с реализацией информационных угроз, и инцидентами операционной надежности.

При взаимодействии IT-аутсорсера с регулятором необходимо проанализировать не только регуляторные, но и надзорные требования. В отношении надзорных методов и средств, применяемых к IT-аутсорсеру, необходимо отметить как общие правила, так и ближайшие специализированные надзорные тенденции.

В рамках антикризисных (антисанкционных) мер до 3 марта 2025 г. в отношении аккредитованных IT-организаций приостановлено проведение выездных (повторных выездных) налоговых проверок. Исключение - проверки, назначенные с согласия руководителя (его заместителя)

вышестоящего налогового органа или руководителя (его заместителя) ФНС России. Проверки, которые были начаты до получения соответствующего письма Минфина России, завершаются в установленном порядке. Срок их проведения не может быть продлен или приостановлен, однако в некоторых случаях возможно проведение дополнительных мероприятий налогового контроля.

В отношении аккредитованных IT-компаний законом запрещены плановые проверки, на которые распространяется Федеральный закон от 26.12.2008 № 294-ФЗ[164]. Запрет действует по 31.12.2024.

Что касается отраслевого надзора, следует отметить, что создание IT-аутосорсера вписывается в концепцию внедрения SupTech- и RegTech-решений. Задачами внедрения RegTech-решений являются:

- автоматизация и стандартизация бизнес-процессов, связанных с обеспечением и выполнением регуляторных требований;
- снижение рисков и затрат, в том числе на соблюдение комплаенс-требований, повышение точности выполнения требований регулятора;
- повышение уровня оперативности выявления мошеннических действий и реагирования на них.

Банк России проводит работу в направлении развития SupTech и RegTech и руководствуется подходами, отраженными в документах Базельского комитета по банковскому надзору, в том числе принципом, согласно которому надзор должен адаптироваться к уровню и трендам цифровизации деятельности поднадзорных организаций[165].

При этом основными направлениями применения SupTech и RegTech решений участниками финансового рынка являются:

---

[164] Федеральный закон от 26.12.2008 N 294-ФЗ «О защите прав юридических лиц и индивидуальных предпринимателей при осуществлении государственного контроля (надзора) и муниципального контроля» // СЗ РФ. 2008, N 52 (ч. 1), ст. 6249.

[165] Доклад Банка России «Основные направления SupTech и RegTech на период 2021-2023 годов». М., 2021. С. 2. // https://cbr.ru/Content/Document/File/120709/SupTech_RegTech_2021-2023.pdf

- противодействие отмыванию доходов, полученных преступным путем, и финансированию терроризма;
- обеспечение информационной безопасности;
- выявление неправомерных действий на финансовом рынке;
- совершенствование процедур идентификации с использованием биометрических технологий;
- внедрение датацентричного подхода.

Такие **подходы как на уровне SupTech и RegTech решений при осуществлении надзора Банка России не только меняют технологии взаимодействия Банка России и поднадзорных субъектов, но и, безусловно, затронут вопросы безопасности передачи информации IT-аутсорсеру.**

Следует отметить и инициативу Банка России в рамках обеспечения информационной безопасности по подготовке «Рекомендаций по использованию облачных сервисов на финансовом рынке». Определение рекомендаций по использованию облачных решений, в том числе с целью создания облачных хранилищ данных, позволит снизить трудозатраты как для Банка России, так и для поднадзорных организаций, оптимизировать процесс предоставления информации от поднадзорных организаций. Облачные сервисы смогут обеспечить централизованный сбор, хранение и использование в надзорных целях информации, получаемой от поднадзорных организаций. В рамках данной инициативы предлагается сформировать рекомендации по использованию облачных сервисов участниками финансового рынка[166].

Банк России полагает, что особое значение для российского финансового рынка будет иметь развитие российских информационных сервисов, ориентированных на участников рынка, экспертов и инвесторов, желающих получать качественную информацию. При этом основными

[166] Инициатива № 37. Доклад Банка России «Основные направления SupTech и RegTech на период 2021-2023 годов». М., 2021. С. 31. // https://cbr.ru/Content/Document/File/120709/SupTech_RegTech_2021-2023.pdf

механизмами воздействия на финансовый рынок, создания условий и стимулов для его развития: нормативно-правовое регулирование и надзор; мягкое регулирование; кодексы, стандарты СРО, рекомендательные письма; создание и развитие элементов цифровой инфраструктуры финансового рынка, обеспечение равного доступа к ней.[167] **Таким образом, правовая модель универсального IT-аутсорсера в целях обеспечения равного доступа к цифровой инфраструктуре должна минимизировать обозначенные риски, сбалансировать возможности различных кредитных организаций на рынке. Тем не менее, в случае создания универсального IT-аутсорсера высока вероятность монополизации рынка со всеми вытекающими негативными последствиями.** Банк России в Докладе также отмечает, что зависимость от поставщика услуг в случае его монопольного положения на рынке или зависимость от отдельных поставщиков услуг, имеющих значительную долю на рынке оказываемых ими услуг и возможность влиять на стоимость своих услуг (market power)[168].

Полагаем, что минимизация данного риска может быть реализована как стандартными механизмами контроля за экономической концентрацией, так и повышением требований, в первую очередь, к универсальному IT-аутсорсеру, через понижение порога установления доминирующего положения на рынке по аналогии с финансовыми организациями.

2. Рекомендации по определению оптимальной организационно-правовой формы компании-аутсорсера при модели универсального посредника (по результатам анализа по вопросам Таблицы № 1 к Техническому заданию), в том числе анализ преимуществ и недостатков для:

5) союзов и ассоциаций;

[167] Основные направления развития финансового рынка Российской Федерации на 2023 год и период 2024-2025 годов. М., 2022. С. 12, 62. // https://cbr.ru/Content/Document/File/143773/onfr_2023-2025.pdf

[168] Доклад Банка России для общественных слушаний «Управление рисками аутсорсинга на финансовом рынке». М., 2022. С. 5. // https://cbr.ru/Content/Document/File/142481/Consultation_Paper_06122022.pdf

6) **кооператива;**

7) **общества с ограниченной ответственностью;**

8) **акционерного общества.**

Ассоциация (союз)

Ассоциацией (союзом) признается объединение юридических лиц и (или) граждан, основанное на добровольном или в установленных законом случаях на обязательном членстве и созданное для представления и защиты общих, в том числе профессиональных, интересов, для достижения общественно полезных целей, а также иных не противоречащих закону и имеющих некоммерческий характер целей (ст. 123.8 ГК РФ, ст. 11 Федерального закона от 12.01.1996 № 7-ФЗ «О некоммерческих организациях»[169] (далее – Закон об НКО)). Полученная некоммерческой организацией прибыль не подлежит распределению между участниками (членами) некоммерческой организации (п. 3 ст. 26 Закона об НКО).

Любая некоммерческая организация (далее также – НКО) может осуществлять предпринимательскую и иную приносящую доход деятельность лишь постольку, поскольку это служит достижению целей, ради которых она создана и соответствует указанным целям, при условии, что такая деятельность указана в ее учредительных документах. Такой деятельностью признаются приносящее прибыль производство товаров и услуг, отвечающих целям создания некоммерческой организации, а также приобретение и реализация ценных бумаг, имущественных и неимущественных прав, участие в хозяйственных обществах и участие в товариществах на вере в качестве вкладчика (п. 2 ст. 24 Закона об НКО). Таким образом, **при создании IT-аутсорсера в организационно-правовой форме ассоциации (союза) основной его целью не сможет выступать извлечение прибыли, а доход, полученный от его деятельности, не будет распределяться среди его членов**. **Полагаем, что организационно-правовые формы**

[169] СЗ РФ. 1996, N 3, ст. 145.

некоммерческих организаций, в том числе такой, как ассоциация (союз), не вполне подходит идее универсального IT-аутсорсера, который, как и действующие на рынке IT-аутсорсинга субъекты, будет осуществлять все или часть функций по поставке услуг аутсорсинга ПО (например: создание/адаптация/развитие/сопровождение прикладного ПО автоматизированной банковской системы (АБС); поставка общесистемного ПО (операционные системы, системы управления базами данных, ПО серверов приложений и т.д.); предоставление эксплуатирующего IT-персонала (аутстаффинг); организация технической поддержки ПО), по предоставлению инфраструктуры (например: предоставление вычислительных мощностей; предоставление систем хранения данных; предоставление услуг телекоммуникационной связи и т.д.), а также услуги в области организации и обеспечения защиты информации (например: средствами защиты информации от воздействия вредоносного кода (СЗИ от ВВК; средствами защиты от несанкционированного доступа (СЗИ от НСД); средствами криптографической защиты информации (СКЗИ); средствами инженерно-технической защиты информации (система контроля и управления доступом (СКУД) и т.д.). Данная деятельность осуществляется субъектами рынка IT-аутсорсинга в целях извлечения прибыли, которые в абсолютном большинстве случаев являются субъектами предпринимательской деятельности, зарегистрированными в организационно-правовых формах коммерческих организаций. Перенесение указанного функционала на универсального IT-аутсорсера не изменит предпринимательскую природу указанной деятельности, в связи с чем создание универсального IT-аутсорсера в организационно-правовой форме ассоциации (союза) может повлечь за собой возникновение споров, в том числе судебных. Так, Министерство Юстиции РФ, являющееся регистрирующим органом для НКО, обращает внимание на

то, что перечень видов деятельности, осуществляемой некоммерческой организацией, должен быть указан в ее уставе в полном объеме[170].

Таким образом, хотя НКО могут осуществлять деятельность, приносящую доход, но делать они это могут только в уставных целях. Поэтому такой IT-аутсорсер будет изначально ограничен теми видами деятельности, которые будут закреплены в его Уставе[171], что видится неудобным, особенно с учетом стремительного развития данной отрасли с возможностью появления все нового функционала.

Кроме того, в отличие от коммерческих организаций, где участник обладает правами на акцию, долю или пай, никаких прав на вложения (членские взносы) у члена ассоциации не возникает, собственником членских взносов и так является сама ассоциация (союз), соответственно, как было отмечено, полученный доход между членами ассоциации не распределяется.

Еще одной препоной, по нашему мнению, является такое право члена ассоциации, как право на равных началах с другими членами пользоваться безвозмездно оказываемыми ассоциацией услугами (ст. 123.11 ГК РФ). В этом случае, если часть кредитных организаций станет членами ассоциации, неизбежно возникнет конфликт интересов между членами ассоциации и иными кредитными организациями, для которых услуги будут платными. Включение же всех кредитных организаций, функционирующих на рынке, в члены ассоциации видится мало реализуемым. При этом перечень IT-услуг, которые могут потребоваться разным кредитным организациям, также может очень сильно разниться. Все это неизбежно создаст сложности в организации деятельности ассоциации, поскольку согласно ст. 123.10 ГК РФ принятие решений о порядке определения размера и способа уплаты членских взносов,

---

[170] См. п. 2 Обзора типичных нарушений обязательных требований, выявленных при осуществлении контрольно-надзорных функций Минюста России с разъяснением положений законодательства Российской Федерации, несоблюдение которых повлекло данные нарушения" (утв. Минюстом России) // Документ опубликован не был. https://minjust.gov.ru

[171] Так, в Апелляционном определении Апелляционной коллегии Верховного Суда РФ от 20.09.2017 N АПЛ17-367 Верховным Судом РФ было принято решение о ликвидации ассоциации за систематическое осуществление ею деятельности, противоречащей ее уставным целям (сдача имущества в аренду). // Документ опубликован не был. Доступ из СПС «КонсультантПлюс».

о дополнительных имущественных взносах членов ассоциации (союза) в ее имущество относится к исключительной компетенции высшего органа ассоциации (союза), которым, как правило, является Собрание членов ассоциации. Включение в качестве членов ассоциации субъектов рынка IT-аутсорсинга, в том числе поставщиков ПО, видится для этой организационно-правовой формы в принципе не рациональным, так как не совсем ясно, какие услуги за счет своих членских взносов им сможет оказывать универсальный IT-аутсорсер.

Кооператив

Производственным кооперативом (артелью) (далее - кооператив) признается добровольное объединение граждан на основе членства для совместной производственной и иной хозяйственной деятельности, основанной на их личном трудовом и ином участии и объединении его членами (участниками), в том числе юридическими лицами, имущественных паевых взносов, являющееся коммерческой организацией (ст. 2 Федерального закона от 08.05.1996 № 41-ФЗ «О производственных кооперативах»[172] (далее – Закон о кооперативах)).

Традиционно производственные кооперативы не являются популярной организационно-правовой формой среди коммерческих организаций и в настоящее время представлены лишь около 0,02% от всех коммерческих организаций[173], что является, на наш взгляд, недостатком и с точки зрения глубины проработки его правового статуса в законодательстве, и с точки зрения доверия к данной организационно-правовой форме со стороны участников рынка. Тем не менее, в зарубежном правопорядке функционируют субъекты финансового рынка в организационно-правовых формах, имеющих общие черты с кооперативом. В связи с этим, в целях исследования преимуществ и недостатков данной организационно-правовой формы для создания универсального IT-аутсорсера целесообразно представить анализ

[172] СЗ РФ. 1996, N 20, ст. 2321.
[173] См.: www.nalog.ru

одной из крупнейших международных компаний СВИФТ - “Society for Worldwide Interbank Financial Telecommunication” (S.W.I.F.T. SC or SWIFT), которая является так называемой кооперативной компанией (société cooperative – SCOP) и включает как переменный капитал, так и переменное количество партнеров[174]. Кооперативная организация предполагает условие о личном трудовом участии, которое, тем не менее, понимается в бельгийском законодательстве совершенно в обратном по сравнению с российским законодательством ключе. Согласно ст. 15 Устава СВИФТ, поскольку компания СВИФТ является кооперативной компанией, она ожидает, что акционеры будут активно поддерживать и вносить свой вклад в использование услуг Компании. Примечательно, что любая передача акций участниками является недействительной, за исключением случаев слияния, приобретения, реструктуризации, разделения, дробления или любой другой аналогичной юридической процедуры с участием передающего акционера, при условии, что получатель отвечает критериям приемлемости и условиям приема в качестве акционера. Таким образом, в организационно-правовой форме кооперативной компании есть ограничения на отчуждение акций, тем не менее не связанное с преимущественным правом покупки и согласия членов кооператива, как это реализовано применительно к российской организационно-правовой форме производственного кооператива, но предполагающие установление определенных требований к приобретателю акций. Также Совет директоров компании СВИФТ может приостановить действие или исключить акционера из Компании, что также возможно и в производственном кооперативе. При этом компания СВИФТ ближе с точки зрения основных характеристик данной организационно-правовой формы не к производственному кооперативу, а к российскому акционерному обществу, а с учетом отмеченных выше характеристик, - именно к непубличному акционерному обществу. Так, согласно действующей редакции Устава

[174]https://guichet.public.lu/en/entreprises/creation-developpement/forme-juridique/societe-capitaux/societe-cooperative.html

СВИФТ[175] 1 января 2020 года Компания выпустила 109,612 акций. Совет директоров на каждом годовом общем собрании информирует акционеров о новых акциях, выпущенных в течение предыдущего финансового года; эта информация включается в годовой отчет Совета директоров. Ответственность акционеров перед третьими лицами ограничивается их обязательством оплатить свои акции. Акционером может стать в принципе любая компания, удовлетворяющая критериям приемлемости и условий приема, изложенных в Корпоративных правилах. Количество акций, принадлежащих акционеру, должно быть пропорционально ежегодному финансовому взносу, выплачиваемому компании СВИФТ таким акционером за сетевые услуги, предоставляемые ему компанией СВИФТ. Таким образом, количество акций фактически распределяется пропорционально трафику передаваемых сообщений. В связи с этим Совет директоров должен (повторно) распределять акции как минимум каждые три года. С целью осуществления такого (повторного) распределения акционеры, вынужденные отказаться от акций, должны отозвать количество акций, определенных Советом директоров, и акционеры, которым необходимо приобрести дополнительные акции, должны приобрести новые акции в количестве, определенном Советом директоров.[176]

Рассмотренная правовая модель организации компании СВИФТ является интересной с точки зрения создания универсального IT-аутсорсера, поскольку предполагает при наличии коммерческой составляющей участие в капитале компаний исходя из объема получаемых от IT-аутсорсера услуг, что в некоторой степени сближает ее с организационно-правовой формой ассоциации. Тем не менее, в российском правопорядке достаточно сложно реализовать такую модель с учетом ограничений, которые имеются в каждой из рассмотренных (см. таблица № 1) организационно-правовых форм. Более того, представляется, что IT-аутсорсер будет обладать гораздо большим объемом функционала, иметь доступ к более широкому объему данных, в том

[175] https://www.swift.com/about-us/legal/corporate-matters/swift-laws
[176] https://www.swift.com/about-us/legal/corporate-matters

числе связанных с обеспечением информационной безопасности, поэтому при перераспределении долей (акций, паев) в уставном (складочном) капитале исходя из объема пользования его услугами могут появляться мажоритарные акционеры (пайщики) и увеличиться риск конфликта интересов с учетом реализации прав при принятии решений общим собранием акционеров (пайщиков) и представительством в Совете директоров с учетом правил кумулятивного голосования (для ПАО).

Если обратиться к требованиям российского законодательства о производственных кооперативах, то помимо непопулярности данной организационно-правовой формы, что может оказать влияние в целом на репутацию универсального IT-аутсорсера, необходимо отметить еще ряд ключевых характеристик. Как было указано, членами (участниками) кооператива могут быть граждане Российской Федерации, иностранные граждане, лица без гражданства. Таким образом, юридическое лицо может участвовать в деятельности кооператива только через своего представителя – физическое лицо, в соответствии с уставом кооператива, что может быть неудобно с учетом того, что потенциальными участниками универсального IT-аутсорсера являются исключительно юридические лица.

С учетом необходимости личного трудового участия пайщиков, рассматриваемая организационно-правовая форма ограничит возможное разнообразие субъектов, которые могут стать ее членами, поскольку, исходя из функций IT-аутсорсера личное трудовое участие можно реализовать в основном только через конкретных физических лиц-представителей поставщиков ПО и других участников рынка IT-аутсорсинга, но не за счет кредитных организаций, ассоциаций или Банка России, поскольку по смыслу российского законодательства пользование услугами компании вряд ли можно отнести к личному трудовому участию. Причем согласно п. 2 ст. 7 Закона о кооперативах не менее 75% пайщиков участвуют личным трудовым вкладом.

Структура органов управления производственного кооператива и их компетенция достаточно гибкая. Так, общее собрание членов кооператива вправе рассматривать и принимать решение по любому вопросу образования и деятельности кооператива (п. 1 ст. 15 Закон о кооперативах). Оно правомочно принимать решения, если на нем присутствует более пятидесяти процентов общего числа членов кооператива. Голосуют простым большинством голосов присутствующих на собрании. Снижению вероятности возможного конфликта интересов и возникновения ситуации существенного влияния и контроля может способствовать правило о том, что каждый член кооператива независимо от размера его пая имеет при принятии решений общим собранием членов кооператива один голос (п. 2 ст. 15 Закон о кооперативах), в связи с чем отсутствует необходимость обеспечения паритетного участия в уставном капитале (для ПАО), установления ограничения количества акций, принадлежащих одному акционеру, и их суммарной номинальной стоимости, а также максимального числа голосов, предоставляемых одному акционеру (для неПАО), установления ограничения максимального размера доли участника общества и изменения соотношения долей участников общества (для ООО). С другой стороны, для крупной компании, каковой видится универсальный IT-аутсорсер, все же более оптимален учет соотношения размера его вклада в уставный капитал и голоса, который он ему предоставляет. Тем не менее, в производственных кооперативах (п. 5 ст. 9 Закон о кооперативах) его член может на договорных началах передавать принадлежащие ему материальные ценности и иные средства кооперативу. При этом выход или исключение из кооператива не являются основанием для одностороннего прекращения или изменения взаимоотношений члена кооператива и кооператива по поводу переданного имущества, если иное не предусмотрено соглашением сторон, что является определенным преимуществом данной организационно-правовой формы, но не определяющим ее приоритет над другими с учетом отмеченных в настоящем разделе недостатков.

Общество с ограниченной ответственностью

Согласно Федеральному закону 08.02.1998 № 14-ФЗ «Об обществах с ограниченной ответственностью»[177] (далее – ФЗ об ООО) обществом с ограниченной ответственностью (далее - ООО) признается созданное одним или несколькими лицами хозяйственное общество, уставный капитал которого разделен на доли; участники общества не отвечают по его обязательствам и несут риск убытков, связанных с деятельностью общества, в пределах стоимости принадлежащих им долей в уставном капитале общества.

В настоящее время общества с ограниченной ответственностью составляют около 96% от всех коммерческих организаций[178], то есть абсолютное большинство. Данное обстоятельство связано с универсальностью данной организационно-правовой формы для самых разных направлений предпринимательской деятельности, и соответственно легкостью государственной регистрации и максимальной гибкостью законодательного регулирования по сравнению с иными хозяйственными обществами.

Число участников (учредителей) ООО не должно быть более пятидесяти. В случае превышения лимита ООО должно преобразоваться в открытое АО[179] или в производственный кооператив. Данное требование может стать препятствием в случае создания универсального IT-аутсорсера с участием большого числа кредитных организаций и субъектов рынка IT-аутсорсинга.

Следует отметить, что ООО не обязано публиковать отчетность о своей деятельности (ст. 49 Закона об ООО), кроме случая публичного размещения

---

[177] СЗ РФ. 1998, N 7, ст. 785.

[178] См.: www.nalog.ru

[179] Как верно отмечается в литературе по вопросу устаревшей редакции ст. 7 Закона об ООО, предусматривающей термин «открытое акционерное общество», «очевидно, что общество с ограниченной ответственностью может преобразоваться в непубличное акционерное общество, поскольку при преобразовании доли участия будут конвертироваться в акции, распределяемые среди ограниченного круга лиц - участников ООО» // Научно-практический комментарий к Федеральному закону "Об обществах с ограниченной ответственностью": в 2 томах под ред. И.С. Шиткиной. Москва: Статут, 2021. Т. 1. 622 с. (автор комментария к ст. 7 Е.П. Губин).

облигаций и иных ценных бумаг, что, на наш взгляд, является недостатком для универсального IT-аутсорсера, для которого важны репутационные риски.

С точки зрения риска потери финансовой устойчивости для ООО негативной характеристикой является право участника выйти из общества путем отчуждения своей доли обществу, если такая возможность предусмотрена уставом общества, или потребовать приобретения обществом доли в случаях, предусмотренных п. 2 ст. 23 Закона об ООО. В случае выхода участника общество обязано выплатить ему действительную стоимость его доли или части доли в уставном капитале общества либо выдать ему в натуре имущество такой же стоимости в течение трех месяцев со дня возникновения соответствующей обязанности, если иной срок или порядок выплаты действительной стоимости доли или части доли не предусмотрен уставом общества (п. 6 ст. 23 Закона об ООО). Таким образом, включение в Устав права участника на выход из общества делает ООО неустойчивой организационно-правовой формой, ведь если доля значительна, то на самом обществе лежит обязанность выплатить ее действительную стоимость, что может крайне негативно отразиться на финансовой устойчивости компании.

В качестве отдельной возможности Законом об ООО предусмотрено формирование Совета директоров (наблюдательного совета) общества, но только если это предусмотрено Уставом общества (п. 2 ст. 32 Закона об ООО). В рамках императивных требований корпоративного законодательства ООО не обязано создавать в структуре органов управления Совет директоров, что, на наш взгляд, является недостатком с точки зрения возможных полномочий Совета директоров по предотвращению конфликта интересов.

В качестве преимущества для универсального IT-аутсорсера как средства снижения вероятности конфликта интересов и получения одним или несколькими учредителями (участниками) контроля или существенного влияния в отношении общества можно рассматривать требование п. 3 ст. 14 Закона об ООО, согласно которому Уставом общества может быть ограничен максимальный размер доли участника

общества. Уставом общества может быть ограничена возможность изменения соотношения долей участников общества. При этом такие ограничения не могут быть установлены в отношении отдельных участников общества. Указанные положения могут быть предусмотрены уставом общества при его учреждении, а также внесены в устав общества, изменены и исключены из устава общества по решению общего собрания участников общества, принятому всеми участниками общества единогласно. В случае, если устав общества содержит указанные выше ограничения, то лицо, которое приобрело долю в уставном капитале общества с нарушением данных требований и соответствующих положений устава общества, вправе голосовать на общем собрании участников ООО частью доли, размер которой не превышает установленный уставом общества максимальный размер доли участника общества.

В целом в организационно-правовой форме ООО достаточно сложно найти недостатки, если учитывать максимальную гибкость данной формы в сравнении с иными хозяйственными обществами, выражающуюся, как было показано выше, в возможности предусмотреть в Уставе фактически диаметрально противоположные модели. Тем не менее, полагаем, что **к IT-аутсорсеру должны предъявляться дополнительные требования с точки зрения минимизации риска конфликта интересов, финансовой устойчивости, раскрытия информации о своей деятельности, формирования уставного капитала и др. Поэтому в отсутствие специального законодательного регулирования в отношении корпоративных требований к IT-аутсорсеру общество с ограниченной ответственностью как организационно-правовая форма не сможет в полной мере обеспечить данные задачи минимизации рисков, поскольку учредители сами будут решать, какова будет структура органов управления обществом, компетенция, структура уставного капитала, права участников, в том числе на выход из ООО, а также какая информация будет раскрываться обществом.**

Акционерное общество

Организационно-правовая форма акционерных обществ представлена в российском законодательстве двумя типами: публичные акционерные общества (далее также – ПАО, ранее ОАО) и непубличные акционерные общества (далее также – неПАО, ранее ЗАО). В настоящее время акционерные общества представлены лишь 2% от всех коммерческих организаций, а публичные акционерные общества (а также ОАО) составляют около 13% от всех акционерных обществ[180], что предопределено тем, что ПАО являются юридической оболочкой для крупного бизнеса, нацеленного на получение сторонних инвестиций, в том числе за счет публичного размещения акций и работе на вторичном рынке ценных бумаг. Это в свою очередь с законодательной точки зрения влечет бо́льшую сложность их государственной регистрации и меньшую гибкость в возможностях самостоятельно определять как структуру органов управления, их компетенцию, так и права и обязанности акционеров. Поэтому правовой статус публичных обществ определяется «от обратного» - путем установления в законодательстве диспозитивных возможностей для непубличных обществ.

В ПАО существуют императивные требования по структуре органов управления общества. В частности, в императивном порядке должен быть создан коллегиальный орган управления – Совет директоров (наблюдательный совет), который осуществляет общее руководство деятельностью общества, за исключением решения вопросов, отнесенных Законом об АО к компетенции общего собрания акционеров (п. 1 ст. 64 Закона об АО). Количественный состав совета директоров (наблюдательного совета) публичного общества составляет пять членов, если Уставом не предусмотрено большее количество[181].

---

[180] См.: www.nalog.ru

[181] В рамках антисанкционного регулирования был принят ряд мер в отношении Совета директоров, что особенно важно для ПАО. Согласно Федеральному закону от 14.07.2022 № 292-ФЗ "О внесении изменений в отдельные законодательные акты Российской Федерации, признании утратившим силу абзаца шестого части первой статьи 7 Закона Российской Федерации "О государственной тайне", приостановлении действия отдельных положений законодательных актов Российской Федерации и об установлении особенностей регулирования корпоративных отношений в 2022 и 2023 годах" до 31 декабря 2023 года Совет директоров

Также в ПАО компетенция и порядок принятия решений органами управления, в частности общим собранием акционеров достаточно сильно формализован. Решения по вопросам, прямо указанным в Законе об АО (ст.48) и ГК РФ (п. 2 ст. 65.3, 67.1) относятся к исключительной компетенции общего собрания. Решение на общем собрании акционеров принимается большинством голосов (абз. 1 п. 2, п. 4.2 ст. 49) либо квалифицированным большинством (п. 4 ст. 49 Закона об АО).

Аспект, осложняющий принятие решений связан с тем, что общее собрание не вправе принимать решения по вопросам, не включенным в повестку дня собрания, а также изменять повестку дня. Такое требование закона (п. 6 ст. 49 Закона об АО) делает процедуру принятия решений не гибкой.

Кроме того, всегда высоки риски обжалования принятых решений на собрании ввиду того, что количество акционеров законом не ограничено, а право на обжалование имеется у широкого круга лиц (акционеров, не присутствующих на собрании (п. 7 ст. 49 З об АО), акционеры, голосовавшие против и чьи интересы нарушены и т.д.

Ввиду того, что для публичного общества не предусмотрена возможность передать решение вопроса на усмотрение единоличного исполнительному органу, порядок принятия решений также осложняется.

В отличие от ПАО непубличные акционерные общества (далее также - неПАО), имея также достаточно сложную процедуру государственной регистрации, связанную с регистрацией эмиссии ценных бумаг, тем не менее,

---

сохраняет свои полномочия при уменьшении количественного состава (но не менее трех) по сравнению с количеством, предусмотренным Законом об АО (п.3 ст. 66, п. 2 ст. 68 Закона об АО), уставом или решением общего собрания акционеров, до принятия решения об образовании нового состава Совета директоров. Заседание Совета директоров акционерного общества правомочно (имеет кворум), если в нем принимают участие не менее половины от числа оставшихся членов Совета директоров такого общества. Также до 31 декабря 2023 года: в хозяйственных обществах, в отношении которых иностранными государствами и международными организациями введены ограничительные меры, Совет директоров, может не образовываться по решению общего собрания акционеров (участников), даже если его образование предусмотрено законодательством РФ или уставом. Данные меры были призваны обеспечить нормальное функционирование российских акционерных обществ в случае невозможности формаирования Совета директоров из-за санкций, а также позволяют проводить заседания Совета директоров, несмотря на выход из его состава членов Совета директоров-граждан недружественных государств и ограничения воздушного сообщения.

имеют более гибкое регулирование по отмеченным выше параметрам структуры и компетенции органов управления, а также прав и обязанностей акционеров. Тем не менее, для универсального IT-аутсорсера, по нашему мнению, недостатком в отношении неПАО будет являться запрет на публичное размещение акций, возможность исключения акционера с выплатой ему действительной стоимости акций, а также преимущественное право их покупки, если это предусмотрено уставом. По нашему мнению, более жесткие стандарты контроля за деятельностью ПАО являются преимуществом для создания IT-аутсорсера, аккумулирующего в рамках своей деятельности широкий функционал, связанный с передаваемой ему кредитными организациями конфиденциальной информацией, оказанием услуг в области информационной безопасности и т.д. Одним из ключевых рисков, отмечаемых для аутсорсинга и в Руководстве ЕВА по аутсорсингу, и в Докладе Банка России является репутационный риск. Как отмечает Банк России, репутационный риск в данной сфере связан с формированием негативного представления о финансовой устойчивости участника финансового рынка, качестве оказываемых им финансовых услуг или характере деятельности в целом в результате недобросовестных действий (мошенничества) поставщика услуг. В этом смысле ПАО традиционно является тем видом хозяйственного общества, которое за счет предъявляемых к нему императивных требований корпоративного законодательства, структуры органов корпоративного управления, как правило, значительного капитала, прозрачности отчетности, имеет наиболее высокую репутационную составляющую.

Государственный контроль за приобретением акций публичного общества осуществляется в соответствии со ст. 84.9 Закона об АО. Банк России осуществляет контроль за приобретением ценных бумаг, за их выкупом, за добровольным или обязательным предложением по приобретению бумаг.

Локальный контроль за финансово-хозяйственной деятельностью общества осуществляется ревизионной комиссией общества в порядке главы

XII Закона об АО путем проверки (ревизии) деятельности компании. Аудиторская организация (индивидуальный аудитор) общества проводит аудит годовой бухгалтерской (финансовой отчетности) в порядке ст. 86 Закона об АО.

Совет директоров (наблюдательный совет) ПАО утверждает внутренние документы общества, определяющие политику общества в области организации управления рисками и внутреннего контроля (пп. 9.2 п. 1 ст. 65, п. 1 ст. 87.1 Закона об АО).

ПАО обязано раскрывать годовой отчет и бухгалтерскую отчетность, проспект ценных бумаг, сообщение о проведении общего собрания акционеров (п. 1 ст. 92 Закона об АО)

Общество обязано обеспечить акционерам доступ по их требованию к документам, указанным в п. 1 ст. 91 Закона об АО (годовые отчеты, протоколы общих собраний, списки аффилированных лиц и т.д.)

По требованию акционера (акционеров), владеющего не менее чем 25 процентами голосующих акций общества, общество обязано обеспечить доступ к протоколам заседаний коллегиального исполнительного органа общества и к документам бухгалтерского учета. Уставом Общества может быть предусмотрено меньшее количество акций, необходимых для доступа к указанным документам (п. 5 ст. 91 Закона об АО). В требовании акционера (акционеров), владеющего менее чем 25 процентами голосующих акций общества должна быть указана деловая цель, с которой запрашиваются документы (п. 4 ст. 91 Закона об АО).

По требованию акционера (акционеров), владеющего не менее чем одним процентом голосующих акций общества, публичное общество обязано обеспечить доступ к следующим информации и документам – информация по сделкам, протоколы заседаний совета директоров, отчеты оценщиков об оценке имущества (п. 2 ст. 91 Закона об АО).

При этом, в случае если в неПАО более 50 акционеров, то его статус несколько сближается в ПАО в части необходимости раскрытия информации

о своей деятельности. Так, неПАО с числом акционеров более пятидесяти обязано раскрывать годовой отчет общества, годовую бухгалтерскую (финансовую) (п.1.1. ст. 92 Закона об АО). Аналогично, как и в публичных, в отношении неПАО применяется п. 1 ст. 91 Закона об АО о раскрытии информации перед акционерами. По требованию акционера (акционеров), владеющего не менее чем одним процентом голосующих акций общества, непубличное общество помимо доступа к информации и документам из п. 2 ст. 91 обязано обеспечить такому акционеру (акционерам) доступ к иным документам, обязанность хранения которых предусмотрена пунктом 1 ст. 89 (Устав Общества, решения Совета директоров, общего собрания) (п. 3 ст. 91 Закона об АО).

Таким образом, прозрачность деятельности акционерных обществ имеет и свои преимущества с точки зрения клиентов, но также и свои недостатки с учетом санкционных рисков[182].

Для целей настоящего исследования полагаем целесообразным провести анализ правового положения кредитных рейтинговых агентств на предмет возможности использования действующей для них модели применительно к

[182] До 01.07.2023 действовали антисанкционные меры, установленные Постановлением Правительства РФ от 12.03.2022 № 351 «Об особенностях раскрытия и предоставления информации, подлежащей раскрытию и предоставлению в соответствии с требованиями Федерального закона "Об акционерных обществах" и Федерального закона "О рынке ценных бумаг", и особенностях раскрытия инсайдерской информации в соответствии с требованиями Федерального закона "О противодействии неправомерному использованию инсайдерской информации и манипулированию рынком и о внесении изменений в отдельные законодательные акты Российской Федерации», согласно которым эмитенты ценных бумаг были вправе раскрывать/предоставлять информацию, подлежащую раскрытию или предоставлению в соответствии с требованиями Закона об АО и Закона о РЦБ, в ограниченном объеме или отказаться от раскрытия в случае, если раскрытие приведет (может привести) к введению мер ограничительного характера в отношении эмитента и (или) иных лиц, в том числе к введению новых мер ограничительного характера в отношении лица, о котором эмитентом раскрывается и (или) предоставляется информация. Раскрывать инсайдерскую информацию в ограниченных составе и (или) объеме либо отказаться от раскрытия инсайдерской информации в случае, если раскрытие соответствующей информации приведет (может привести) к введению мер ограничительного характера в отношении лица, о котором раскрывается инсайдерская информация, вправе осуществлять: эмитенты, в том числе иностранные; управляющие компании; организаторы торговли, клиринговые организации, а также депозитарии и кредитные организации, осуществляющие расчеты по результатам сделок, совершенных через организаторов торговли; проф.участники рынка ценных бумаг и иные лица, осуществляющие в интересах клиентов операции с финансовыми инструментами, иностранной валютой и (или) товарами, получившие инсайдерскую информацию от клиентов; государственные и муниципальные органы, иные осуществляющие функции указанных органов органы или организации, органы управления государственных внебюджетных фондов, имеющих в соответствии с нормативными правовыми актами РФ право размещать временно свободные средства в финансовые инструменты, публично-правовые компании, Банк России; информационные агентства; лица, осуществляющие присвоение кредитных рейтингов.

универсальному IT-аутсорсеру. Такое решение продиктовано рядом причин, делающих их организацию и деятельность схожими с IT-аутсорсером, в частности: потенциально небольшим числом кредитных рейтинговых агентств в мире и в России с учетом специфики их деятельности, связанной с высокими стандартами деловой репутации на рынке, с близкими рисками, связанными с передачей, обработкой и хранением конфиденциальной информации, с возможным конфликтом интересов[183], особым статусом субъекта, оказывающего профессиональные услуги на финансовом рынке[184] и т.д. Согласно Федеральному закону от 13.07.2015 № 222-ФЗ «О деятельности кредитных рейтинговых агентств в Российской Федерации, о внесении изменения в статью 76.1 Федерального закона «О Центральном банке Российской Федерации (Банке России)» и признании утратившими силу отдельных положений законодательных актов Российской Федерации»[185] (далее – Закон о рейтинговых агентствах) кредитное рейтинговое агентство - юридическое лицо, созданное в организационно-правовой форме хозяйственного общества в соответствии с законодательством Российской Федерации, внесенное Банком России в реестр кредитных рейтинговых агентств в соответствии с требованиями настоящего Федерального закона и осуществляющее рейтинговую деятельность (ст. 2). В настоящее время в реестр Банка России включено четыре кредитных рейтинговых агентства: АКРА (АО), АО «Эксперт РА», ООО «НКР» и ООО «НРА»[186]. Как видно из перечня, два агентства являются акционерными общества и два – обществами с ограниченной ответственностью. При этом крупнейшее рейтинговое агентство АКРА является акционерным обществом.

Таким образом, полагаем, что **ПАО является более устойчивой формой по сравнению с ООО, так как не предполагает выхода участников**

[183] Банк России в Докладе «Управление рисками аутсорсинга на финансовом рынке». М., 2022, отмечает, что одним из отрицательных последствий также может являться высокая вероятность возникновения конфликта интересов при оказании одним поставщиком услуг нескольким участникам финансового рынка. С. 5.
[184] Данный вопрос будет раскрыт отдельно далее.
[185] СЗ РФ. 2015, N 29 (часть I), ст. 4348.
[186] https://cbr.ru/finm_infrastructure/ra/

и выплаты им действительной стоимости доли. Из преимуществ также можно выделить большую привлекательность для инвесторов, и соответственно, выход на международный уровень, в том числе сотрудничество с «дружественными» юрисдикциями[187]. Преимуществом ПАО по сравнению с неПАО и ООО в случае создания IT-аутсорсера, является, по нашему мнению, также обязанность создания Совета директоров, органа, который по примеру требований к кредитным организациям, может быть нацелен на минимизацию конфликта интересов в структуре корпоративного управления компании.

Жесткость требований к аутсорсеру как универсальному посреднику будет компенсироваться эффектом масштаба (соединением большинства функций всего множества посредников). При этом **полагаем нецелесообразным ограничивать возможность создания IT-аутсорсера исключительно организационно-правовой формой акционерного общества, как это сделано, например, в отношении акционерного инвестиционного фонда. Оптимально установление требования по одной из организационно-правовых форм хозяйственных обществ с установлением публичных требований в законодательстве, минимизирующих отмеченные недостатки каждой из организационно-правовых форм.**

Опыт построения правового регулирования финансового рынка показывает, что основная часть регулирования для достижения целей минимизации рисков идет не только и даже не столько через выбранную организационно-правовую форму юридического лица, а через установление публичных требований со стороны законодателя и регулятора финансового

[187] Для сравнения, АКРА Осенью 2017 года объявили о создании партнёрства с китайским агентством Golden Credit Rating International, которое входит в пятерку крупнейших на рынке КНР // https://rg.ru/2017/11/02/akra-sozdaet-partnerstvo-s-kitajskim-rejtingovym-agentstvom.html. Сотрудничество предполагает обмен базами данных, а также проведение совместных исследований. Основной акционер — государственная управляющая компания China Orient Asset Management, учрежденная Минфином КНР //https://www.vedomosti.ru/finance/articles/2017/11/02/740289-akra-partnera-kitae.
В феврале 2019 года АКРА также заключило соглашение о сотрудничестве со вторым по величине рейтинговым агентством Индии – CARE Ratings Ltd // https://tass.ru/ekonomika/6157808. АКРА представляет Россию на переговорах по созданию единого рейтингового агентства в рамках БРИКС.

рынка, а также Федеральной антимонопольной службы. Полагаем, что данная модель применима и оптимальна для универсального IT-аутсорсера, так как такими гражданско-правовыми средствами, как юридическое лицо нельзя добиться всего комплекса эффектов, важных для отдельных участников рынка (например, минимизация рисков информационной безопасности), так и всего рынка в целом (например, минимизации системного риска). Кроме того, организационно-правовая форма юридического лица как гражданско-правовое средство обеспечения интересов участников рынка (банков, их клиентов) может в большей степени раскрыться через другое гражданско-правовое средство, договор, в рамках которого могут быть установлены содержание и пределы гражданско-правовой ответственности IT-аутсорсера по отношению к участникам правоотношений на рынке IT-аутсорсинга с учетом тех возможностей и ограничений, которые составляют контур той или иной организационно-правовой формы. Более того, как верно отмечает Н.Г. Семилютина «особенностью договорных отношений на рынке финансовых услуг является то, что они развиваются с учетом и/или в рамках жестких норм публичного права …Особенностью отношений, возникающих на рынке финансовых услуг, является то, что в данной области государство осуществляет регулирование указанных отношений, активно используя различные формы и методы государственного регулирования, в том числе и властно-административный метод»[188].

В связи с этим, для создания правовой модели универсального IT-аутсорсера в настоящем разделе помимо вопроса его оптимальной организационно-правовой формы, необходимо рассмотреть и вопрос регуляторных требований. **Наиболее оптимальным полагаем путь анализа через требования, предъявляемые к финансовыми организациям и субъектам, оказывающим профессиональные услуги на финансовом рынке.**

[188] Семилютина Н.Г. Формирование правовой модели российского рынка финансовых услуг. Автореферат дисс… д.ю.н. М., 2005. С.7.

В настоящее время Закон о Банке России относит ряд организаций к финансовым, из чего следует установление дополнительного регулирования и надзора со стороны Банка России (глава X.I). Кроме того, с 1 января 2022 года Закон о Банке России был дополнен новой главой X.1-1 «Регулирование, контроль и надзор в сфере оказания профессиональных услуг на финансовом рынке». В данную главу были перемещены бюро кредитных историй, кредитные рейтинговые агентства и лица, осуществляющие актуарную деятельность, которые не привлекают и не размещают средства клиентов, но выполняют важные инфраструктурные для рынка банковских услуг задачи информационного, аналитического характера. Таким образом, они перестали быть финансовыми организациями, соответственно, оказывать финансовые услуги. Одновременно появилась и новая категория посредников на финансовом рынке - лица, оказывающие профессиональные услуги на финансовом рынке.

Очевидно, что предъявление к финансовым организациям особых требований обусловлено не организационно-правовой формой корпоративной организации, а связано именно со спецификой деятельности таких корпораций:

- все они связаны с аккумулированием значительных ликвидных ресурсов, зачастую привлекаемых не только от профессиональных предпринимателей, но и от обычных граждан-потребителей;
- они функционируют на финансовом рынке, предоставляя соответствующие финансовые услуги, предметом которых являются активы, обладающими свойствами высокой мобильности[189];
- их деятельность является высокорискованной, и поэтому такие корпорации в большей степени подвержены опасности потери устойчивости;

[189] Как отмечает Н.Г. Семилютина, «…финансовые услуги связаны с движением денежных средств. При этом речь не идет о движении денежных средств в смысле осуществления расчетов (например, оплата покупателем товара или услуг), а о трансформации их в денежный капитал» // Семилютина Н.Г. Инвестиции и рынок финансовых услуг: проблемы законодательного регулирования. Журнал российского права. 2003. № 2.

- как правило, они являются профессиональными предпринимателями - коммерческими корпоративными организации, чаще всего хозяйственными обществами.

Что касается финансовых организаций, являющихся инфраструктурными, а также новой категории субъектов, оказывающих профессиональные услуги на финансовом рынке (далее также профессиональные субъекты на финансовом рынке), то они также, как правило, осуществляют предпринимательскую деятельность. От их нормального функционирования и организации в ряде случаев может зависеть стабильное функционирование рынка финансовых услуг. Предъявление к ним особых требований в большей степени продиктовано тем, что в большинстве своем они призваны защищать права клиентов тех финансовых корпораций, которые собственно и предоставляют финансовые услуги по привлечению и размещению средств клиентов. **В случае универсального IT-аутсорсера придание ему такого статуса может быть связано с необходимостью хранения, передачи и обработки информации в соответствующих информационных системах и их компонентах, необходимые для осуществления банковских операций банков, что непосредственно связано с необходимостью обеспечения защиты прав их клиентов – физических и юридических лиц.**

Указанные свойства предопределяют наличие особенностей в правовом регулировании их деятельности, проявляющихся в установлении со стороны государства по отношению к ним особых требований:

- к созданию, прекращению и правовому положению финансовых организаций и профессиональных субъектов на финансовом рынке;
- к осуществляемой ими предпринимательской деятельности.

Можно выделить ряд общих требований, предъявляемых к ним законодательством, которые вытекают из специфики их высокорискованной финансовой деятельности и направлены на минимизацию этих рисков,

обеспечение их устойчивости и, как следствие, защиту интересов их клиентов – юридических и физических лиц.

Следует заметить, что данные требования носят публично-правовой характер и зачастую являются средствами государственного регулирования соответствующих видов предпринимательской деятельности, регламентируя при этом особенности отношений, возникающих в сферах создания, прекращения и организации деятельности финансовых организаций и профессиональных субъектов на финансовом рынке, то есть корпоративных отношений с участием указанных субъектов.

По мнению М.Г. Ионцева, характерными чертами специального правового регулирования корпораций в данных трех сферах являются: установление закрытого перечня видов деятельности; определение минимального размера уставного капитала и соотношение его денежной и неденежной частей и, наконец, установление особой компетенции специальных органов осуществлять государственную регистрацию и надзор за деятельностью соответствующих юридических лиц[190].

По нашему мнению, рассмотренных выше особых требований гораздо больше. При этом исходя из отмеченной выше группировки на требования корпоративного характера и регуляторные требования к участникам финансового рынка, в целях настоящего исследования, предполагающего создание правовой модели IT-аутсорсера с учетом необходимости минимизации различных рисков при помощи частноправовых и публично-правовых средств, можно выделить и сгруппировать их в два следующих вида:

1. Требования к финансовым организациям как к корпорациям:

- требования к организационно-правовой форме коммерческой корпоративной организации;
- особая процедура регистрации и ликвидации данных корпораций;

[190] См.: Ионцев М.Г. Акционерные общества. – 4-е изд. М., 2009. С. 45-48.

- требования к фирменному наименованию данных корпораций, к содержанию учредительных документов;
- повышенные требования к минимальному размеру уставного капитала, его составу и порядку его оплаты;
- особые требования, предъявляемые к положению учредителей, как правовому, так и финансовому;
- дополнительная или ограниченная по сравнению с корпоративным законодательством компетенция органов управления;
- ограничения прав участников (акционеров) или дополнительные права участников (акционеров) на основании норм специального, а не корпоративного законодательства;
- особенности эмиссии и/или приобретения акций (долей, паев) корпораций.

2. Требования к финансовым организациям как участникам рынка финансовых услуг:

- требования к лицензированию деятельности или ведению иного учета (например, включение в специальный реестр);
- запрет на совмещение с определенными или всеми иными видами предпринимательской деятельности;
- необходимость разработки и утверждения особых документов (например, бизнес-плана, правил страхования, инвестиционной декларации);
- особые требования к размеру и составу собственных средств (капитала) финансовой организации;
- квалификационные и иные требования к должностным лицам корпораций;
- особые требования к деловой репутации должностных лиц и учредителей финансовых организаций[191].

[191] Подробнее об этом см.: Корпоративное право: Учебный курс. В 2 т./ Отв. Ред. И.С. Шиткина. Т. 2. М., 2017 С. 779-799. (автор главы Лаутс Е.Б.).

И та, и другая группа требований определяет особенности правового положения финансовой организации, а также профессиональных субъектов на финансовом рынке по сравнению с другими организациями, имеющими общий режим в соответствии с гражданским и корпоративным законодательством. **Поскольку IT-аутсорсер в отличие от финансовых организаций очевидно финансовых услуг не оказывает, полагаем, что он может быть отнесен Законом о Банке России к субъектам, оказывающим профессиональные услуги на финансовом рынке.** Во-первых, с такими субъектами его роднит передача, обработка и хранение конфиденциальной информации, связанной с осуществлением деятельности финансовой, в том числе кредитной, страховой и др. организаций. Так, отнесение IT-аутсорсера к данной категории участников финансового рынка позволит распространить на них требования Банка России к обеспечению защиты информации при осуществлении деятельности в сфере оказания профессиональных услуг на финансовом рынке в целях противодействия осуществлению незаконных финансовых операций, обязательные для лиц, оказывающих профессиональные услуги на финансовом рынке. В соответствии со ст. 76.9-6 Закона о Банке России ЦБ РФ по согласованию с федеральным органом исполнительной власти, уполномоченным в области обеспечения безопасности, и федеральным органом исполнительной власти, уполномоченным в области противодействия техническим разведкам и технической защиты информации, устанавливает обязательные для лиц, оказывающих профессиональные услуги на финансовом рынке, требования к обеспечению защиты информации при осуществлении деятельности в сфере оказания профессиональных услуг на финансовом рынке в целях противодействия осуществлению незаконных финансовых операций, за исключением требований к обеспечению защиты информации, установленных федеральными законами и принятыми в соответствии с ними иными нормативными правовыми актами.

Согласно Положению Банка России от 17.10.2022 № 808-П[192] лица, оказывающие профессиональные услуги на финансовом рынке, должны обеспечить защиту информации, получаемой, подготавливаемой, обрабатываемой, передаваемой и хранимой лицами, оказывающими профессиональные услуги на финансовом рынке, с использованием автоматизированных систем, программного обеспечения, средств вычислительной техники, телекоммуникационного оборудования (объекты информационной инфраструктуры) в рамках: обеспечения защиты информации при управлении доступом; обеспечения защиты вычислительных сетей; контроля целостности и защищенности объектов информационной инфраструктуры; защиты от воздействия программных кодов, приводящих к нарушению штатного функционирования средства вычислительной техники (вредоносные коды); предотвращения утечек информации; управления инцидентами защиты информации; защиты среды виртуализации; защиты информации при осуществлении удаленного логического доступа с использованием мобильных (переносных) устройств.

Во-вторых, придание данного правового статуса позволит выбрать оптимальный набор дополнительных требований, предъявляемых к IT-аутсорсеру как корпорации и как к участнику финансового рынка. Для определения оптимального перечня дополнительных требований необходимо указать, какого рода требования из приведенной выше классификации применяются к профессиональным субъектам финансового рынка, за основу взяв кредитные рейтинговые агентства с учетом отмеченных выше сходств потенциального масштаба деятельности, необходимости минимизации конфликта интересов, а также обеспечения независимости от какого-либо политического и экономического влияния (системный риск).

[192] Положение Банка России от 17.10.2022 № 808-П «О требованиях к обеспечению защиты информации при осуществлении деятельности в сфере оказания профессиональных услуг на финансовом рынке в целях противодействия осуществлению незаконных финансовых операций, обязательных для лиц, оказывающих профессиональные услуги на финансовом рынке, к обеспечению бюро кредитных историй защиты информации, указанной в статье 4 Федерального закона "О кредитных историях", при ее обработке, хранении и передаче сертифицированными средствами защиты, а также к сохранности информации, полученной в процессе деятельности кредитного рейтингового агентства» // Вестник Банка России. 2022. № 62.

Основываясь на представленной выше классификации требований, согласно Закону о рейтинговых агентствах кредитные рейтинговые агентства обязаны:

- быть зарегистрированными в одной из организационно-правовых форм хозяйственного общества;
- быть включенными в реестр Банка России;
- в части необходимости разработки и утверждения особых документов представить для включения в реестр Банка России, например, документы, содержащие правила раскрытия кредитных рейтингов и других связанных с ними сообщений, включая прогнозы по кредитным рейтингам, документы, содержащие описание политики ценообразования, в том числе в отношении различных видов объектов рейтинга, документы, содержащие процедуры осуществления рейтинговых действий и др.[193];
- иметь минимальный размер собственных средств (капитала) в сумме 50 миллионов рублей (п. 2 ст. 3)[194];
- обеспечить независимость рейтинговой деятельности, в том числе от любого политического и (или) экономического влияния (п. 9 ст. 3);
- обеспечить предотвращение, выявление конфликтов интересов, управление ими и раскрытие информации о них (п. 9 ст. 3)[195];

[193] Положение Банка России от 12.09.2019 № 692-П «О требованиях к представлению в Банк России заявления о внесении сведений о хозяйственном обществе в реестр кредитных рейтинговых агентств, перечне документов, прилагаемых к указанному заявлению, порядке внесения Банком России филиала и представительства иностранного кредитного рейтингового агентства, осуществляющего в соответствии со своим личным законом рейтинговую деятельность, в реестр филиалов и представительств иностранных кредитных рейтинговых агентств, порядке ведения Банком России реестра кредитных рейтинговых агентств и составе включаемых в него сведений, порядке ведения Банком России реестра филиалов и представительств иностранных кредитных рейтинговых агентств и составе включаемых в него сведений, требованиях к порядку и форме представления кредитными рейтинговыми агентствами в Банк России уведомлений о назначении (избрании) на должность или об освобождении от должности (прекращении полномочий) должностных лиц (органов управления) кредитного рейтингового агентства, а также порядке доступа заинтересованных лиц к информации, содержащейся в реестре кредитных рейтинговых агентств»

[194] Методика определяется Банком России согласно Указанию Банка России от 07.12.2015 № 3887-У «О методике определения размера собственных средств (капитала) кредитного рейтингового агентства» // Вестник Банка России. 2015. № 122 // Вестник Банка России. 2020. № 76.

[195] Данное требования достигается как созданием Совета директоров соответствующими полномочиями, так и разработкой и выполнением требований документов, содержащих правила и процедуры предотвращения, выявления конфликтов интересов, их раскрытия и управления ими в целях обеспечения независимости кредитных рейтингов и рейтинговых аналитиков от учредителей (акционеров, участников) и органов

- не совмещать рейтинговую деятельность с иными видами деятельности, за исключением деятельности по оказанию некоторых дополнительных услуг, определенных Законом о рейтинговых агентствах (п. 3 ст. 3);
- закрепить определенную структуру органов управления (Совет директоров), требования к их членам и компетенцию (ст. 8);
- выполнять особые требования, предъявляемые к правовому положению и деловой репутации учредителей, владеющих прямо или косвенно более 10% акций (долей) уставного капитала, влекущие ограничения их прав при несоблюдении данных требований (ст. 6);
- квалификационные и требования к деловой репутации должностных лиц (ст. 7);
- дополнительные требования к раскрытию информации (ст. 13).

Полагаем, что все указанные требования целесообразно закрепить при создании правовой модели универсального IT-аутсорсера, так как они гармонично вписываются в его функционал и позволяют частично минимизировать риски потери финансовой устойчивости за счет требований к минимальному размеру собственных средств (капитала), запрета на совмещение с иными видами деятельности и др., правовые риски в части регуляторных требований и контроля из их исполнением, репутационные риски, в том числе возникновение конфликта интересов путем закрепления определенной структуры органов управления (Совет директоров), требований к их членам и компетенции, а также операционные риски с учетом необходимости разработки и исполнения внутренних документов, позволяющих уменьшить риски ошибок и сбоев.

Основываясь на предложенной выше классификации дополнительных требований к финансовым организациям и профессиональным субъектам финансового рынка в части

управления заявителя, а также от подразделений и работников, ответственных за рекламу, привлечение клиентов и заключение договоров об осуществлении рейтинговых действий.

корпоративного блока, полагаем целесообразным также установление требований к фирменному наименованию данных субъектов в части обязательного указания на универсального IT-аутсорсера, а также к содержанию его учредительных документов, что было рассмотрено выше, в частности, по структуре органов управления, их компетенции, ограничении прав акционеров (участников) на выход, ограничении доли участия, раскрытии информации и т.д., если универсальный IT-аутсорсер будет иметь возможность создания в организационно-правовой форме ООО.

2.1. Рекомендации по оптимальной модели корпоративного управления компании-аутсорсера.

Как было отмечено, в случае создания универсального IT-аутсорсера как ПАО, в любом случае необходимо создание Совета директоров. В случае же создания IT-аутсорсера как неПАО или ООО полагаем целесообразным установление требований по обязательному формированию Совета директоров, который, например, в кредитных организациях, традиционно отвечает за избежание конфликта интересов, контроль за уровнем рисков, а также организацию внутреннего контроля. Кроме того, в целях минимизации конфликта интересов целесообразно закрепить требования к составу Совета директоров в кредитных рейтинговых агентствах, где как минимум одна треть, но не менее двух членов совета директоров (наблюдательного совета) должны быть независимыми членами, не осуществляющими рейтинговых действий, рекламы услуг кредитного рейтингового агентства и иных действий по привлечению клиентов (ст. 8 Закона о рейтинговых агентствах). Данное решение может быть воспринято с преломлением на функции IT-аутсорсера.

По аналогии с кредитными организациями и с учетом создания IT-аутсорсера как хозяйственного общества, в особенности ПАО, полагаем целесообразным применение близких по смыслу требований к системе внутреннего контроля в IT-аутсорсере:

1. Закрепление в Уставе IT-аутсорсера сведений о системе органов внутреннего контроля, порядке их образования и полномочиях;

2. Организационная структура IT-аутсорсера в части распределения полномочий между членами совета директоров (наблюдательного совета) коллегиального исполнительного органа, определения полномочий единоличного исполнительного органа, полномочий, подотчетности и ответственности всех подразделений IT-аутсорсера, служащих должна соответствовать характеру и масштабу осуществляемой деятельности, уровню и сочетанию принимаемых рисков;

3. Внутренний контроль должны осуществлять в соответствии с полномочиями, определенными учредительными и внутренними документами IT-аутсорсера: органы управления IT-аутсорсера при обязательном формировании совета директоров вне зависимости от организационно-правовой формы хозяйственного общества; ревизионная комиссия (ревизор); главный бухгалтер; подразделения и служащие, осуществляющие внутренний контроль в соответствии с полномочиями, определяемыми внутренними документами IT-аутсорсера, включая службу внутреннего аудита и службу внутреннего контроля.

Рекомендации по изменению модели корпоративного управления в кредитных организациях-клиентах IT-аутсорсера

Как было отмечено, в отношении кредитных организаций действуют специальные требования в части компетенции Совета директоров (ст.11.1-1 Закона о банках и банковской деятельности), в том числе в части управления рисками кредитной организации и предотвращения конфликта интересов, утверждения плана восстановления финансовой устойчивости в случае существенного ухудшения финансового состояния кредитной организации, плана действий, направленных на обеспечение непрерывности деятельности и (или) восстановление деятельности кредитной организации в случае возникновения нестандартных и чрезвычайных ситуаций, утверждения плана работы службы внутреннего аудита кредитной организации и др.

Следуя зарубежному опыту, целесообразно отдельно закрепить за Советом директоров кредитной организации компетенцию по утверждению стратегии управления кредитной организации, связанными с IT-аутсорсингом, а также утверждение порядка применения методик управления рисками с учетом рисков IT-аутсорсинга (ст. 36 Руководства EBA по аутсорсингу), выявлению, оценке и урегулированию конфликта интересов в отношении соглашений об аутсорсинге (ст. 45 Руководства EBA по аутсорсингу), по утверждению планов по обеспечению непрерывности деятельности в отношении переданных на аутсорсинг критических и существенных функций (ст. 48 Руководства EBA по аутсорсингу), по утверждению планов проведения службой внутреннего аудита независимой проверки аутсорсинговой деятельности и соглашений об аутсорсинге критических и существенных функций (ст. 50 Руководства EBA по аутсорсингу). Близкие по смыслу требования к функциям Совета директоров в отношении передачи функций на аутсорсинг содержатся в Директиве Резервного банка Индии[196], Заявлении надзорного органа 2/21 «SS2/21 Аутсорсинг и управление рисками третьих сторон» Великобритании[197], в Пруденциальном стандарте Австралийской администрации регулирования (APRA)[198], в Руководящих принципах регулятора Сингапура[199].

В Таиланде Совет директоров финансовых организаций также несет ответственность за формулирование политики аутсорсинга, которая охватывает факторы, учитываемые при аутсорсинге. При этом Политика аутсорсинга в финансовой организации должна охватывать как минимум следующие ключевые вопросы: 1) объем и характер передаваемых на

---

[196] Reserve Bank of India (Outsourcing of Information Technology Services) Directions, 2023 https://rbidocs.rbi.org.in/rdocs/notification/PDFs/102MDITSERVICES56B33FD530B1433187D75CB7C06C8F70.PDF

[197] Supervisory Statement | SS2/21 Outsourcing and third party risk management March 2021 https://www.bankofengland.co.uk/-/media/boe/files/prudential-regulation/supervisory-statement/2021/ss221-march-21.pdf

[198] Prudential Standard CPS 231 Outsourcing July 2017 https://www.apra.gov.au/sites/default/files/Prudential-Standard-CPS-231-Outsourcing-%28July-2017%29.pdf

[199] Guidelines on Outsourcing. Monetary Authority of Singapore. 27 July 2016. https://www.mas.gov.sg/-/media/mas/regulations-and-financial-stability/regulatory-and-supervisory-framework/risk-management/outsourcing-guidelines_jul-2016-revised-on-5-oct-2018.pdf

аутсорсинг услуг; 2) процесс выбора поставщика услуг, в том числе его минимальную квалификацию и описание процесса найма; 3) система оценки рисков и управления рисками; 4) внутренний контроль; 5) эффективная система информационной безопасности финансовых организаций и клиентов; 6) план непрерывности бизнеса финансовых организаций в случае, если аутсорсинговые компании не могут предоставлять непрерывные услуги; 7) управление изменениями, включая случай прекращения оказания услуг поставщиком; 8) объем ответственности подразделения, ответственного за принятие решения об аутсорсинге; 9) политика поддержки потенциального воздействия такого, как сокращение или увольнение персонала или сопротивление со стороны затронутого персонала; 10) регулярный анализ эффективности и целесообразности политики[200]. **Близкие по смыслу требования к внутренней политике IT-аутсорсинга могут быть закреплены и в отношении российских кредитных организаций нормативными актами Банка России.**

По нашему мнению, в кредитных организациях также целесообразно дополнить требования в части организации системы внутреннего контроля.

Если обратиться к зарубежному опыту, то согласно п. с ст. 38 Руководства EBA по аутсорсингу финансовая организация обязана создать подразделение по аутсорсингу или назначить ответственного сотрудника, который будет непосредственно подотчетен руководящему органу (например, ключевому должностному лицу, отвечающему за соответствующие контрольные функции). В сферу ответственности назначенного сотрудника или подразделения должно входить управление рисками, связанными с соглашениями об аутсорсинге, надзор за ними в рамках системы внутреннего контроля организации, а также контроль за документированием аутсорсинга. Так, например, в Германии, которая также применяет данное Руководство

[200] Уведомление Банка Таиланда № FPG 8/2557 «Положения об аутсорсинге финансовых организаций» // Notification of the Bank of Thailand No. FPG 8/ 2557 Re: Regulations on Outsourcing of Financial Institutions https://www.bot.or.th/content/dam/bot/fipcs/documents/FPG/2558/EngPDF/25580002.pdf

ЕВА по аутсорсингу в финансовых организациях, существует распространенная практика (в 3 из 4 компаний) создания отдельного сотрудника по аутсорсингу, который напрямую подчиняется высшему руководству и осуществляет, развивает, контролирует и документирует управление аутсорсингом. Чуть менее 20 процентов финансовых организаций еще не соответствуют этому требованию[201]. В России согласно Положению Банка России от 16.12.2003 № 242-П «Об организации внутреннего контроля в кредитных организациях и банковских группах»[202] (далее – Положение о внутреннем контроле) к одной из функций службы внутреннего контроля (далее также – СВК) относится анализ экономической целесообразности заключения кредитной организацией договоров с юридическими лицами и индивидуальными предпринимателями на оказание услуг и (или) выполнение работ, обеспечивающих осуществление кредитной организацией банковских операций (аутсорсинг) (п. 4(1)1). **Полагаем, что при изменении архитектуры рынка IT-аутсорсинга с появлением универсального IT-аутсорсера, функции СВК должны быть расширены в части анализа не только экономической целесообразности, но и оценке комплаенс-рисков при заключении банками договоров с IT-аутсорсером. Кроме того, следуя зарубежному опыту, целесообразно выделение такого сотрудника в рамках службы управления рисками либо службы внутреннего контроля с близким статусом к ответственному сотруднику (структурному подразделению) по противодействию легализации (отмыванию) доходов, полученных преступным путем, и финансированию терроризма, что способствовало бы минимизации целого ряда рисков как при создании универсального IT-аутсорсера, так и при продолжении существования децентрализованного рынка IT-аутсорсинга в финансовой сфере.**

[201] См.: Daniel Wildhirt «MaRisk-Novelle 2021 – Readiness-Analyse (AT 9)» // https://www.pwc.de/de/finanzdienstleistungen/sechste-marisk-novelle-erhoehte-anforderungen-fuer-auslagerungen.html
[202] Вестник Банка России. 2004. № 7.

2.2. Предложения по возможным вариантам формирования уставного капитала компании-аутсорсера:

2.2.1. Предложения по возможным вариантам формирования уставного капитала компании-аутсорсера с участием средств Банка России (например, на момент организации лица с последующей постепенной продажей долей в капитале).

Возможности участия Банка России в уставных капиталах организаций ограничены его особым правовым статусом и вытекающими из него требованиями Федерального закона от 10.07.2002 № 86-ФЗ «О Центральном банке Российской Федерации (Банке России)»[203] (далее - Закон о Банке России).

Согласно ст. 8 Закона о Банке России он не вправе участвовать в капиталах кредитных организаций, если иное не установлено федеральными законами. При этом законодатель, очевидно, расширительно трактует данную норму. Так, в ст. 189.57-1 Федерального закона от 26.10.2002 № 127-ФЗ «О несостоятельности (банкротстве)» (далее – Закон о банкротстве) отдельно указывается, что ст. 8 Закона о Банке России не распространяется на участие в капитале общества с ограниченной ответственностью «Управляющая компания Фонда консолидации банковского сектора» (далее – ООО УК «ФКБС»). Тем не менее, данная организация не является кредитной организацией и при буквальном толковании требования п. 1 ст. 8 Закона о Банке России на нее распространяться были не должны. Тем не менее, согласно ст. 76.10 Закона о Банке России в целях осуществления мероприятий по финансовому оздоровлению кредитных организаций, мероприятий по предупреждению банкротства страховых организаций или негосударственных пенсионных фондов Банк России вправе в качестве единственного участника учредить общество с ограниченной ответственностью «Управляющая компания Фонда консолидации банковского сектора», действующее в

[203] СЗ РФ. 2002, N 28, ст. 2790.

соответствии с Федеральным законом от 29 ноября 2001 года № 156-ФЗ «Об инвестиционных фондах»[204], Федеральным законом от 22 апреля 1996 года № 39-ФЗ «О рынке ценных бумаг»[205] с особенностями, установленными Законом о Банке России и Законом о банкротстве.

Действие п. 1 ст. 8 Закона о Банке России также не распространяется на участие Банка России в капитале Сберегательного банка Российской Федерации.

Статьей 8 Закона о Банке России установлено общее правило, согласно которому Банк России не вправе участвовать в капиталах или являться членом иных коммерческих или некоммерческих организаций, если они не обеспечивают деятельность Банка России, его учреждений, организаций и служащих, за исключением случаев, установленных федеральными законами.

Таким образом, данная норма может стать существенной препоной в отношении участия Банка России в уставном капитале универсального IT-аутсорсера. Так, данный вопрос поднимался депутатами при рассмотрении, например, законопроекта № 1056530-7 «О внесении изменений в отдельные законодательные акты Российской Федерации в части создания автоматизированной информационной системы страхования»[206], которые высказывали опасение о принадлежности 100% акций оператора АИС Страхование Банку России как регулятору на страховом рынке, поскольку это создает предмет для формирования дискреционных полномочий и коррупционной составляющей[207]. В итоге законопроект был отклонен.

В связи с этим полагаем, что без внесения изменений в федеральное законодательство или принятия отдельного федерального закона о статусе универсального IT-аутсорсера с установлением права Банка России учредить такое юридическое лицо или стать одним из его учредителей (участников)

[204] СЗ РФ. 2002, N 43, ст. 4190.
[205] СЗ РФ. 1996, ст. 1918.
[206] https://sozd.duma.gov.ru/
[207] См. подробнее: Чуб А. Правовые инициативы страховщиков // Современные страховые технологии. 2021. N 3. С. 70 - 77.

данная модель нереализуема, так как будет противоречить Закону о Банке России.

2.2.2. Предложения по возможным вариантам формирования уставного капитала компании-аутсорсера с участием средств кредитных организаций.

Учредителями АО и ООО могут быть граждане и юридические лица (п. 1 ст. 10 Закона об АО; п.1 ст. 7 Закона об ООО). Таким образом, корпоративное законодательство базово не содержит каких-то ограничений в части того, может ли быть акционером (участником) хозяйственного общества другое хозяйственное общество (кредитные организации могут быть только хозяйственными обществами). Единственное ограничение существует для АО, которое в отличие от ООО не может иметь в качестве единственного учредителя (акционера) другое хозяйственное общество.

Тем не менее, банковское законодательство содержит ряд ограничений для кредитных организаций, если они планируют стать учредителями (участниками) других юридических лиц. Банковским законодательством (ст. 62 Закона о Банке России) предусмотрен такой обязательный норматив, установленный Банком России для каждой кредитной организации, как норматив использования собственных средств (капитала) банка для приобретения акций (долей) других юридических лиц (Н12). Он регулирует совокупный риск вложений банка в акции (доли) других юридических лиц и определяет максимальное отношение сумм, инвестируемых банком на приобретение акций (долей) других юридических лиц, к собственным средствам (капиталу) банка. Максимальный размер данного норматива установлен на уровне 25% от собственных средств банка[208]. Таким образом, банк не имеет права вкладывать больше, чем 25% от собственных средств (капитала), в приобретение акций (долей) любой другой корпорации.

[208] Для банков с универсальной лицензией данный норматив регулируется главой 9 Инструкции Банка России от 29.11.2019 N 199-И «Об обязательных нормативах и надбавках к нормативам достаточности капитала банков с универсальной лицензией» // Вестник Банка России. 2020. № 11-12.

Кроме того, при наличии значительной доли участия кредитной организации в уставном капитале универсального IT-аутсорсера существует вероятность признания данного вертикально интегрированного объединения банковской группой. Согласно ст. 4 Закона о банках и банковской деятельности банковской группой признается не являющееся юридическим лицом объединение юридических лиц, в котором одно юридическое лицо или несколько юридических лиц (далее - участники банковской группы) находятся под контролем либо значительным влиянием одной кредитной организации.

Основанием возникновения холдинговых отношений является установление контроля либо значительного влияния головной кредитной организации на юридические лица (в том числе кредитные организации), входящие в состав данного предпринимательского объединения.

Для определения оснований возникновения контроля и существенного влияния Закон о банках и банковской деятельности фактически отсылает к международным стандартам финансовой отчетности. Так, согласно ст. 4 Закона о банках и банковской деятельности контроль и значительное влияние для определения участников банковской группы (банковского холдинга) и составления отчетности, установленной Законом о банках и банковской деятельности, определяются в соответствии с Международными стандартами финансовой отчетности, признанными на территории Российской Федерации[209] (далее – МСФО).

Согласно МСФО для установления контроля и значительного влияния используются оценочные критерии, направленные на выявление сущности отношений, в которых состоят компании. При этом, если одной компании принадлежит более 20% акций (долей) в уставном капитале другой компании, то наличие значительного влияния презюмируется и является достаточным для

[209] «Международный стандарт финансовой отчетности (IFRS) 10 «Консолидированная финансовая отчетность» (введен в действие на территории Российской Федерации Приказом Минфина России от 28.12.2015 N 217н); «Международный стандарт финансовой отчетности (IAS) 28 «Инвестиции в ассоциированные организации и совместные предприятия» (введен в действие на территории Российской Федерации приказом Минфина России от 28.12.2015 N 217н) // http://www.minfin.ru/

вывода о наличии контроля. Тем не менее, для вывода о наличии контроля необходимо по существу также установить возможность направлять предпринимательскую деятельность компании, а для вывода о наличии значительного влияния – возможность участвовать в принятии решений по ее финансовой и операционной политике.

Таким образом, при установлении контроля или значительного влияния и признания такого объединения банковской группой возникнут определенные банковским законодательством регуляторные и надзорные последствия, которые сводятся к обязанности уведомления об образовании банковской группы, необходимости подготовки и сдачи консолидированной отчетности, выполнении обязательных нормативов, установленных для банковских групп, а также особенностям осуществления банковского надзора за банковскими группами на консолидированной основе, в том числе путем формирования надзорных групп.

В связи с проанализированными требованиями полагаем важным для создаваемого универсального IT-аутсорсера установление ограничений на предельную долю участия кредитных организаций в его уставном капитале. Для сравнения можно привести схожие требования применительно к рейтинговым агентствам. Так, согласно ст. 6 Закона о рейтинговых агентствах доля кредитной организации, участников банковской группы, участников банковского холдинга, некредитной финансовой организации или участника страховой группы, бюро кредитных историй, кредитного рейтингового агентства в уставном капитале кредитного рейтингового агентства не может превышать 20%. При нарушении данных требований Банк России в установленном им порядке направляет указанным лицам предписание с требованием об устранении нарушений. В случае неисполнения предписания указанными лицами Банк России вправе требовать в судебном порядке уменьшения их участия в уставном капитале до размера, не превышающего 20%. При этом такие «нарушители» вправе распоряжаться количеством голосов, не превышающем 20% голосов, приходящихся на голосующие акции

(доли), составляющие уставный капитал кредитного рейтингового агентства. При этом остальные акции (доли), принадлежащие указанным лицам, при определении кворума общего собрания акционеров (участников) кредитного рейтингового агентства и при голосовании по вопросам повестки дня общего собрания акционеров (участников) кредитного рейтингового агентства не учитываются. Более того, Банк России вправе обжаловать в судебном порядке решения общего собрания акционеров (участников) кредитного рейтингового агентства, принятые с нарушением обозначенных требований, и сделки, совершенные во исполнение указанных решений, если участие в голосовании такими акциями (долями) с превышением допустимого размера, повлияло на решения, принятые общим собранием акционеров (участников) кредитного рейтингового агентства.

Как было рассмотрено ранее, в связи с анализом различных организационно-правовых форм, соблюдение такого паритета позволит частично минимизировать риск возникновения конфликта интересов, избежав значительного влияния мажоритарных акционеров (участников) на принимаемых IT-аутсорсером решения. В свете же настоящего раздела можно сделать дополнительный вывод о том, что установление таких ограничений для кредитных организаций позволит избежать создания банковской группы, предпринимательского объединения, которое не является оптимальным для цели создания IT-аутсорсера и повлечет дополнительную надзорную нагрузку, по существу не обусловленную спецификой и задачами его деятельности.

2.2.3. Предложения по возможным вариантам формирования уставного капитала компании-аутсорсера с участием средств разработчиков банковского ПО или иных субъектов рынка IT- аутсорсинга.

Традиционно субъекты рынка IT-аутсорсинга создаются в различных организационно-правовых формах хозяйственных обществ и, соответственно, без каких-либо ограничений могут стать акционерами (участниками, пайщиками, членами) универсального IT-аутсорсера.

Наиболее важный для настоящего раздела вопрос состоит в том, какое имущество субъекты рынка IT-аутсорсинга могут внести в уставный капитал универсального IT-аутсорсера, если он создается в разных организационно-правовых формах. Данный анализ также является важным также и для вывода об оптимальной организационно-правовой форме самого IT-аутсорсера, если он будет создаваться на основе участия, в том числе субъектов соответствующего рынка, потенциально заинтересованных во внесении в уставный капитал и имущество универсального IT-аутсорсера интеллектуальной собственности.

Так, уставный капитал АО составляется из номинальной стоимости акций общества, приобретенных акционерами (ст. 25 Закона об АО). Таким образом, уставный капитал АО формируется путем первичной эмиссии акций (первый выпуск после государственной регистрации), то есть после реализации выпущенных акций первым владельцам. При этом решение об учреждении общества, утверждении его устава и утверждении денежной оценки ценных бумаг, других вещей или имущественных прав либо иных прав, имеющих денежную оценку, вносимых учредителем в оплату акций общества, принимается учредителями единогласно (п. 3 ст. 9 Закона об АО).

Если иное не установлено уставом общества, оплата акций при их приобретении осуществляется деньгами (п. 4 ст. 72 Закона об АО). Устав общества может содержать ограничения на виды имущества, которым могут быть оплачены акции общества (п. 2 ст. 34 Закона об АО). В любом случае согласно ст. 66.2 ГК РФ и ст. 26 Закона об АО минимальный размер уставного капитала (100.000 руб. для ПАО и 10.000 руб. для неПАО) должен быть оплачен деньгами.

При внесении в уставный капитал АО не денежных средств, а иного имущества акционер, осуществивший такую оплату, и независимый оценщик в случае недостаточности имущества общества солидарно несут субсидиарную ответственность по его обязательствам в пределах суммы, на которую завышена оценка имущества, внесенного в уставный капитал, в

течение пяти лет с момента государственной регистрации общества или внесения в устав общества соответствующих изменений (п. 3 ст. 66.2 ГК РФ).

Таким образом, при принятии учредителями решения о принятии интеллектуальной собственности в качестве вклада в уставный капитал акционерных обществ, требуется в обязательном порядке ее оценка независимым оценщиком. При этом согласно п. 3 ст. 34 Закона об АО при учреждении АО денежная оценка имущества, вносимого в оплату акций общества, производится по соглашению между учредителями. В дальнейшем такую стоимость утверждает Совет директоров или собрание акционеров, если по уставу функции Совета директоров переданы общему собранию (для неПАО). В любом случае величина денежной оценки имущества, произведенной учредителями общества и Советом директоров АО, не может быть выше величины оценки, произведенной оценщиком[210].

Схожим является порядок внесения неденежных средств в уставный капитал ООО, который составляется из номинальной стоимости долей его участников (п. 1 ст. 14 Закона об ООО). Кроме того, как было отмечено, уставом ООО могут быть ограничены как максимальный размер доли участника ООО, так и возможность изменения соотношения долей участников общества (п. 3 ст. 14 Закона об ООО). Оплата долей в уставном капитале общества может осуществляться деньгами, ценными бумагами, другими вещами или имущественными правами либо иными имеющими денежную оценку правами (п. 1 ст. 15 Закона об ООО). Как и в АО уставом ООО могут быть установлены виды имущества, которое не может быть внесено для оплаты долей в уставном капитале общества. Аналогично, как и в случае с АО, оплатить имуществом долю в уставном капитале общества возможно только сверх минимально установленного размера уставного капитала общества (10

[210] Как отмечает Банк России, величина денежной оценки имущества, произведенной учредителями общества или советом директоров (наблюдательным советом) общества, не может быть выше величины оценки, произведенной оценщиком без учета НДС. // п. 1.9. Информации Банка России «Перечень часто выявляемых нарушений и типичных ошибок». Документ опубликован не был. СПС «КонсультантПлюс».

000 руб.). Согласно ст. 66.2 ГК РФ и ст. 14 Закона об ООО минимальный размер уставного капитала должен быть оплачен деньгами.

Независимый оценщик привлекается для определения стоимости имущества, если номинальная стоимость или увеличение номинальной стоимости доли участника ООО в уставном капитале общества, оплачиваемой неденежными средствами, составляет более чем 20.000 рублей (п. 2 ст. 15 Закона об ООО). Денежная оценка имущества, вносимого для оплаты долей в уставном капитале общества, утверждается решением общего собрания участников общества, принимаемым всеми участниками общества единогласно (п. 2 ст. 15 Закона об ООО). При оплате долей в уставном капитале ООО не денежными средствами, а иным имуществом участники общества и независимый оценщик в случае недостаточности имущества общества солидарно несут субсидиарную ответственность по его обязательствам в пределах суммы, на которую завышена оценка имущества, внесенного в уставный капитал, в течение пяти лет с момента государственной регистрации общества или внесения в устав общества соответствующих изменений.

Согласно ст. 66.1 ГК РФ вкладом участника хозяйственного товарищества или общества в его имущество могут быть в числе прочего имущества подлежащие денежной оценке исключительные, иные интеллектуальные права и права по лицензионным договорам, если иное не установлено законом. Например, нельзя передать право авторства, право на фирменное наименование (п. 1 ст. 1265, п.2 ст. 1474 ГК РФ).

В соответствии с п. 45 Постановления Пленума Верховного Суда РФ от 23.04.2019 № 10 «О применении части четвертой Гражданского кодекса Российской Федерации»[211] в случае внесения подлежащего денежной оценке исключительного права, иного интеллектуального права (например, права на получение патента) или права по лицензионному договору в качестве вклада в

[211] Бюллетень Верховного Суда РФ, N 7, июль, 2019.

уставный (складочный) капитал хозяйственного товарищества или общества при наличии указания об этом в решении о создании (решении о внесении имущества в уставный (складочный) капитал или договоре об учреждении (создании) товарищества или общества), а также при наличии в таком решении всех существенных условий, подлежащих включению, соответственно, в договор об отчуждении исключительного права или в лицензионный договор, заключения отдельного договора об отчуждении исключительного права или лицензионного договора, отвечающего требованиям, установленным п. 1 ст. 1233 ГК РФ, не требуется. В этом случае государственная регистрация отчуждения исключительного права на подлежащие государственной регистрации результат интеллектуальной деятельности, средство индивидуализации, а равно и предоставление права использования таких результата, средства может осуществляться и по заявлению учредителя при условии представления (в соответствующей части) решения о создании товарищества или общества.

Таким образом, в любом случае даже при понимании безвозмездности передачи исключительного права необходимо предусматривать все существенные условия договора об отчуждении исключительного права, в том числе предусмотренное п. 3 ст. 1234 ГК РФ о размере вознаграждения или порядке его определения, в отсутствие которого договор считается незаключенным. Более того, законодательство фактически не регламентирует порядок передачи имущества при оплате долей в уставном капитале, а также не устанавливает требований к документальному оформлению такой передачи. Но на практике имущество передается, как правило, по акту приема-передачи.

Также необходимо отметить, что гражданское и корпоративное законодательство предусматривают добровольное и обязательное внесение вкладов в имущество хозяйственного общества. Как верно отмечает И.С. Шиткина, «в сравнении с вкладом в уставный капитал вклад в имущество обладает рядом неоспоримых преимуществ. Так, при внесении вклада в

имущество не требуется проведение корпоративных процедур, связанных с увеличением уставного капитала. Не требуется и привлечения независимого оценщика для оценки вносимого неденежного вклада, что не только экономит организационные и материальные затраты общества на осуществление независимой оценки и снижает риски солидарной ответственности участников и оценщика, которую они субсидиарно несут в случае завышения оценки при внесении имущественных вкладов в уставный капитал (п. 3 ст. 66.2 ГК РФ), но и позволяет достаточно гибко организовать движение имущества и финансовых потоков, что особенно актуально для групп компаний (холдингов)»[212]. Отмечаются также преимущества с точки зрения антимонопольного и налогового законодательства.

Внести вклад в добровольном порядке в любое время могут акционеры как ПАО, так и неПАО. Согласно ст. 32.2 Закона об АО акционеры на основании договора с обществом имеют право в целях финансирования и поддержания деятельности общества в любое время вносить в имущество общества безвозмездные вклады в денежной или иной форме, которые не увеличивают уставный капитал общества и не изменяют номинальную стоимость акций. При этом в неПАО уставом могут быть предусмотрены максимальная стоимость вкладов в имущество неПАО, вносимых всеми или определенными акционерами, и иные ограничения, связанные с внесением вкладов в имущество непубличного общества, а также может быть возложена обязанность по внесению вкладов в имущество общества, порядок, основания и условия такого внесения.

В ООО участники также обязаны, если это предусмотрено уставом, по решению общего собрания участников общества вносить вклады в имущество общества. Такая обязанность участников общества может быть предусмотрена уставом общества при учреждении общества или путем внесения в устав общества изменений по решению общего собрания участников общества,

[212] Шиткина И. Вклады в имущество хозяйственного общества: вопросы квалификации и практического применения // Хозяйство и право. 2017. N 10. С. 22 - 41.

принятому всеми участниками общества единогласно. При этом вклады в имущество ООО вносятся всеми участниками пропорционально их долям в уставном капитале общества, если иной порядок определения размеров вкладов в имущество общества не предусмотрен уставом общества (ст. 27 Закона об ООО).

В производственном кооперативе имущество образуется за счет паевых взносов членов кооператива, предусмотренных его уставом, прибыли от собственной деятельности, кредитов, имущества, переданного в дар физическими и юридическими лицами, иных допускаемых законодательством источников (ст. 9 Закона о производственных кооперативах). Имущество, находящееся в собственности кооператива, делится на паи его членов в соответствии с уставом кооператива.

Пай члена кооператива состоит из паевого взноса члена кооператива и соответствующей части чистых активов кооператива (за исключением неделимого фонда) (ст. 9 Закон о производственных кооперативах). При этом паевым взносом члена кооператива могут быть деньги, ценные бумаги, иное имущество, в том числе и имущественные права, а также иные объекты гражданских прав (п. 2 ст. 9 Закон о ПК). Уставом кооператива может быть установлено, что определенная часть принадлежащего кооперативу имущества составляет неделимый фонд кооператива, используемый в целях, определяемых уставом кооператива. Имущество, составляющее неделимый фонд кооператива, не включается в паи членов кооператива. Таким образом, внесение в паевой фонд кооператива интеллектуальной собственности также возможно.

Если IT-аутсорсер будет образован в организационно-правовой форме ассоциации (союза), то его члены также могут передавать ему различное имущество, в том числе неденежное. Согласно ст. 26 Закона о некоммерческих организациях источниками формирования имущества некоммерческой организации в денежной и иных формах являются регулярные и единовременные поступления от учредителей (участников, членов);

добровольные имущественные взносы и пожертвования; выручка от реализации товаров, работ, услуг; дивиденды (доходы, проценты), получаемые по акциям, облигациям, другим ценным бумагам и вкладам; доходы, получаемые от собственности некоммерческой организации. Имущество, которое передано ассоциации или союзу его учредителями (участниками), является собственностью самого объединения (ассоциации и союза). Такой же режим установлен законом и в отношении имущества, приобретенного ассоциацией (союзом) по иным основаниям (п. 3 ст. 213 ГК, п. 1 ст. 24 Закона о некоммерческих организациях). Таким образом, запрета на передачу ассоциации (союзу) имущества, в том числе интеллектуальной собственности, в законодательстве нет. Тем не менее, как было отмечено, в случае, если IT-аутсосер будет создан как ассоциация (союз), то смысл для разработчиков банковского ПО и иных субъектов рынка IT- аутсорсинга становиться его участниками практически отсутствует, так как при передаче ему имущества они не будут пользоваться его услугами.

В заключение анализа участия разработчиков банковского ПО или иных субъектов рынка IT- аутсорсинга в капитале универсального IT-аутсорсера необходимо отметить, что такое участие является оптимальным также и по причине предлагаемых законодательных новелл в области IT-аутсорсинга. Согласно законопроекту «О внесении изменений в отдельные законодательные акты Российской Федерации» ст. 2 Федерального закона от 27.07.2006 № 149-ФЗ «Об информации, информационных технологиях и о защите информации»[213] дополняется пунктом 23, согласно которому поставщик услуг аутсорсинга информационных технологий и облачных услуг – это лицо, являющееся ***владельцем*** *(выделено нами – Е.Л. и А.Б.)* информационных систем и их компонентов, в частности облачных и файловых хранилищ, серверов, иных устройств и систем сбора, хранения и обработки информации, предоставляющее услуги по размещению, хранению и иной

[213] СЗ РФ. 2006, N 31 (1 ч.), ст. 3448.

обработке сведений в соответствующих информационных системах и их компонентах. **При внесении в уставный капитал и имущество IT-аутсорсера имущества, в том числе интеллектуальной собственности, универсальный IT-аутсорсер становится ее владельцем, что снимает риск оказания им соответствующих услуг на посреднической основе с привлечением лиц, не соответствующих требованиям к поставщикам услуг аутсорсинга информационных технологий и облачных услуг, определенных законопроектом.**

2.2.4. Предложения по возможным вариантам формирования уставного капитала компании-аутсорсера с участием средств союзов и ассоциаций.

В законодательстве России не существует запрета на участие ассоциаций (союзов) в уставных капиталах других юридических лиц, если это не противоречит их уставным целям.

Для рассматриваемой модели универсального IT-аутсорсера, исходя из намеченных выше направлений оптимального субъектного состава его участников (акционеров) такими ассоциациями могут стать ассоциации кредитных организаций, а также разработчиков банковского ПО и иных субъектов рынка IT- аутсорсинга.

Для ассоциаций (союзов) кредитных организаций банковское законодательство предусматривает помимо общих гражданско-правовых норм специальное регулирование. Согласно ст. 3 Закона о банках и банковской деятельности кредитные организации могут создавать союзы и ассоциации, не преследующие цели извлечения прибыли, для защиты и представления интересов своих членов, координации их деятельности, развития межрегиональных и международных связей, удовлетворения научных, информационных и профессиональных интересов, выработки рекомендаций по осуществлению банковской деятельности и решению иных совместных задач кредитных организаций. Союзам и ассоциациям кредитных организаций запрещается осуществление банковских операций. Двумя крупнейшими

банковскими ассоциациями, объединяющими всех участников рынка банковских услуг, являются Ассоциация банков России и Ассоциация российских банков.

В IT-сфере также функционируют ассоциации (союзы), объединяющие участников данной отрасли. Так, членами одной из крупнейших является «Ассоциация предприятий компьютерных и информационных технологий» (АПКИТ), которая объединяет отечественные и мировые компании в области разработки и внедрения программного обеспечения, дистрибуции, системной интеграции, сервисных услуг, производства компьютеров и оборудования, интернета, а также нишевые ассоциации: Ассоциация защиты информации АЗИ, Ассоциация поставщиков программных продуктов НП ППП, АРПП «Отечественный софт», НП РУССОФТ, Ассоциация Предприятий в сфере Радиоэлектроники, IT, Цифровых Инноваций и Инжиниринга, IT-кластер Сибири. Ассоциация позиционирует себя как ключевого участника во всей повестке развития цифровой экономики, обсуждения и правке новых программно-стратегических документов отрасли в РФ, которые нацелены на качественные изменения, формирования консолидированной позиции игроков рынка по ключевым вопросам и др.[214].

Следует отметить, что до реформы гражданского законодательства участие союзов (ассоциаций) в предпринимательской деятельности могло осуществляться исключительно через участие в хозяйственных обществах. Поэтому в целом можно сделать вывод о том, что участие банковских ассоциаций и ассоциаций, объединяющих субъектов IT-рынка, является как целесообразным точки зрения обеспечения защиты интересов их участников на соответствующем рынке, так и вполне гармонирующим с их организационно-правовой формой.

Проведя анализ преимуществ и недостатков различных организационно-правовых форм с точки зрения возможности участия в их уставных капиталах

[214] https://apkit.ru/about/

различных субъектов, функционирующих, регулирующих, организующих и обслуживающих банковский рынок, полагаем важным отметить, что **структура капитала универсального IT-аутсорсера может стать одним из средств, минимизирующих как риск его финансовой устойчивости, так и его правовой и репутационный риски.**

Как было неоднократно отмечено, близость рисков конфликта интересов и обеспечения конфиденциальности информации позволяет в качестве одной из возможных моделей формирования уставного капитала универсального IT-аутсорсера использовать законодательную модель кредитных рейтинговых агентств. Среди четырех кредитных рейтинговых агентств наиболее ярко диверсификация уставного капитала с установлением предельного размера доли участия можно обнаружить в корпоративной модели одного из крупнейших кредитных рейтинговых агентств АКРА (АО), имеющего 27 акционеров, среди которых кредитные организации и иные крупные российские компании с равными долями 3,7037%. В числе акционеров, помимо крупных банков, также АФК «Система», АО «Коммерсант», Управляющая компания «Лидер», Московская биржа, «Федеральная сетевая компания Россети»[215]. Такое решение, безусловно, интересно для правовой модели универсального IT-аутсорсера, **структуру участников (акционеров) которого могут представлять кредитные организации-потребители услуг, разработчики банковского ПО или иные субъекты рынка IT- аутсорсинга – поставщики услуг, инфраструктурные организации, в том числе обеспечивающие услуги телекоммуникации и связи, а также представляющие интересы предпринимательского сообщества на соответствующих банковском и технологическом рынках, - ассоциации (союзы) кредитных организаций, а также ассоциации (союзы) субъектов рынка IT-аутсорсинга.**

[215] https://acra-ratings.ru/company/

При этом, как было отмечено, для минимизации риска возникновения конфликта интересов по аналогии с кредитными рейтинговыми агентствами, а также для минимизации обозначенных рисков возникновения контроля и существенного влияния как основания возникновения банковской группы, полагаем, что требование по предельному проценту участия кредитных организаций (20%) может быть установлено для универсального IT-аутсорсера.

2.3. Определение ограничений на возможную организационно-правовую форму компании, исходя из необходимости получения лицензий и/или прохождения сертификаций, ориентируясь на перечень необходимых IT-функций.

В соответствии со ст. 3 Федерального закона от 04.05.2011 № 99-ФЗ «О лицензировании отдельных видов деятельности»[216] (далее – Закон о лицензировании) лицензия представляет собой специальное разрешение на право осуществления юридическим лицом или индивидуальным предпринимателем конкретного вида деятельности (выполнения работ, оказания услуг, составляющих лицензируемый вид деятельности), которое подтверждается записью в реестре лицензий. **Таким образом, данный закон не содержит ограничений для отдельных организационно-правовых форм юридических лиц на получение лицензий для осуществления соответствующих видов деятельности.**

Компании IT-аутсорсеру согласно ст. 12 Закона о лицензировании может потребоваться получение лицензии при осуществлении следующих видов деятельности:

1) разработка, производство, распространение шифровальных (криптографических) средств, информационных систем и телекоммуникационных систем, защищенных с использованием шифровальных (криптографических) средств, выполнение работ, оказание

[216] СЗ РФ. 2011, N 19, ст. 2716.

услуг в области шифрования информации, техническое обслуживание шифровальных (криптографических) средств, информационных систем и телекоммуникационных систем, защищенных с использованием шифровальных (криптографических) средств[217];

2) разработка и производство средств защиты конфиденциальной информации[218];

3) деятельность по технической защите конфиденциальной информации[219];

4) оказание услуг связи[220]: в частности, к лицензируемым подвидам такой деятельности относятся услуги связи по предоставлению каналов связи и услуги связи по передаче данных, за исключением услуг связи по передаче данных для целей передачи голосовой информации[221].

Соответственно, при привлечении IT-аутсорсером сторонних организаций, выполняющих указанные функции, данные компании должны иметь указанные виды лицензий.

Кроме получения лицензий на осуществление соответствующих видов деятельности, функционирование IT-аутсорсера может быть связано с продукцией, подлежащей добровольной сертификации согласно

---

[217] Следует отметить, что осуществление лицензируемой деятельности иностранными юридическими лицами не допускается. См.: Постановление Правительства РФ от 16.04.2012 N 313 «Об утверждении Положения о лицензировании деятельности по разработке, производству, распространению шифровальных (криптографических) средств, информационных систем и телекоммуникационных систем, защищенных с использованием шифровальных (криптографических) средств, выполнению работ, оказанию услуг в области шифрования информации, техническому обслуживанию шифровальных (криптографических) средств, информационных систем и телекоммуникационных систем, защищенных с использованием шифровальных (криптографических) средств (за исключением случая, если техническое обслуживание шифровальных (криптографических) средств, информационных систем и телекоммуникационных систем, защищенных с использованием шифровальных (криптографических) средств, осуществляется для обеспечения собственных нужд юридического лица или индивидуального предпринимателя)» // СЗ РФ. 2012, N 17, ст. 1987.

[218] Постановление Правительства РФ от 03.03.2012 N 171 «О лицензировании деятельности по разработке и производству средств защиты конфиденциальной информации» // СЗ РФ. 2012, N 11, ст. 1297.

[219] Постановление Правительства РФ от 03.02.2012 N 79 «О лицензировании деятельности по технической защите конфиденциальной информации» // СЗ РФ. 2012, N 7, ст. 863

[220] Федеральный закон от 07.07.2003 N 126-ФЗ «О связи» // СЗ РФ. 2003, N 28, ст. 2895.

[221] Постановление Правительства РФ от 30.12.2020 N 2385 «О лицензировании деятельности в области оказания услуг связи и признании утратившими силу некоторых актов Правительства Российской Федерации» // 2021, N 2 (Часть II), ст. 435.

Федеральному закону от 27.12.2002 № 184-ФЗ «О техническом регулировании»[222] (далее – Закон о техническом регулировании).

Следует отметить, что Законом о техническом регулировании, а также Перечнями продукции, утвержденными Постановлением Правительства РФ от 23.12.2021 № 2425[223] согласно п. 3 ст. 46 указанного Закона, обязательная сертификация, в частности ПО, не предусмотрена. Обязательная сертификация проводится для ПО, которое используется для защиты сведений, составляющих государственную тайну. Закон о государственной тайне[224] предусматривает обязательную сертификацию средств защиты информации, а к ним относятся, в том числе и программные средства (ст. 2, ст. 28 Закона о государственной тайне, п. 1 Положения о сертификации средств защиты информации).

В остальных случаях согласно п. 2 ст. 20, ст. 21 Закона о техническом регулировании проводится сертификация ПО в форме добровольной сертификации.

Однако, с учетом того, что IT-аутсорсинг предполагает взаимодействие с кредитными организациями, очевидно, что ПО и услуги соответствующего IT-аутсорсера должны будут соответствовать повышенным требованиям, которые предъявляются Банком России к кредитным организациям в данной сфере. Как было отмечено, кредитные организации должны соблюдать требования в части осуществления контроля за передачей отдельных функций на аутсорсинг в рамках системы внутреннего контроля[225] (п. 4.1., пп. 4.1.1 Положения Банка России от 16.12.2003 № 242-П «Об организации внутреннего контроля в кредитных организациях и банковских группах»).

---

[222] СЗ РФ. 2002, N 52 (ч. 1), ст. 5140.

[223] Постановление Правительства РФ от 23.12.2021 № 2425 «Об утверждении единого перечня продукции, подлежащей обязательной сертификации, и единого перечня продукции, подлежащей декларированию соответствия, внесении изменений в постановление Правительства Российской Федерации от 31 декабря 2020 г. N 2467 и признании утратившими силу некоторых актов Правительства Российской Федерации» // СЗ РФ. 2022, N 1 (Часть I), ст. 136 (начало); 2022, N 1 (Часть II), ст. 136 (продолжение).

[224] Закон РФ от 21.07.1993 № 5485-1 «О государственной тайне» // СЗ РФ. 1997, N 41, стр. 8220-8235.

[225] Доклад Банка России «Основные направления SupTech и RegTech на период 2021-2023 годов». М., 2021. С. 12. // https://cbr.ru/Content/Document/File/120709/SupTech_RegTech_2021-2023.pdf

Согласно п. 7.8 Положения Банка России от 08.04.2020 № 716-П «О требованиях к системе управления операционным риском в кредитной организации и банковской группе»[226] в политике информационной безопасности **кредитная организация** (головная кредитная организация банковской группы) в целях управления риском информационной безопасности **определяет, в частности, требования к третьим лицам (внешним подрядчикам, контрагентам, участникам банковской группы), которым могут быть переданы функции кредитной организации (головной кредитной организации банковской группы) по обеспечению информационной безопасности, а также определение порядка взаимодействия и распределения ответственности между кредитной организацией (головной кредитной организацией банковской группы) и привлеченными ею третьими лицами**.

Так, Банк России установил требования к операционной надёжности, которым должно соответствовать программное обеспечение банка или небанковской кредитной организации[227]. Положение содержит пороговый уровень допустимого времени простоя и (или) деградации технологических процессов кредитных организаций и другие обязанности по содержанию ПО. Во внутренних документах должен быть определён показатель уровня операционного риска, при нарушении которого проводится ежедневный мониторинг значений показателя и реализация мер, направленных на устранение превышения фактического значения данного показателя, а также предельное значение показателя риска, при нарушении которого информация доводится до Совета директоров[228].

Кредитные организации в соответствии с пунктом 9 Положения Банка России № 683-П должны обеспечить проведение оценки соответствия уровню

[226] Вестник Банка России. 2020. № 51.
[227] Положение Банка России от 12.01.2022 N 787-П "Об обязательных для кредитных организаций требованиях к операционной надежности при осуществлении банковской деятельности в целях обеспечения непрерывности оказания банковских услуг" // "Вестник Банка России", N 25, 27.04.2022.
[228] П. 5.1 Положения Банка России от 08.04.2020 N 716-П «О требованиях к системе управления операционным риском в кредитной организации и банковской группе».

защиты информации не реже одного раза в два года. Оценка соответствия защиты информации должна осуществляться с привлечением сторонних организаций, имеющих лицензию на проведение работ и услуг:

1) услуги по контролю защищенности конфиденциальной информации от несанкционированного доступа и ее модификации в средствах и системах информатизации;

2) работы и услуги по проектированию в защищенном исполнении:

- средств и систем информатизации;
- помещений со средствами (системами) информатизации, подлежащими защите;
- защищаемых помещений;

3) услуги по установке, монтажу, наладке, испытаниям, ремонту средств защиты информации (технических средств защиты информации, защищенных технических средств обработки информации, технических средств контроля эффективности мер защиты информации, программных (программно-технических) средств защиты информации, защищенных программных (программно-технических) средств обработки информации, программных (программно-технических) средств контроля эффективности защиты информации)[229].

Далее результаты оценки соответствия требованиям представляются Банку России[230]. Системно значимые кредитные организации, кредитные организации, выполняющие функции оператора услуг платежной инфраструктуры системно значимых платежных систем, кредитные организации, значимые на рынке платежных услуг, должны реализовывать усиленный уровень защиты информации. Кредитные организации, не

[229] Подпункты "б", "д" или "е" пункта 4 Положения «О лицензировании деятельности по технической защите конфиденциальной информации», утвержденного постановлением Правительства РФ от 03.02.2012 N 79 // СЗ РФ. 13.02.2012, N 7, ст. 863

[230] Информационное письмо Банка России от 21.07.23 № ИН-017-56/48 «О порядке проведения оценки соответствия защиты информации».

относящиеся к кредитным организациям, перечисленным выше, должны реализовывать стандартный уровень защиты информации.

Кроме того, кредитные организации должны обеспечить ежегодное тестирование на проникновение и анализ уязвимостей информационной безопасности объектов информационной инфраструктуры[231]. Пункт 4.1 Положения Банка России № 683-П устанавливает обязательную сертификацию прикладного программного обеспечения, автоматизированных систем и приложений, распространяемых кредитной организацией клиентам для совершения действий в целях осуществления банковских операций, а также программного обеспечения, обрабатывающего защищаемую информацию на участках, используемых для приема электронных сообщений к исполнению в автоматизированных системах и приложениях с использованием информационно-телекоммуникационной сети "Интернет" в системе сертификации Федеральной службы по техническому и экспортному контролю или оценку соответствия по требованиям к оценочному уровню доверия не ниже чем ОУД 4 в соответствии с требованиями национального стандарта Российской Федерации ГОСТ Р ИСО/МЭК 15408-3-2013. К иному прикладному программному обеспечению кредитная организация должна самостоятельно определить необходимость сертификации. Таким образом, полагаем, что **для оказания кредитным организациям услуг IT-аутсорсинга, компания IT-аутсорсер должна соответствовать требованиям не ниже, чем указаны в нормативных актах Банка России для кредитных организаций, и выше.**

Полагаем, что аналогичная ситуация возникает и в сфере использования СКЗИ. На финансовом рынке существует специальное регулирование в отношении использования СКЗИ. Соответственно, при передаче кредитными организациями данных функций на аутсорсинг возникнет очевидная

[231] Пункт 3.2 Положения Банка России от 17.04.2019 N 683-П "Об установлении обязательных для кредитных организаций требований к обеспечению защиты информации при осуществлении банковской деятельности в целях противодействия осуществлению переводов денежных средств без согласия клиента" // "Вестник Банка России", N 33, 22.05.2019.

необходимость соблюдения повышенных стандартов, установленных нормативными актами Банка России. Так, деятельность, связанная с изготовлением криптографических ключей СКЗИ, а также комплекс мер по защите данной информации должны осуществляться в соответствии с технической документацией на СКЗИ[232].

При этом, как было указано ранее, **при отнесении универсального IT-аутсорсера к лицам, оказывающим профессиональные услуги на финансовом рынке, многие проблемы подстройки повышенным банковским стандартам могут быть нивелированы, поскольку на таких субъектов распространяется действие Положения Банка России 17.10.2022 № 808-П[233], согласно которому данные субъекты применяют СКЗИ российского производства, СКЗИ должны иметь сертификаты соответствия федерального органа исполнительной власти в области обеспечения безопасности.** В случае наличия в технической документации на СКЗИ требований к оценке влияния аппаратных, программно-аппаратных и программных средств сети (системы) конфиденциальной связи, совместно с которыми предполагается штатное функционирование СКЗИ, на выполнение предъявляемых к ним требований, такая оценка должна проводиться в соответствии с Положением ПКЗ-2005 по техническому заданию, согласованному с федеральным органом исполнительной власти в области обеспечения безопасности[234].

---

[232] Пункт 6.3 Положения Банка России от 17.04.2019 N 683-П "Об установлении обязательных для кредитных организаций требований к обеспечению защиты информации при осуществлении банковской деятельности в целях противодействия осуществлению переводов денежных средств без согласия клиента" // "Вестник Банка России", N 33, 22.05.2019.

[233] Положение Банка России от 17.10.2022 N 808-П «О требованиях к обеспечению защиты информации при осуществлении деятельности в сфере оказания профессиональных услуг на финансовом рынке в целях противодействия осуществлению незаконных финансовых операций, обязательных для лиц, оказывающих профессиональные услуги на финансовом рынке, к обеспечению бюро кредитных историй защиты информации, указанной в статье 4 Федерального закона "О кредитных историях", при ее обработке, хранении и передаче сертифицированными средствами защиты, а также к сохранности информации, полученной в процессе деятельности кредитного рейтингового агентства» // ВБР. 2022. № 62.

[234] Приказ ФСБ РФ от 09.02.2005 N 66 "Об утверждении Положения о разработке, производстве, реализации и эксплуатации шифровальных (криптографических) средств защиты информации (Положение ПКЗ-2005)" // Российская газета", N 55, 19.03.2005.

Нельзя обойти вниманием и антисанкционную меру, связанную с критической инфраструктурой. С 12.09.2023 вступили в силу положения Федерального закона от 13.06.2023 № 243-ФЗ «О внесении изменений в Федеральный закон «О Центральном банке Российской Федерации (Банке России)»[235], который предусматривает дополнительные требования к кредитным организациям и некредитным финансовым организациям, связанным с переходом на преимущественное использование российского ПО. Так, согласно ст. 57.5-1 Закона о Банке России в целях обеспечения непрерывности оказания банковских услуг Банк России осуществляет согласование планов мероприятий кредитных организаций по переходу на преимущественное использование российского программного обеспечения, отечественных радиоэлектронной продукции и телекоммуникационного оборудования, в том числе в составе программно-аппаратных комплексов, на принадлежащих им значимых объектах критической информационной инфраструктуры Российской Федерации и заявок кредитных организаций на согласование закупок иностранного программного обеспечения, радиоэлектронной продукции и телекоммуникационного оборудования, в том числе в составе программно-аппаратных комплексов, а также закупок услуг, необходимых для их использования на таких объектах, в соответствии с порядком, установленным Правительством Российской Федерации по согласованию с Банком России.

Примечательно, что в Докладе Банка России в качестве одного из существенных рисков аутсорсинга неоднократно отмечается проблема привлечения к выполнению функций поставщиков услуг, использующих программно-аппаратные средства, инфраструктуру, расположенные за пределами Российской Федерации. Более того, по статистике Банка России достаточно часто участниками финансового рынка в рамках аутсорсинга привлекаются организации–нерезиденты, входящие в одну банковскую,

[235] СЗ РФ. 2023, N 25, ст. 4432.

финансово-промышленную группу с российской финансовой организацией[236]. Полагаем, что **такая практика в текущих условиях и с учетом новых антисанкционных требований должна быть либо полностью пресечена, либо ограничена компаниями из «дружественных» стран.**

Закон о Банке России устанавливает, что кредитные организации обязаны обеспечить переход на преимущественное использование российского программного обеспечения, отечественных радиоэлектронной продукции и телекоммуникационного оборудования, в том числе в составе программно-аппаратных комплексов, на принадлежащих им значимых объектах критической информационной инфраструктуры РФ в соответствии с согласованными Банком России планами мероприятий кредитных организаций по переходу на преимущественное использование российского программного обеспечения, отечественных радиоэлектронной продукции и телекоммуникационного оборудования, в том числе в составе программно-аппаратных комплексов, на принадлежащих им значимых объектах критической информационной инфраструктуры Российской Федерации, и осуществлять закупки иностранного программного обеспечения, радиоэлектронной продукции и телекоммуникационного оборудования, в том числе в составе программно-аппаратных комплексов, а также закупки услуг, необходимых для их использования на таких объектах, в соответствии с согласованными Банком России заявками. Закон о Банке России предполагает принятие совместно Банком России и профильными ведомствами документов в целях обеспечения реализации данных положений.

На наш взгляд, как и в отношении иной продукции и услуг, очевидно, что и IT-аутсорсеры при передаче им соответствующих функций должны будут соответствовать данным повышенным стандартам, чтобы иметь возможность взаимодействия с кредитными организациями.

---

[236] Доклад Банка России для общественных слушаний «Управление рисками аутсорсинга на финансовом рынке». М., 2022. С. 6, 15. // https://cbr.ru/Content/Document/File/142481/Consultation_Paper_06122022.pdf

3. Юридическая модель распределения ответственности в сфере IT- безопасности между пользователями информационных услуг, их клиентами и IT-аутсорсером: частноправовой и публично-правовой аспекты. Указанная модель должна также включать распределение ответственности в сфере банковской деятельности за действия IT-аутсорсера.

3.1. Частноправовой аспект юридической модели распределения ответственности в сфере IT безопасности между пользователями информационных услуг, их клиентами и IT аутсорсером.

Разделение ответственности за информационную безопасность в соглашениях об IT-аутсорсинге может варьироваться в различных странах и зависеть от требований, закрепленных в нормативно-правовых актах, отраслевых стандартах, а также зависеть от воли самих сторон, которые вступают в договорные отношения.

Общий Регламент по защите данных (General Data Protection Regulation 2016/679), вступивший в силу 25 мая 2018 года[237], года является самым строгим законом о конфиденциальности и безопасности в мире. Этот регламент обновил и модернизировал принципы Директивы о защите данных 1995 года. Регламент определяет основные права человека в эпоху цифровых технологий, обязательства лиц, обрабатывающих данные, методы обеспечения комплаенса, санкции для нарушителей правил. Хотя Регламент был разработан и принят Европейским Союзом, он налагает обязательства на любые организации по всему миру, если они собирают данные или планируют использовать данные, связанные с гражданами Европейского Союза, что особенно актуально для работы с облачными сервисами. В соответствии с Регламентом на нарушителей конфиденциальности и безопасности накладываются значительные штрафы, достигающие сумм в десятки

[237] Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation) https://eur-lex.europa.eu/eli/reg/2016/679/oj

миллионов евро[238]. Регламент закрепляет права субъекта, чьи персональные данные обрабатываются, что дает субъектам контроль над своими личными данными, в том числе посредством необходимости четкого согласия физического лица на обработку его персональных данных, обеспечения более легкого доступа субъекта данных к своим собственным данным, право на исправление и стирание данных, право «быть забытым», право на возражение, в том числе против использования персональных данных в целях «профилирования», право на то, чтобы согласовывать передачу данных от одного поставщика услуг к другому. Регламент также устанавливает обязанность контролеров, которые отвечают за обработку данных, тех, кто обрабатывает персональные данные от их имени (обработчиков), предоставлять физическим лицам прозрачную и легкодоступную информацию об обработке их данных.

Необходимо провести оценку воздействия на защиту данных, чтобы выявить и снизить любые потенциальные риски для прав и свобод граждан Европейского союза, возникающие в результате обработки персональных данных в рамках соглашений об IT-аутсорсинге. Обработчики, которые могут работать по договору IT-аутсорсинга, обязаны принимать соответствующие меры безопасности в соответствии с риском, связанным с выполняемыми ими операциями по обработке данных. В некоторых случаях контролеры также обязаны предоставлять уведомление об утечках персональных данных. Все государственные органы и компании, которые выполняют определенные рискованные операции по обработке данных, также должны будут назначить ответственного за защиту данных. **Строгие санкции предусмотрены в отношении контролеров или обработчиков, нарушающих правила защиты данных. Контролерам данных грозит штраф в размере до 20 миллионов евро или 4% от их мирового годового оборота**. В ст. 28 Регламента установлено, что контролер

[238] https://gdpr.eu/what-is-gdpr/

должен наложить на своего обработчика, которым скорее всего будет IT-аутсорсер список обязательств, которым он должен следовать, например, обеспечение технических и организационных процедур, улучшение связи между сторонами договора и определение того, какая сторона несет риск при неисполнении обязательства. Аутсорсинговым компаниям придется следовать правилам, установленным для их клиентов в соответствии с Регламентом, и усилить свои процедуры безопасности, чтобы гарантировать отсутствие утечки данных[239]. Кроме того, они должны быть в состоянии продемонстрировать свое соответствие требованиям Регламента, подтвердить принятые меры для защиты персональных данных, что может включать договорное условие о защите данных или такое условие, которое следует по умолчанию. Кроме того, в договоре могут быть перечислены, какие меры безопасности должны быть приняты и как ответственность следует за утечку данных. **Если обработка персональных данных является основной деятельностью поставщика IT-аутсорсинга, может потребоваться назначение уполномоченного по защите данных** (DPO) для контроля соблюдения Регламента.

Регламент подтверждает существующее обязательство государств-членов создать независимый надзорный орган на национальном уровне, который будет обеспечивать применении Регламента. Европейский совет по защите данных следит за тем, чтобы Регламент применялся в полной мере. Физические лица могут подать жалобу в надзорный орган и имеют право на судебную защиту и компенсацию. Они имеют право на пересмотр решения своего органа по защите данных в национальном суде[240]. Если поставщик IT-аутсорсинга передает персональные данные за пределы Европейского Союза, он должен обеспечить наличие соответствующих мер безопасности для защиты данных, таких, как стандартные положения о защите данных или обязательные корпоративные правила.

[239] https://cloudemployee.co.uk/blog/it-outsourcing/gdpr-and-its-impact-on-outsourcing
[240] https://www.consilium.europa.eu/en/policies/data-protection/data-protection-regulation/

В соглашении об аутсорсинге необходимо определить роли и обязанности каждой стороны по защите данных. Во-первых, необходимо четко описать меры безопасности, которые обязан реализовать поставщик IT-услуг, а также обязанности и обязательства клиента в отношении защиты данных. Во-вторых, необходимо указать персональные данные, которые будут обработаны, а также цель, для которой они будут использоваться. В-третьих, необходимо изложить механизм передачи данных, особенно в случае, если персональные данные будут передаваться за пределы Европейского Союза. В-четвертых, контракт должен включать положения о безопасности данных, включая технические и организационные меры, которые поставщик IT-услуг будет реализовывать для защиты персональных данных от несанкционированного доступа, использования или раскрытия. В-пятых, необходимо включить положения об утечке данных, включая процедуры, которые должны быть соблюдены в случае утечки данных, включая требования к уведомлению и отчетности. В-шестых, необходимо указать права субъектов данных, в том числе право на доступ, исправление, удаление или ограничение обработки персональных данных. В-седьмых, необходимо предусмотреть сотрудничество с контролирующими органами, включая предоставление ему информации для обеспечения соблюдения Регламента[241].

В Канаде действует Закон о защите личной информации и электронных документах (PIPEDA)[242], который регулирует сбор, использование и раскрытие личной информации. При аутсорсинге организация продолжает нести ответственность за защиту личной информации. Организации, на которые распространяется действие PIPEDA, обычно должны получать согласие человека, когда они собирают, используют или раскрывают его личную информацию. Человек имеет право на доступ к своей личной

[241] https://kruschecompany.com/navigating-gdpr-requirements-in-it-outsourcing-a-practical-guide/#:~:text=Regulation%20(GDPR)%3A-,GDPR%20compliance,security%20measures%2C%20and%20data%20breaches.

[242] Personal Information Protection and Electronic Documents Act (S.C. 2000, c. 5) chrome-extension://efaidnbmnnnibpcajpcglclefindmkaj/https://laws-lois.justice.gc.ca/PDF/P-8.6.pdf

информации, хранящейся в организации, имеет право оспорить ее точность. Личная информация может быть использована только в тех целях, для которых она была собрана. Личная информация должна быть защищена соответствующими мерами безопасности[243]. **В Канаде банк или финансовая организация должны быть уверены в том, что поставщик IT-услуг имеет действующие политики и процессы, включая обучение персонала, а также эффективные меры безопасности, направленные на то, чтобы гарантировать, что информация, находящаяся под его контролем, всегда будет должным образом защищена**[244].

Индия является крупным центром IT-аутсорсинга. В контрактах между индийскими поставщиками IT-услуг и иностранными клиентами часто указываются требования безопасности, стандарты соответствия и штрафы за несоблюдение требований безопасности данных. Поставщик IT-услуг обычно несет ответственность за реализацию мер безопасности и должен соблюдать требования, установленные клиентом. В 2008 году были внесены поправки в Закон об информационных технологиях 2000 года[245], предусматривающие меры по защите данных **в Индии,** которые могут уменьшить опасения по поводу неправильного использования данных / информации в сфере IT-аутсорсинговая. Так, Закон был дополнен разделом 43A, который **предусматривает выплату компенсации в случае, если юридическое лицо не сможет защитить данные**. Закон о поправках также внес несколько новых положений (разделы 66A-F и 67A-C), которые предусматривают такие **преступления, как кража личных данных, получение украденных компьютерных мощностей/устройств, мошенничество, нарушение конфиденциальности, кибертерроризм**. Закон о поправках также внес

[243] PIPEDA in brief https://www.priv.gc.ca/en/privacy-topics/privacy-laws-in-canada/the-personal-information-protection-and-electronic-documents-act-pipeda/pipeda_brief/

[244] Privacy and outsourcing for businesses https://www.priv.gc.ca/en/privacy-topics/employers-and-employees/outsourcing/02_05_d_57_os_01/

[245] Information Technology Act, 2000 chrome-extension://efaidnbmnnnibpcajpcglclefindmkaj/https://eprocure.gov.in/cppp/rulesandprocs/kbadqkdlcswfjdelrquehwuxcfmijmuixngudufgbuubgubfugbububjxcgfvsbdihbgfGhdfgFHytyhRtMjk4NzY=#:~:text=%5B9th%20June%2C%202000%5D%20An,communication%20and%20storage%20of%20information%2C

положения, содержащие требования к посредникам о защите данных/информации, а также предусматривавшие **штрафы за раскрытие информации в нарушение правил** (раздел 72A)[246].

В Австралии действует Закон о конфиденциальности 1988 года[247], который регулирует обработку личной информации. При аутсорсинге ответственность за ее защиту остается за организацией, владеющей информацией. Соглашение об аутсорсинге в отношении личной информации представляет собой письменный договор между провайдером и банком или финансовой организацией, которые заключили с ним договор, в соответствии с которым аутсорсер будет выполнять одно или оба из следующих действий: собирать данные от своего имени или от имени банка или финансовой организации, предоставлять услуги банку или финансовой организации, используя данные, которые он собрал от ее имени или которые были раскрыты ему банком или финансовой организацией. Целью соглашения об аутсорсинге является регулирование обработки «служебных данных», представляющих собой данные, которые собраны аутсорсером по соглашению или были раскрыты ему банком или финансовой организацией для целей соглашения[248].

Как было рассмотрено ранее, в Российской Федерации в законодательстве и нормативных документах Банка России содержатся, скорее, требования публично-правового характера, согласно которым банк или кредитная организация в любом случае будут нести ответственность в случае нарушения требований информационной безопасности, в части конфиденциальной информации, при этом работа с банковской тайной может быть разрешена IT-аутсорсеру при внесении изменений в ст. 26 Закона о банках.

---

[246] Data Protection and Outsourcing https://www.legalservicesindia.com/article/1199/Data-Protection-and-Outsourcing.html

[247] The Privacy Act https://www.oaic.gov.au/privacy/privacy-legislation/the-privacy-act

[248] CDR outsourcing arrangement: privacy obligations for an outsourced service provider https://www.oaic.gov.au/consumer-data-right/consumer-data-right-guidance-for-business/privacy-obligations/cdr-outsourcing-arrangement-privacy-obligations-for-an-outsourced-service-provider

Согласно п. 3.4 Основных направлений развития информационной безопасности кредитно-финансовой сферы на период 2023−2025 годов, разработанных Банком России, использование услуг поставщиков аутсорсинга информационных технологий и облачных сервисов требует от организаций кредитно-финансовой сферы отдельного внимания к передаваемым бизнес-процессам и функциям, подпадающим под регулирование в области защиты информации и операционной надежности со стороны Банка России. При этом поставщики услуг аутсорсинга информационных технологий и облачных сервисов должны в полной мере соблюдать требования законодательства в отношении выполнения бизнес-процессов и функций, переданных на аутсорсинг. **Помимо административной и уголовной ответственности, которая должна быть наложена на поставщиков IT-аутсорсинга наряду с банками в договоре об IT-аутсорсинге должно быть предусмотрено, что поставщик услуг должен выплатить компенсацию банку в случае, если аутсорсер не сможет защитить данные. Банк России должен установить, что на преддоговорной стадии в рамках комплексной проверки поставщика IT-услуг банк, который заключает с ним договор, должке убедиться, что аутсорсер имеет действующие политики в отношении защиты информации, а также процессы, направленные на такую защиту, включая обучение персонала. В договоре должно быть предусмотрено, что IT-аутсорсер должен обеспечить эффективные меры безопасности, направленные на то, чтобы гарантировать, что информация, находящаяся под его контролем, всегда будет должным образом защищена. При этом в договоре об аутсорсинге необходимо определить роли и обязанности каждой стороны по защите данных, что может ограничить ответственность IT-аутсорсера, но не может ограничить ответственность банка.**

Необходимо отдельно остановиться на возможности привлечения к ответственности IT-аутсорсера в случае разглашения банковской тайны.

Согласно пункту 3 статьи 857 ГК РФ в случае разглашения банком сведений, составляющих банковскую тайну, клиент, права которого нарушены, вправе потребовать от банка возмещения причиненных убытков. Для привлечения банка к гражданско-правовой ответственности клиенту необходимо доказать, что разглашение банковской тайны повлекло за собой убытки или упущенную выгоду. При принятии рассмотренных выше изменений в ст. 26 Закона о банках IT-аутсорсер также станет субъектом гражданско-правовой ответственности за разглашение банковской тайны. Поскольку, исходя из норм банковского законодательства и нормативных актов Банка России, ответственность за разглашение банком банковской тайны не снимается в случае ее передачи IT-аутсорсеру, возникает вопрос о распределении данной ответственности перед клиентом между банком и IT-аутсорсером, в том числе в рамках заключенного договора, а также возможность страхования данного риска. **Представляется, что IT-аутсорсер фактически может нести в данном случае ответственность перед клиентом банка лишь в порядке регресса перед самим банком, в аспекте возмещения ущерба в рамках предполагаемых изменений ст. 26 Закона о банках, поскольку договорные отношения между IT-аутсорсером и клиентом банка отсутствует, а также клиент не обладает всей полнотой информации, какие сведения, охраняемые режимом банковской тайны, переданы кредитной организацией IT-аутсорсеру. Как было рассмотрено в разделе о страховании киберрисков, в практике не развито страхование ответственности за причиненный ущерб, за исключением ущерба в виде санкций (как правило, штрафов) за нарушение требований законодательства. Однако при решении проблем, мешающих развитию киберстрахования, возможно более широкое применение института страхования ответственности банков за ущерб, причиненный клиентам в результате раскрытия конфиденциальной информации, в том числе банковской тайны.**

При этом необходимо отметить сложность привлечения к подобного рода ответственности самого банка из-за проблем с доказыванием реального ущерба. Клиенту потребуется обосновать причинно-следственную связь между двумя событиями. Таким образом, риск привлечения к гражданско-правовой ответственности в виде возмещения убытков не является высоким в текущей ситуации. В судебной практике, по крайне мере в настоящее время, практически отсутствуют такие случаи, на что также единодушно ссылаются и эксперты[249].

Отдельно необходимо также коснуться вопроса защиты персональных данных в рамках договорных отношений банка с IT-аутсорсером. Согласно п. 2 ст. 24 Закона о персональных данных предусматривается возмещение морального вреда субъекту персональных данных при условии доказанности свершившегося противоправного поведения банка. То есть общие основания компенсации морального вреда возлагают на лицо обязанность по доказыванию обстоятельств причинения морального вреда. При этом согласно статье 24 Закона о персональных данных возмещение морального вреда осуществляется независимо от возмещения имущественного вреда и понесенных субъектом персональных данных убытков. Как известно, сложность доказывания причинно-следственной связи по искам о взыскании убытков приводит практически к полному отсутствию такого рода дел в судебной практике (что было отмечено применительно и к банковской тайне). Однако, в случае с передачей персональных данных действительно имеется судебная практика о взыскании морального вреда[250], а относительно широкое использование данной формы гражданско-правовой ответственности

[249] См., например: Заем, кредит, факторинг, вклад и счет: постатейный комментарий к статьям 807 - 860.15 Гражданского кодекса Российской Федерации / В.В. Байбак, О.М. Иванов, А.Г. Карапетов и др.; отв. ред. А.Г. Карапетов. М.: М-Логос, 2019. 1282 с. // СПС «КонсультантПлюс».

[250] Апелляционное определение Самарского областного суда от 17.10.2019 N 33-12118/2019. Требование: О защите персональных данных, взыскании компенсации морального вреда. Обстоятельства: Истец указал, что управляющая организация осуществляет доставку квитанций об оплате коммунальных услуг без принятия мер по сохранению персональных данных, а именно в открытом виде; доставка квитанций в незапечатанном виде является нарушением закона, приводит к распространению его персональных данных; незаконными действиями ответчика ему был причинен моральный вред. Решение: Требование удовлетворено частично. // Документ опубликован не был. СПС «Консультант Плюс».

подтверждается и в экспертной литературе[251]. **Как было проанализировано ранее, в рамках передачи осуществления IT-услуг по договору аутсорсинга на поставщика накладывается обязанность соблюдения требований к работе с персональными данными. При этом с точки зрения привлечения к гражданско-правовой ответственности полагаем, что де-факто перед клиентом будет отвечать банк именно в силу наличия договорных отношений между банком и клиентом и отсутствия у клиента достоверной информации об объемах переданной IT-аутсорсеру информации. При этом за причинение ущерба и морального вреда IT-аутсорсер может быть привлечен к ответственности в порядке регресса в целях компенсации финансовых потерь банка.**

3.2. Публично-правовой аспект юридической модели распределения ответственности в сфере IT безопасности между пользователями информационных услуг, их клиентами и IT аутсорсером с учетом требований по распределению ответственности в сфере банковской деятельности за действия IT-аутсорсера.

Как было неоднократно отмечено в настоящем исследовании, ответственность за несоблюдение требований законодательства и регулятора возлагается на банки в том числе и в случае, когда они передали свои функции или отдельные виды деятельности сторонним поставщикам услуг по соглашению аутсорсинга.

Как указывает Банк России, кредитные организации должны соблюдать требования в части осуществления контроля за передачей отдельных функций на аутсорсинг в рамках системы внутреннего контроля.

Согласно п. 7.8 Положения Банка России от 08.04.2020 № 716-П «О требованиях к системе управления операционным риском в кредитной организации и банковской группе»[252] в политике информационной

[251] Савельев А.И. Научно-практический постатейный комментарий к Федеральному закону "О персональных данных". М.: Статут, 2017. 320 с. // СПС «КонсультантПлюс».
[252] Вестник Банка России. 2020. № 51.

безопасности кредитная организация в целях управления риском информационной безопасности определяет, в частности, требования к третьим лицам (внешним подрядчикам, контрагентам, участникам банковской группы), которым могут быть переданы функции кредитной организации (головной кредитной организации банковской группы) по обеспечению информационной безопасности, а также определение порядка взаимодействия и распределения ответственности между кредитной организацией и привлеченными ею третьими лицами.

Банк России ориентирует кредитные организации на то, что **в ряде случаев ущерб от реализации рисков нарушения информационной безопасности не может быть компенсирован поставщиком услуг в рамках заключенных договорных отношений. В связи с этим кредитные организации при привлечении для аутсорсинга поставщиков услуг должны обеспечить реализацию механизмов управления и контроля риска нарушения информационной безопасности, создающей основу для обеспечения соответствия уровня риска нарушения информационной безопасности при передаче бизнес-функций на аутсорсинг уровню риска, принятому самостоятельно кредитной организацией**[253].

Таким образом, помимо установления требований к IT-аутсорсеру по работе с конфиденциальной информацией на уровне, не ниже, чем предъявляется к кредитным организациям, или некредитным финансовым организациям, а также лицам, оказывающим профессиональные услуги на финансовом рынке, сами банки также будут оставаться ответственными за реализацию указанных выше рисков.

Административная ответственность за разглашение информации, доступ к которой ограничен федеральным законом (за исключением случаев, если разглашение такой информации влечет уголовную ответственность)

[253] Стандарт Банка России "Обеспечение информационной безопасности организаций банковской системы Российской Федерации. Управление риском нарушения информационной безопасности при аутсорсинге" СТО БР ИББС-1.4-2018 (принят и введен в действие Приказом Банка России от 06.03.2018 N ОД-568) // Вестник Банка России. 2018. № 27.

предусмотрена статьей 13.14 Кодекса об административных правонарушениях Российской Федерации от 30 декабря 2011 года № 195-ФЗ[254] (далее – КоАП). Субъектом данного правонарушения может быть только физическое лицо, получившее доступ к такой информации в связи с исполнением служебных или профессиональных обязанностей. Также в случае распространения оператором персональных данных без согласия субъекта персональных данных, административная ответственность, как и в случае с банковской и коммерческой тайнами, возникает согласно статье 13.14 КоАП, и на оператора возлагается штраф. Ответственность за разглашение персональных данных в случае совершения юридическим лицом (в нашем понимании – кредитной организацией или IT-аутсорсером) административного правонарушения (пункт 3 статьи 2.1 КоАП) и ответственность лиц, которые данному правонарушению способствовали (статья 2.4 КоАП), может наступить по одной и той же норме, как у юридического лица, так и у должностных лиц (пункт 15 Постановления Пленума Верховного Суда РФ от 24 марта 2005 г. № 5 «О некоторых вопросах, возникающих у судов при применении Кодекса Российской Федерации об административных правонарушениях»[255]).

В уголовном законодательстве предусмотрена также ответственность за передачу персональных данных в случае распространения конфиденциальных сведений о субъекте персональных данных без его согласия (ст. 137 УК РФ).

Помимо административной ответственности, установленной КоАП, в случае нарушения требований статьи 26 Закона о банках за нарушение банковского законодательства к банку могут быть применены меры воздействия Банка России, установленные ст. 74 Закона о Банке России. Таким образом, если к административной ответственности могут быть привлечены должностные лица IT-аутсорсера, то меры воздействия Банка России могут

[254] Кодекс Российской Федерации об административных правонарушениях от 30.12.2001 № 195-ФЗ // СЗ РФ. 2002. N 1 (ч. 1). ст. 1.

[255] Постановление Пленума Верховного Суда РФ от 24.03.2005 N 5 (ред. от 19.12.2013) «О некоторых вопросах, возникающих у судов при применении Кодекса Российской Федерации об административных правонарушениях» // Документ опубликован не был. СПС «Консультант Плюс».

быть применены только к субъектам, регулирование деятельности которых он осуществляет. **Поэтому в случае нарушения требований банковского законодательства, в том числе в части надлежащего уровня управления рисками, кредитная организация вне зависимости от договорных условий с компанией IT-аутсорсером будет нести публично-правовую ответственность перед регулятором. При отнесении универсального IT-аутсорсера к лицам, оказывающим профессиональные услуги на финансовом рынке, помимо всех иных регуляторных требований, которые были рассмотрены ранее, он будет включен как субъект финансового рынка также в сферу регуляторного и надзорного воздействия финансового мегарегулятора и, соответственно, за нарушения требований законодательства данная компания также будет нести публично-правовую ответственность перед Банком России, что будет являться существенным фактором минимизации рисков соответствующих нарушений. Кроме того, минимизации последствий риска распространения персональных данных и сведений, составляющих банковскую тайну, как было рассмотрено в разделе о страховании, может способствовать страхование ответственности кредитных организаций в части публичных санкций (штрафов) вследствие нарушения законодательства, вызванного несоблюдением требований к обеспечению защиты конфиденциальной информации, а также вреда, причиненного имуществу выгодоприобретателей (клиентов банков) вследствие такого раскрытия.**

4. Описание комплексной целевой модели правоотношений, возникающих при создании рынка IT-аутсорсинга в банковской сфере Российской Федерации, по итогам осуществленного анализа.

В рамках анализа общей схемы правоотношений на рынке IT-аутсорсинга, необходимо определить какие услуги не могут передаваться на аутсорсинг банками или финансовыми организациями. Как показывает анализ

международной практики, перечень услуг, которые могут быть переданы на аутсорсинг, оставляется регуляторами открытым. В законодательстве могут содержаться ограничения на передачу определенных услуг на аутсорсинг банками или финансовыми организациями, а также для передачи определенного вида услуг могут быть установлены дополнительные требования. В основе выделения услуг для IT-аутсорсинга должен находиться критерий существенности функций и видов деятельности, передаваемых на аутсорсинг, а также соблюдение принципа о том, что банк или финансовая организация не передает сторонним поставщикам услуг выполнение действий, которые составляют ядро их деятельности.

Ключевой основополагающий принцип рекомендаций регуляторов в отношении соглашений аутсорсинга заключается в том, что банк или финансовая организация должны гарантировать, что такие соглашения не влияют на способность банков или финансовых организаций выполнять свои обязательства перед клиентами и регулятором. Банки и финансовые организации должны принять меры для обеспечения того, чтобы поставщик услуг исходил из тех же стандартов при оказании услуг, из которых исходит сам банк или финансовая организация. Ответственность за соблюдения требований законодательства и регулятора возлагается на банк или финансовую организацию, в том числе и в случае, когда они передали свои функции или отдельные виды деятельность сторонним поставщикам услуг по соглашению IT-аутсорсинга.

В законодательстве не предусмотрены особые статусы в отношении субъектов правоотношений на рынке IT-аутсорсинга, которые могут включать в себя поставщиков услуг, компании, отвечающие за информационную безопасность, провайдеров (поставщиков) инфраструктуры. Между ними могут быть заключены различные соглашения для достижения различных целей: договор поставки, например, на поставку программного обеспечения и оборудования, договор возмездного оказания услуг для оформления договоров аутсорсинга, аутстаффинга (с учетом ограничений российского

законодательства), соглашений об уровне (качестве) обслуживания, договор аренды для использование элементов IT-инфраструктуры, особенно когда речь идет о предоставлении систем хранения данных, предоставление услуг телекоммуникационной связи и облачных серверов с использованием договорной конструкции абонентского обслуживания, договор на техническое обслуживание информационных и технических систем, используемых для обеспечения безопасности, договор о защите конфиденциальной информации.

При определении основных субъектов правоотношений на рынке IT-аутсорсинга на основании выделенных IT-функций можно предположить, что данные функции могут осуществляться единым поставщиком услуг на основании договора аутсорсинга или множеством компаний, которые привлекаются на основании различных гражданско-правовых договоров (модели универсального аутсорсера и модели множественности аутсорсеров). Выбор между универсальной моделью аутсорсинга и моделью множественности аутсорсеров зависит от различных факторов, включая направленность IT-стратегии банка или финансовой организации, их бюджет, толерантность к риску и требуемые им конкретные услуги, при этом проводится тщательный процесс оценки, чтобы определить, какая модель аутсорсинга или комбинация моделей лучше всего соответствует потребностям и целям банка или финансовой организации.

Среди недостатков универсального поставщика услуг можно выделить опасение по поводу излишней концентрации значимых процессов в руках одной компании, что создает риск утраты контроля над функцией и риск создания конкурента на рынке. В этом смысле, если банк или финансовая организация стремится заключить договор аутсорсинга с несколькими компаниями одновременно, это понижает риск монополизации функции в руках одного аутсорсера, которого впоследствии будет сложно заменить. Вместе с тем модели множественности аутсорсеров предполагают увеличение издержек, сложность организации контроля над несколькими аутсорсерами со стороны внутренних ресурсов банка или финансовой организации.

В IT-сфере можно выделить транзакции, которые относятся к разовым или краткосрочным контрактам, и отношения, которые относятся к долгосрочным контрактам, договор аутсорсинга относится к последнему виду в отличие от услуг сервиса и поддержки, имеющих разовый, эпизодический характер и ограниченных временными рамками. Кроме того, транзакции могут быть ориентированы на затраты или на результат. Используя опцию затрат, компании закупают ресурсы у поставщиков, но напрямую управляют своей IT-деятельностью, при опции, ориентированной на результат, поставщики услуг самостоятельно управляют реализацией IT-деятельности. В результате сопоставления выделенных параметров можно выявить четыре различных вида контракта: «покупай», предпочтительный поставщик, «нанимай», предпочтительный подрядчик, каждая из которых имеет преимущества и недостатки.

Архитектуру правоотношений между основными субъектами рынка IT-аутсорсинга составляют помимо договорной стадии также стадия предварительной комплексной проверки, а также стадии мониторинга и контроля, которые необходимы при передаче услуг на аутсорсинг, особенно в банковской сфере. На преддоговорной стадии должна быть проведена комплексная проверка как самого поставщика услуг, так и деятельности, которую он осуществляет. Банк или финансовая организация, которые передают IT-деятельность на аутсорсинг, должны иметь комплексную внутреннюю политику, позволяющую оценить, может ли такая деятельность быть передана на аутсорсинг и если да, то каким образом. Мониторинг деятельности в рамках аутсорсинга, который позволяет отслеживать сохранение контроля за функцией со стороны банка или финансовой организации и соблюдение законодательства, должен проводиться прежде всего самим банком или финансовой организацией с определенной регулярностью и лишь в некоторых случаях проверки должны осуществляться также со стороны регулятора, выполняющего в основном контрольно-надзорные функции. В договоре аутсорсинга должно быть предусмотрено

обеспечение доступа банка или финансовой организации к данным и документам поставщика IT-услуг, которые его касаются, а также право на мониторинг и аудит в отношении деятельности IT-аутсорсера в том числе, требований к отчетности, включая содержание и частоту отчетности.

Действующее российское гражданское право не знает определения договоров аутсорсинга. С юридической точки зрения аутсорсинг представляет собой договор возмездного оказания услуг внешнего исполнителя - специализированной фирмы для выполнения ею определенной деятельности в пользу организации-заказчика, то есть выполнение каких-либо функций, чаще всего непрофильных для организации.

В международной практике встречаются следующие виды контрактов, которые в различных правопорядках регулируются по-разному. Во-первых, необходимо назвать генеральное соглашение об оказании услуг, которое представляет собой основополагающий документ, содержащий общие положения и условия аутсорсинговых отношений. Во-вторых, это соглашение об уровне обслуживания, которое представляет собой подробный контракт, определяющий конкретные показатели производительности и уровни обслуживания, которым должен соответствовать аутсорсинговый поставщик. В-третьих, это соглашение об обработке данных, которое имеет решающее значение, когда аутсорсинг предполагает обработку личных или конфиденциальных данных, таких как финансовая информация клиентов. В нем описывается, как данные будут обрабатываться, защищаться и обеспечиваться в соответствии с правилами защиты данных и конфиденциальности. Данный контракт обычно касается доступа к данным, их хранению, уведомлениям о нарушениях. В-четвертых, в рамках правоотношений между основными субъектами рынка IT-аутсорсинга может заключаться соглашение о неразглашении информации, которое используется для защиты конфиденциальной информации. Все перечисленные соглашения могут войти в качестве разделов в генеральное соглашение об оказании услуг или соглашение об уровне обслуживания.

Важным вопросом в отношении архитектуры правоотношений между основными субъектами рынка IT-аутсорсинга является форма заключения договора IT-аутсорсинга, а также необходимость сообщать о заключении такого договора в уведомительном порядке регулятору или необходимость получать одобрение регулятора на заключение такого договора. В большинстве юрисдикций установлены требования к письменной форме заключения соглашения об IT-аутсорсинге, обычно требуется согласие регулятора на привлечение стороннего поставщика услуг по договору IT-аутсорсинга в банковской сфере.

Различные страны устанавливают минимальные требования к условиям соглашений аутсорсинга, которые могут отличаться друг от друга. В случае, если регулятор установит необходимость включения в договор аутсорсинга определенных условий, стороны такого договора будут обязаны соблюдать данное требование.

Существенными условиями договора возмездного оказания услуг по ГК РФ признается предмет, иногда также в судебной практике срок и цена, что должно быть отражено в договоре аутсорсинга. Предмет соглашения должен включать в себя перечень и описание предоставляемых услуг, которые передаются на аутсорсинг (четкая идентификация и описание аутсорсинговых услуг). Срок оказания услуг, хоть и не признается в судебной практике существенным условием, имеет важное значение для передачи IT-услуг на аутсорсинг и, по нашему мнению, должен быть отражен в договоре об IT-аутсорсинге по требованию регулятора. Стороны вправе включить в договор условие о том, что размер вознаграждения исполнителя зависит от достижения им определенного результата. Это касается, например, требований (стандартов) к производительности стороннего поставщика услуг, которые называются зарубежными регуляторами одним из минимально необходимых условий. Существует и иная модель оплаты услуг на основе абонентской платы, которая также может быть применена к договорам аутсорсинга, причем

как в универсальной модели, так и в модели со множественностью аутсорсеров.

В минимальных требованиях зачастую значится условие договора аутсорсинга о порядке пересмотра соглашения. Так, по российскому праву, в договоре можно установить запрет на его изменение в связи с существенным изменением обстоятельств (п. 1 ст. 451 ГК РФ), если стороны хотят придать договорным отношениям стабильность и неизменность. Возможно также установление срока, в течение которого осуществляется расторжение соглашения после принятия решения о раннем расторжении, чтобы обеспечить плавность передачи осуществления услуг и осуществить непрерывность реализации функции банка или финансовой организации.

Для обеспечения конфиденциальности информации важно прописать в соглашении, как стороны взаимодействуют при ее передаче и работе с ней, в том числе формы, в которых должны храниться данные, положения, определяющие владение и контроль данных, что значится среди минимальных для закрепления условий договора IT-аутсорсинга в требованиях зарубежных регуляторов. В договоре может быть предусмотрена обязанность одной из сторон или обеих сторон не совершать в течение определенного периода действия, в результате которых информация может быть раскрыта третьим лицам.

Так как поставщик услуг аутсорсинга программного обеспечения занимается созданием/адаптацией/развитием/сопровождением прикладного программного обеспечения автоматизированной банковской системы, в процессе своей деятельности он может создавать результаты интеллектуальной деятельности, в связи с чем необходимо определить, кому будут принадлежать исключительные права на них. Это может быть сделано как в договоре аутсорсинга, так и в самостоятельных договорах, например, лицензионных или договорах о передаче исключительных прав на результаты интеллектуальной деятельности.

В договоре об аутсорсинге должно быть установлено, имеет ли поставщик услуг право использовать активы банка или финансовой организации и каким образом. Вопросы поставки оборудования или программного обеспечения могут быть урегулированы в договорах поставки.

Полагаем, что использование правового механизма страхования киберрисков может способствовать в рамках договорных отношений между кредитной организацией и IT-аусорсером снижению большинства ключевых рисков, рассматриваемых в настоящем исследовании: риска потери финансовой устойчивости (риск утраты контроля за функцией, системный риск), операционного риска (риск ошибки персонала, риск сбоя информационных систем, риск информационной безопасности), правового риска (комплаенс-риск, риск раскрытия конфиденциальной информации, риск нарушения договора с IT-аутсорсером, риск прекращения договора с IT-аутсорсером), репутационного риска (риск недобросовестных действий IT-аутсорсера). Однако очевидно, что минимизировать указанные риски киберстрахование сможет только при расширении страховых продуктов, предлагаемых страховыми организациями, что возможно в результате решения проанализированных правовых проблем: появления регулярной аналитики о киберинцидентах, закрепления в нормативных актах Банка России права страховых организаций на получение обезличенных данных о кибератаках, а также установления единых методик анализа текущих угроз информационной безопасности и операционной надежности кредитной организации и IT-аутсорсера.

Очевидно, что необходимость осуществления взаимодействия IT-аутсорсера с регулирующими органами возникает в основном вследствие передачи ему от банка соответствующей, в том числе конфиденциальной, информации. Ключевыми рисками в данной сфере являются операционный и правовой, так как в рамках различных нарушений при осуществлении ключевых функций IT-аутсорсера (оказание услуг аутсорсинга ПО, инфраструктурных услуг, а также услуг в области безопасности) через

реализацию рисков ошибок персонала, рисков сбоя информационных систем, рисков информационной безопасности может реализоваться риск раскрытия конфиденциальной информации.

Предоставление IT-аутсорсеру сведений, составляющих банковскую тайну возможно только в случае прямого разрешения такой передачи в банковском законодательстве.

При работе IT-аутсорсера с персональными данными необходимо выполнение ряда требований в данной сфере, которые зависят от вида персональных данных, с которыми работает IT-аутсорсер, а также от уровня угрозы им.

При передаче и обработке кредитной организацией информации, IT-аутсорсер должен выполнять требования защиты информации, не ниже, чем это установлено для кредитных организаций или некредитных финансовых организаций, а также лиц, оказывающих профессиональные услуги на финансовом рынке. Однако в отсутствие специального регулирования в отличие от кредитных организаций IT-аутсорсер будет обязан привлекать организацию, имеющую лицензию на осуществление деятельности по технической защите конфиденциальной информации, для проведения работ и предоставления услуг, предусмотренных Положением о лицензировании деятельности по технической защите конфиденциальной информации.

Таким образом, с точки зрения осуществления взаимодействия IT-аутсорсера с регулирующими органами вследствие передачи ему от банка соответствующей информации, следует отметить, что передача IT-аутсорсеру информации от кредитных организаций, в том числе персональных данных и сведений, охраняемых режимом банковской тайны, неизбежно повлечет такое взаимодействие. При этом для того, чтобы кредитные организации могли взаимодействовать с IT-аутсорсером, и поскольку они остаются ответственными за обеспечение надлежащего уровня защиты конфиденциальной информации, очевидна необходимость распространения на IT-аутсорсера стандартов обеспечения защиты, в том числе

конфиденциальной информации, не ниже, чем для кредитных организаций или некредитных финансовых организаций, а также лиц, оказывающих профессиональные услуги на финансовом рынке, в том числе рассмотренных стандартов, устанавливающих общие подходы к управлению инцидентами, связанными с реализацией информационных угроз, и инцидентами операционной надежности. Помимо установления требований к IT-аутсорсеру по работе с конфиденциальной информацией на уровне не ниже, чем предъявляется к кредитным организациям, или некредитных финансовых организаций, а также лиц, оказывающих профессиональные услуги на финансовом рынке, сами банки также будут оставаться ответственными за реализацию указанных выше рисков.

В части рекомендаций по определению оптимальной организационно-правовой формы компании-аутсорсера при модели универсального посредника, в том числе анализа преимуществ и недостатков для союзов и ассоциаций, кооператива, общества с ограниченной ответственностью и акционерного общества, можно сделать следующие выводы.

Полагаем, что у ассоциации (союза) как возможной организационно-правовой формы для универсального IT-аутсорсера больше недостатков, чем преимуществ. Хотя некоммерческие организации могут осуществлять деятельность, приносящую доход, но делать они это могут только в уставных целях. Поэтому такой IT-аутсорсер будет изначально ограничен теми видами деятельности, которые будут закреплены в его Уставе, что видится неудобным, особенно с учетом стремительного развития данной отрасли с возможностью появления все нового функционала.

Кроме того, в отличие от коммерческих организаций, где участник обладает правами на акцию, долю или пай, никаких прав на вложения (членские взносы) у члена ассоциации не возникает, собственником членских взносов и так является сама ассоциация (союз), соответственно, полученный доход между членами ассоциации не распределяется.

Еще одной препоной, по нашему мнению, является такое право члена ассоциации, как право на равных началах с другими членами пользоваться безвозмездно оказываемыми ассоциацией услугами. В этом случае, если часть кредитных организаций станет членами ассоциации, неизбежно возникнет конфликт интересов между членами ассоциации и иными кредитными организациями, для которых услуги будут платными. Включение же всех кредитных организаций, функционирующих на рынке, в члены ассоциации видится мало реализуемым. При этом перечень IT-услуг, которые могут потребоваться разным кредитным организациям, также может очень сильно разниться. Все это неизбежно создаст сложности в организации деятельности ассоциации, поскольку принятие решений о порядке определения размера и способа уплаты членских взносов, о дополнительных имущественных взносах членов ассоциации (союза) в ее имущество относится к исключительной компетенции высшего органа ассоциации (союза), которым, как правило, является Собрание членов ассоциации. Включение в качестве членов ассоциации субъектов рынка IT-аутсорсинга, в том числе поставщиков ПО, видится для этой организационно-правовой формы в принципе не рациональным, так как не совсем ясно, какие услуги за счет своих членских взносов им сможет оказывать универсальный IT-аутсорсер.

У производственного кооператива как потенциальной организационно-правовой формы IT-аутсорсера также обнаружено больше недостатков, чем преимуществ. С учетом необходимости личного трудового участия пайщиков данная организационно-правовая форма ограничит возможное разнообразие субъектов, которые могут стать ее членами, поскольку, исходя из функций IT-аутсорсера, личное трудовое участие можно реализовать в основном только через конкретных физических лиц-представителей поставщиков ПО и других участников рынка IT-аутсорсинга, но не за счет кредитных организаций, ассоциаций или Банка России, поскольку по смыслу российского законодательства пользование услугами компании вряд ли можно отнести к личному трудовому участию. Причем не менее 75% пайщиков участвуют

личным трудовым вкладом. Структура органов управления производственного кооператива и их компетенция достаточно гибкая. Снижению вероятности возможного конфликта интересов и возникновения ситуации существенного влияния и контроля может способствовать правило о том, что каждый член кооператива независимо от размера его пая имеет при принятии решений общим собранием членов кооператива один голос, в связи с чем отсутствует необходимость обеспечения паритетного участия в уставном капитале (для ПАО), установления ограничения количества акций, принадлежащих одному акционеру, и их суммарной номинальной стоимости, а также максимального числа голосов, предоставляемых одному акционеру (для неПАО), установления ограничения максимального размера доли участника общества и изменения соотношения долей участников общества (для ООО). С другой стороны, для крупной компании, каковой видится универсальный IT-аутсорсер, все же более оптимален учет соотношения размера его вклада в уставный капитал и голоса, который он ему предоставляет. Тем не менее, в производственных кооперативах его член может на договорных началах передавать принадлежащие ему материальные ценности и иные средства кооперативу. При этом выход или исключение из кооператива не являются основанием для одностороннего прекращения или изменения взаимоотношений члена кооператива и кооператива по поводу переданного имущества, если иное не предусмотрено соглашением сторон, что является определенным преимуществом данной организационно-правовой формы, но не определяющим ее приоритет над другими с учетом отмеченных в настоящем разделе недостатков.

Организационно-правовая форма общества с ограниченной ответственностью, хотя и имеет ряд недостатков, все же представляется имеющей значительное количество преимуществ для создания в ней универсального IT-аутсорсера. В качестве преимущества для универсального IT-аутсорсера как средства снижения вероятности конфликта интересов и получения одним или несколькими учредителями (участниками) контроля или

существенного влияния в отношении общества можно рассматривать требования п. 3 ст. 14 Закона об ООО, согласно которому Уставом общества может быть ограничен максимальный размер доли участника общества. Тем не менее, полагаем, что к IT-аутсорсеру должны предъявляться дополнительные требования с точки зрения минимизации риска конфликта интересов, финансовой устойчивости, раскрытия информации о своей деятельности, формирования уставного капитала и др. Поэтому в отсутствие специального законодательного регулирования в отношении корпоративных требований к IT-аутсорсеру общество с ограниченной ответственностью как организационно-правовая форма не сможет в полной мере обеспечить данные задачи минимизации рисков, поскольку учредители сами будут решать, какова будет структура органов управления обществом, компетенция, структура уставного капитала, права участников, в том числе на выход из ООО, а также какая информация будет раскрываться обществом.

ПАО является более устойчивой формой по сравнению с ООО, так как не предполагает выхода участников и выплаты им действительной стоимости доли. Из преимуществ также можно выделить большую привлекательность для инвесторов и, соответственно, выход на международный уровень, в том числе сотрудничество с «дружественными» юрисдикциями. Преимуществом ПАО по сравнению с неПАО и ООО в случае создания IT-аутсорсера, является, по нашему мнению, также обязанность создания Совета директоров, органа, который по примеру требований к кредитным организациям, может быть нацелен на минимизацию конфликта интересов в структуре корпоративного управления компании. Что касается обеспечения прозрачности деятельности акционерных обществ, то данное требование имеет и свои преимущества с точки зрения клиентов, но также и свои недостатки с учетом санкционных рисков.

Полагаем, что жесткость требований к аутсорсеру как универсальному посреднику будет компенсироваться эффектом масштаба (соединением большинства функций всего множества посредников). При этом

нецелесообразно ограничивать возможность создания IT-аутсорсера исключительно организационно-правовой формой акционерного общества, как это сделано, например, в отношении акционерного инвестиционного фонда. Оптимально установление одной из организационно-правовых форм хозяйственных обществ с определением публичных требований в законодательстве, минимизирующих риски каждой из организационно-правовых форм.

Полагаем целесообразным придание универсальному IT-аутсорсеру правового статуса лица, оказывающего профессиональные услуги на финансовом рынке путем внесения изменений в главу X.1-1 Закона о Банке России. Установление такого статуса связано с осуществлением IT-аутсорсером хранения, передачи и обработки информации в соответствующих информационных системах и их компонентах, используемых для осуществления банковских операций банков, что влечет необходимость обеспечения защиты прав их клиентов – физических и юридических лиц.

В связи с этим на основе анализа предъявляемых к финансовым организациям и лицам, оказывающим профессиональные услуги на финансовом рынке, полагаем целесообразным установить для универсального IT-аутсорсера следующие требования:

- регистрация в одной из организационно-правовых форм хозяйственного общества;
- включение в реестр Банка России;
- необходимость разработки и утверждения внутренних документов по минимизации рисков, их согласование для включения в реестр Банка России;
- установление минимального размера собственных средств (капитала);
- обеспечение предотвращения, выявления конфликтов интересов, управление ими и раскрытие информации о них;

- запрет на совмещение с иными видами деятельности, за исключением деятельности по оказанию некоторых дополнительных услуг, определенных в законодательстве;
- закрепление определенной структуры органов управления (Совет директоров), требований к их членам и компетенции;
- установление особых требований, предъявляемых к правовому положению и деловой репутации учредителей, владеющих прямо или косвенно более 10% акций (долей) уставного капитала, влекущие ограничения их прав при несоблюдении данных требований;
- определение квалификационных требований и требований к деловой репутации должностных лиц;
- закрепление дополнительных требований к раскрытию информации.

Полагаем, что все указанные требования целесообразно закрепить при создании правовой модели универсального IT-аутсорсера, так как они гармонично вписываются в его функционал и позволяют частично минимизировать риски потери финансовой устойчивости за счет требований к минимальному размеру собственных средств (капитала), запрета на совмещение с иными видами деятельности и др., правовые риски в части регуляторных требований и контроля из их исполнением, репутационные риски, в том числе возникновение конфликта интересов путем закрепления определенной структуры органов управления (Совет директоров), требований к их членам, их компетенции, а также операционные риски с учетом необходимости разработки и исполнения внутренних документов, позволяющих уменьшить риски ошибок и сбоев.

Основываясь на предложенной классификации дополнительных требований к финансовым организациям и профессиональным субъектам финансового рынка в части корпоративного блока, полагаем целесообразным также установление требований к фирменному наименованию данных субъектов в части обязательного указания на универсального IT-аутсорсера, а также к содержанию его учредительных документов, в частности, по

структуре органов управления, их компетенции, ограничении прав акционеров (участников) на выход, ограничении доли участия, раскрытии информации и т.д., если универсальный IT-аутсорсер будет иметь возможность создания в организационно-правовой форме ООО.

В отношении корпоративного управления по аналогии с кредитными организациями и с учетом создания IT-аутсорсера как хозяйственного общества, в особенности ПАО, полагаем целесообразным применение близких по смыслу требований к системе внутреннего контроля в IT-аутсорсере:

1) закрепление в Уставе IT-аутсорсера сведений о системе органов внутреннего контроля, порядке их образования и полномочиях;

2) организационная структура IT-аутсорсера в части распределения полномочий между членами совета директоров (наблюдательного совета) коллегиального исполнительного органа, определения полномочий единоличного исполнительного органа, полномочий, подотчетности и ответственности всех подразделений IT-аутсорсера, служащих должна соответствовать характеру и масштабу осуществляемой деятельности, уровню и сочетанию принимаемых рисков;

3) внутренний контроль должны осуществлять в соответствии с полномочиями, определенными учредительными и внутренними документами IT-аутсорсера: органы управления IT-аутсорсера при обязательном формировании совета директоров вне зависимости от организационно-правовой формы хозяйственного общества; ревизионная комиссия (ревизор); главный бухгалтер; подразделения и служащие, осуществляющие внутренний контроль в соответствии с полномочиями, определяемыми внутренними документами IT-аутсорсера, включая службу внутреннего аудита и службу внутреннего контроля.

Полагаем, что при изменении архитектуры рынка IT-аутсорсинга с появлением универсального IT-аутсорсера, функции службы внутреннего контроля (СВК) кредитных организаций также должны быть расширены в

части анализа не только экономической целесообразности, но и оценки комплаенс-рисков при заключении банками договоров с IT-аутсорсером. Кроме того, следуя зарубежному опыту, целесообразно закрепление требования по разработке и утверждению Советом директоров кредитных организаций Политики аутсорсинга, а также выделение ответственного сотрудника в рамках службы управления рисками либо службы внутреннего контроля с близким статусом к ответственному сотруднику (структурному подразделению) по противодействию легализации (отмыванию) доходов, полученных преступным путем, и финансированию терроризма, что способствовало бы минимизации целого ряда рисков как при создании универсального IT-аутсорсера, так и при продолжении существования децентрализованного рынка IT-аутсорсинга в финансовой сфере.

По блоку возможных вариантов формирования уставного капитала универсального IT-ауторсера, можно сделать следующие выводы и предложения.

В части участия Банка России в капитале IT-аутсорсера полагаем, что без внесения изменений в федеральное законодательство или принятия отдельного федерального закона о статусе универсального IT-аутсорсера с установлением права Банка России учредить такое юридическое лицо или стать одним из его учредителей (участников) данная модель нереализуема, так как будет противоречить Закону о Банке России.

В отношении участия кредитных организаций в уставном капитале универсального IT-аутсорсера следует отметить, что при установлении контроля или значительного влияния и признания такого объединения банковской группой возникнут определенные банковским законодательством регуляторные и надзорные последствия, которые сводятся к обязанности уведомления об образовании банковской группы, необходимости подготовки и сдачи консолидированной отчетности, выполнении обязательных нормативов, установленных для банковских групп, а также особенностям осуществления банковского надзора за банковскими группами на

консолидированной основе, в том числе путем формирования надзорных групп. Поэтому полагаем важным для создаваемого универсального IT-аутсорсера установление ограничений на предельную долю участия кредитных организаций в его уставном капитале. Установление таких ограничений для кредитных организаций позволит избежать создания банковской группы, предпринимательского объединения, которое не является оптимальным для цели создания IT-аутсорсера и повлечет дополнительную надзорную нагрузку по существу не обусловленную спецификой и задачами его деятельности.

В части анализа участия разработчиков банковского ПО или иных субъектов рынка IT- аутсорсинга в капитале универсального IT-аутсорсера необходимо отметить, что такое участие является оптимальным также и по причине предлагаемых законодательных новелл в области IT-аутсорсинга. При внесении в уставный капитал и имущество IT-аутсорсера имущества, в том числе интеллектуальной собственности, универсальный IT-аутсорсер становится ее владельцем, что снимает риск оказания им соответствующих услуг на посреднической основе с привлечением лиц, не соответствующих требованиям к поставщикам услуг аутсорсинга информационных технологий и облачных услуг, определенных законопроектом.

Полагаем, что структура капитала универсального IT-аутсорсера может стать одним из средств, минимизирующих как риск его финансовой устойчивости, так и его правовой и репутационный риски.

С этой целью структуру участников (акционеров) универсального IT-аутсорсера могут составлять кредитные организации-потребители услуг, разработчики банковского ПО или иных субъектов рынка IT- аутсорсинга – поставщики услуг, инфраструктурные организации, в том числе обеспечивающие услуги телекоммуникации и связи, а также представляющие интересы предпринимательского сообщества на соответствующих банковском и технологическом рынках, - ассоциации (союзы) кредитных организаций, а также ассоциации (союзы) субъектов рынка IT-аутсорсинга.

Как было рассмотрено ранее в связи с анализом различных организационно-правовых форм, соблюдение такого паритета позволит частично минимизировать риск возникновения конфликта интересов, избежав значительного влияния мажоритарных акционеров (участников) на принимаемых IT-аутсорсером решения.

В отношении определения ограничений на возможную организационно-правовую форму компании, исходя из необходимости получения лицензий и/или прохождения сертификаций, ориентируясь на перечень необходимых IT-функций, следует отметить, что Закон о лицензировании не содержит ограничений для отдельных организационно-правовых форм юридических лиц на получение лицензий для осуществления соответствующих видов деятельности.

Однако, с учетом того, что IT-аутсорсинг предполагает взаимодействие с кредитными организациями, очевидно, что ПО и услуги соответствующего IT-аутсорсера должны будут соответствовать повышенным требованиям, которые предъявляются Банком России к кредитным организациям в данной сфере. Для оказания кредитным организациям услуг IT-аутсорсинга, компания IT-аутсорсер должна соответствовать требованиям не ниже, чем указаны в нормативных актах Банка России для кредитных организаций, и выше, чтобы иметь возможность взаимодействия с кредитными организациями.

Полагаем, что при отнесении универсального IT-аутсорсера к лицам, оказывающим профессиональные услуги на финансовом рынке, многие проблемы подстройки повышенным банковским стандартам могут быть нивелированы, поскольку на таких субъектов распространяется действие нормативных актов Банка России в рассматриваемой сфере.

При этом в части распределения публично-правовой ответственности между кредитными организациями и универсальным IT-аутсорсером следует отметить, что в случае нарушения требований банковского законодательства, в том числе в части надлежащего уровня управления рисками, кредитная организация вне зависимости от договорных условий с компанией IT-

аутсорсером будет нести публично-правовую ответственность перед регулятором. При отнесении универсального IT-аутсорсера к лицам, оказывающим профессиональные услуги на финансовом рынке, помимо всех иных регуляторных требований, которые были рассмотрены ранее, он будет включен как субъект финансового рынка также в сферу регуляторного и надзорного воздействия финансового мегарегулятора и, соответственно, за нарушение требований законодательства данная компания также будет нести публично-правовую ответственность перед Банком России, что будет являться существенным фактором минимизации рисков соответствующих нарушений. Кроме того, минимизации последствий риска распространения персональных данных и сведений, составляющих банковскую тайну, как было рассмотрено в разделе о страховании, может способствовать страхование ответственности кредитных организаций в части публичных санкций (штрафов) вследствие нарушения законодательства, вызванного несоблюдением требований к обеспечению защиты конфиденциальной информации, а также вреда, причиненного имуществу выгодоприобретателей (клиентов банков) вследствие такого раскрытия.

В заключение считаем необходимым отметить, что создание правовой модели IT-аутсорсера по аналогии установления требований к компаниям, осуществляющим партнерское финансирование, возможно реализовать через модель экспериментального правового режима. В целом можно согласиться с идеей Банка России, что с целью обеспечения пилотирования цифровых финансовых инноваций на финансовом рынке с возможностью изменять или исключать действие отдельных положений федеральных законов Банк России совместно с Правительством Российской Федерации будет развивать регулирование для внедрения экспериментальных правовых режимов на финансовом рынке. В указанных целях планируется внесение изменений в ряд федеральных законов, регулирующих отношения на финансовом рынке, что

создаст необходимые правовые условия для пилотирования инновационных решений в реальных условиях с привлечением клиентов[256].

Для построения оптимальной правовой модели универсального IT-аутсорсера в настоящем исследовании были выявлены гражданско-правовые (договорные), корпоративные (с учетом корпоративных и иных внутренних процедур в IT-аутсорсере и в кредитной организации-клиенте), а также публично-правовые средства минимизации ключевых рисков: риска потери финансовой устойчивости (риск утраты контроля за функцией, системный риск), операционного риска (риск ошибки персонала, риск сбоя информационных систем, риск информационной безопасности), правового риска (комплаенс-риск, риск раскрытия конфиденциальной информации, риск нарушения договора с IT-аутсорсером, риск прекращения договора с IT-аутсорсером), репутационного риска (риск недобросовестных действий IT-аутсорсера, риск возникновения конфликта интересов), а также риск монополизации рынка (риск злоупотребления доминирующим положением на рынке, риск нарушения законодательства о защите конкуренции в форме недобросовестной конкуренции).

Для наглядности и систематизации проведенного анализа по различным правовым средствам создания правовой модели универсального IT-аутсорсера целесообразно представить ее контуры в табличном формате:

[256] Основные направления развития финансового рынка Российской Федерации на 2023 год и период 2024-2025 годов. М., 2022. С. 47 // https://cbr.ru/Content/Document/File/143773/onfr_2023-2025.pdf

№ п/п	Виды рисков для КО от деятельности IT-аутсорсера / способы минимизации рисков	Способы минимизации рисков договорными условиями	Способы минимизации рисков корпоративными и внутренними процедурами IT-аутсорсера	Способы минимизации рисков публичными требованиями к IT-аутсорсеру	Способы минимизации рисков корпоративными и внутренними процедурами кредитной организации
1.	**Риск потери финансовой устойчивости**				
1.1.	**Утрата контроля за функцией**	1. Ориентация принципа закупок на затраты или на результат: - при опции затрат компании закупают ресурсы у поставщиков, но напрямую управляют своей IT-деятельностью; - при опции, ориентированной на результат, поставщики услуг самостоятельно управляют реализацией IT -деятельности. 2. Страхование риска утраты контроля за функцией.	1. Разработка внутренних документов, содержащих план действий, каким образом должен себя вести поставщик услуг, если функция IT–деятельности была передана или временно перешла к нему, при возникновении проблем, которые могут иметь потенциальную возможность существенно повлиять на предоставление IT-услуги.	1. Определение в законодательстве признаков существенности функций в целях возможности их передачи на аутсорсинг. 2. Установление ограничения/запрета на передачу определенных услуг на аутсорсинг, а также для передачи определенного вида услуг установление дополнительных требований. 3. Установление в нормативных актах Банка России требований по содержанию и согласованию Банком России внутренней политики банка по оценке возможности передачи функции на аутсорсинг	1. Наличие комплексной внутренней политики (Политика аутсорсинга), позволяющей оценить, может ли эта деятельность быть передана на аутсорсинг и если да, то каким образом. 2. Установление корпоративной процедуры одобрения такой политики, например, Советом директоров банка. 3. В политике банка должно быть предусмотрено, каким образом осуществляется минимизация рисков.
1.2.	**Системный риск, в т.ч. качество услуг**	1. Возможность смены поставщика при одностороннем отказе от договора при оплате фактически понесенных расходов поставщика IT - услуг.	1. Диверсификация структуры уставного капитала за счет паритетного участия разных субъектов рынка: КО, поставщиков ПО и других участников рынка	1. Установление требований к организационно-правовой форме. 2. Внесение в реестр Банка России. 3. Установление требований по разработке IT-	1. Разработка Советом директоров кредитной организации Политики аутсорсинга, содержащей порядок действий банка при

		2. Включение в договор условия о том, что размер вознаграждения исполнителя зависит от достижения им определенного результата. 3. Установление в договоре требований (стандартов) к производительности стороннего поставщика. 4. Включение в договор требований в отношении отчетов, которые позволяют заказчику оценить, соблюдаются ли показатели эффективности, а также любую другую информацию, необходимую для мониторинга деятельности стороннего поставщика IT-услуг со стороны банка или финансовой организации.	IT-аутсорсинга, ассоциаций и др. 2. Установление требований по ограничению доли участия (если ООО). 3. Отсутствие права на выход (если ООО) с выплатой действительной стоимости доли.	аутсорсером внутренних документов, утверждаемых Банком России. 4. Установление повышенных требований к размеру собственных средств (капитала) IT-аутсорсера. 5. Установление требований к максимальному размеру участия субъектов в УК. 6. Запрет за совмещение с иными видами предпринимательской деятельности. 7. Дополнительные требования к учредителям и должностным лицам. 8. Установление требований по формированию УК и внесению взносов в имущество, в том числе интеллектуальной собственностью (тогда IT-аутсорсер – владелец). 9. Необходимость получения банком согласия Банка России на привлечение IT-аутсорсера.	необходимости смены поставщика IT-услуг.
2.	**Операционный риск**				
2.1.	**Ошибки персонала**	1. Договорное обязательство поставщиков услуг - сообщать о любых существенных неблагоприятных	1. Установление процедур по минимизации операционного риска во внутренних документах IT-аутсорсера.	1. Установление требований по созданию системы управления операционным риском в IT-аутсорсере. 2. Распространение на IT-аутсорсера Стандартов	1. Разработка Советом директоров кредитной организации Политики аутсорсинга, предусматривающей установление системы

		инцидентах, которые могут иметь потенциальную возможность существенно повлиять на предоставление услуги банку или финансовой организации. 2. Страхование от непреднамеренных ошибок персонала.		Банка России по информационной безопасности и операционной надежности.	контроля за деятельностью персонала IT-аутсорсера со стороны сотрудников банка.
2.2.	**Сбои информационных систем**	1. Наличие технической поддержки, которая доступна 24 часа на основании договорной конструкции абонентской платы. 2. Хранение резервных копий всех документов, в частности, в облачных сервисах, в том числе по договору аренды. 3. Договорное обязательство IT-аутсорсера - сообщать о любых информационных сбоях, недоступности или перебоях в предоставлении услуг, которые могут иметь потенциальную возможность существенно повлиять на предоставление услуги. 4. Поддержание в актуальном состоянии	1. Разработка внутреннего документа, который подробно описывает, что должна иметь компания, чтобы незамедлительно привести планы минимизации рисков в исполнение в случае реализации угрозы.	1.Лицензирование. 2. Сертификация. 3. Распространение на IT-аутсорсера Стандартов Банка России по информационной безопасности и операционной надежности. 4. Взаимодействие с ФинЦЕРТ.	1. Наличие протокола на случай сбоя информационной системы. 2. Разработка Советом директоров кредитной организации Политики аутсорсинга, предусматривающей, в том числе возможность незамедлительно привлечь иного стороннего поставщика услуг при необходимости или наличие внутренних специалистов, способных временно осуществлять работу при сбоях информационных систем (тех. поддержка 24/7).

		планов непрерывности бизнеса и управления инцидентами вместе со стратегией непрерывности. 5. Страхование от технических сбоев.			
2.3.	**Риск информационной безопасности**	1. Письменные договорные условия или отдельный договор для обеспечения конфиденциальности информации, в котором прописано, как стороны взаимодействуют при ее передаче и работе с ней. 2. В договоре может быть предусмотрена обязанность одной из сторон или обеих сторон не совершать в течение определенного периода действий, в результате которых информация может быть раскрыта третьим лицам. 3. Страхование киберрисков: -риск потери или недоступности важных данных; -риск использования неполной или искаженной информации; -риск ответственности за ущерб.	1. Разработка внутренних документов в отношении хранения данных, контроля за данными.	1. Лицензирование. 2. При распространении на IT-аутсорсера статуса профессиональных субъектов финансового рынка, Банк России может установить обязательные требования к обеспечению защиты информации при осуществлении деятельности в сфере оказания профессиональных услуг на финансовом рынке в целях противодействия осуществлению незаконных финансовых операций. 3. Распространение на IT-аутсорсера Стандартов Банка России по информационной безопасности и операционной надежности.	1. Выполнение требований к уровню защищенности информации согласно банковскому законодательству и нормативным актам Банка России с учетом передачи функций на аутсорсинг.
3.	**Правовой риск**				

3.1.	**Комплаенс-риск**	1. Проведение комплексной проверки как самого поставщика услуг, так и его деятельности на преддоговорной стадии. 2. Договорное обязательство об обеспечении доступа банка или финансовой организации к данным и документам поставщика услуг, которые его касаются. 3. Закрепление в договоре права на мониторинг и аудит в отношении деятельности аутсорсера, в том числе требований к отчетности, включая содержание и частоту отчетности.	1. Создание в IT-аутсорсере системы внутреннего контроля по аналогии с системой внутреннего контроля, функционирующей в кредитных организациях.	1. Установление требований к организации в IT-аутсорсере к организации системы внутреннего контроля.	1. Расширение функций СВК в части анализа не только экономической целесообразности, но и оценке комплаенс-рисков при заключении банками договоров с IT-аутсорсером. 2. Выделение в структуре СВК сотрудника с близким статусом к ответственному сотруднику (структурному подразделению) по ПОД/ФТ, ответственного за минимизацию рисков IT-аутсорсинга. 3. Установление во внутренних документах (например, Политике аутсорсинга) порядка мониторинга деятельности IT-аутсорсера со стороны банка с определенной регулярностью с закреплением данного условия в договоре с IT-аутсорсером.
3.2.	**Риск раскрытия конфиденциальной информации**	1. На преддоговорной стадии в рамках комплексной проверки поставщика IT-услуг банк,	1. Разработка внутренних документов по минимизации рисков раскрытия	1. Требования к работе с персональными данными на уровне КО или лицами, оказывающими	1. Выполнение требований Банка России к кредитным организациям по работе

		который заключает с ним договор, должен убедиться, что аутсорсер имеет действующие политики в отношении защиты информации, а также процессы, направленные на такую защиту, включая обучение персонала. 2. Заключение соглашения о том, как стороны взаимодействуют с конфиденциальной информацией при ее передаче, хранении и работе с ней. 3. Возможность предусмотреть обязанность одной из сторон или обеих сторон не совершать в течение определенного периода действий, в результате которых информация может быть раскрыта третьим лицам. 4. Договорное обязательство поставщиков услуг сообщать о любых существенных неблагоприятных инцидентах, в том числе и утечке данных.	конфиденциальной информации.	профессиональные услуги на финансовом рынке. 2. Требования к работе с банковской тайной в ст. 26 Закона о банках, ответственность за ущерб, причиненный раскрытием банковской тайны. 3. Распространение на IT-аутсорсера требований и стандартов Банка России по информационной безопасности и операционной надежности.	с конфиденциальной информацией, в том числе со сведениями, составляющими банковскую тайну и персональными данными при их передаче IT-аутсорсеру.

		5. Установление договорной ответственности поставщика услуг за утечку данных, в том числе выплата компенсации банку в случае, если аутсорсер не сможет защитить данные. 6. Страхование киберриска: риск утечки конфиденциальной информации, в том числе в части компенсации размера ущерба перед клиентом банка, а также санкций (штрафов) за нарушение.			
3.3.	**Риск нарушения договора**	1. Установление штрафных санкций за нарушение договора, в частности неустойки. 2. Расторжение договора по воле стороны, чьи права нарушены существенно, если участник не получил того, на что рассчитывал при заключении договора.	1. Проверка договоров об аутсорсинге службой внутреннего контроля и службой внутреннего аудита на предмет соответствия законодательству и стратегии управления рисками.	1. Установление требований к обязательным условиям договоров между банками и IT-аутсорсером. 2. Установление требований по согласованию условий договоров с Банком России.	1. Проверка договоров об аутсорсинге службой внутреннего контроля и службой внутреннего аудита на предмет соответствия законодательству и стратегии управления рисками.
3.4.	**Риск прекращения договора**	1. Установление в договоре запрета на изменение договора в связи с существенным изменением обстоятельств. 2. Возможность установления в договоре срока, в течение которого	1. Проверка договоров об аутсорсинге службой внутреннего контроля и службой внутреннего аудита на предмет соответствия законодательству и	1. Установление требований к обязательным условиям договоров между банками и IT-аутсорсером.	1. Проверка договоров об аутсорсинге службой внутреннего контроля и службой внутреннего аудита на предмет соответствия законодательству и

		осуществляется расторжение соглашения после принятия решения о раннем расторжении, чтобы обеспечить плавность передачи осуществления услуг другому поставщику услуг. 3. Определение в договоре положения о непрерывности бизнеса.	стратегии управления рисками.		стратегии управления рисками.
4.	**Репутационный риск**				
4.1.	**Недобросовестные действия IT-аутсорсера**	1. Установление штрафных санкций за нарушение договора, в частности неустойки. 2. Расторжение договора по инициативе банка в случае недобросовестных действий IT-аутсорсера с условием о возмещении убытков, причиненных его недобросовестными действиями. 3. Страхование киберриска: риск распространения во внешней среде информации, угрожающей репутации организации.	1. Раскрытие информации в рамках требований к хозяйственным обществам, приоритетно ПАО или установление дополнительных требований в законодательстве к раскрытию информации IT-аутсорсером при выборе иных организационно-правовых форм хозяйственных обществ.	1. Установление дополнительных требований к учредителям и должностным лицам IT-аутсорсера, в том числе в части деловой репутации 2. Согласие регулятора на привлечение IT-аутсорсера.	1. Разработка Советом директоров кредитной организации Политики аутсорсинга, предусматривающей действия банка в случае недобросовестных действий IT-аутсорсера.
4.2.	**Конфликт интересов**	1. Конфликт интересов должен выявляться в ходе комплексной проверки на преддоговорной стадии.	1. Диверсификация структуры уставного капитала за счет паритетного представительства разных	1. Установление требований по согласованию с Банком России приобретения акций (долей) в уставном капитале IT-аутсорсера.	1. Дополнение новыми полномочиями Совета директоров банков в части управления рисками IT-аутсорсинга,

			участников рынка: КО, поставщиков ПО и других участников рынка IT-аутсорсинга, ассоциаций и др. 2. Требование об обязательном наличии в структуре органов управления IT-аутсорсера Совета директоров с полномочиями, близкими к требованиям к КО по управлению конфликтом интересов. 3. Требование к включению независимых директоров в состав Совета директоров.		предотвращения конфликта интересов, утверждения планов финансовой устойчивости и планов проверки службой внутреннего аудита в части IT-аутсорсинга. 2. Разработка Советом директоров кредитной организации Политики аутсорсинга, предусматривающей процедуры, направленные на избежание конфликта интересов при передаче функций IT-аутсорсеру.
5.	**Риск монополизации рынка**				
5.1.	**Злоупотребление доминирующим положением на рынке**		1. Установление требований по осуществлению IT-аутсорсером антимонопольного комплаенса.	1. Установление повышенных требований к порогу доминирующего положения на рынке	1. Разработка Советом директоров кредитной организации Политики аутсорсинга, предусматривающей порядок выбора IT-аутсорсера с учетом минимизации риска концентрации функций у IT-аутсорсера, занимающего доминирующее положение на рынке.

Доктор юридических наук,
профессор кафедры предпринимательского права
Юридического факультета
МГУ имени М.В. Ломоносова ***А.В. Белицкая***

Кандидат юридических наук,
доцент кафедры предпринимательского права
Юридического факультета
МГУ имени М.В. Ломоносова, доцент ***Е.Б. Лаутс***

Приложение № 1

Вопросы	Публичное АО	Непубличное АО	ООО	Кооператив	Союзы и ассоциации
Простота регистрации, в т.ч.: -сроки; -порядок; -необходимые документы.	**Документы** (ст. 12 ФЗ «О госрегистрации ЮЛ»: 1. Заявление по форме о форме № Р11001. 2. Устав АО. 3. Решение (Протокол) о создании АО. 4. Документ, подтверждающий присвоение выпуску (выпускам) акций регистрационного номера (форму документа устанавливает ЦБ РФ). 5. Документ об оплате госпошлины. 6. Не обязательно: документ, подтверждающий адрес АО (например, гарантийное письмо на юридический адрес от собственника или арендодателя помещения). **Порядок (при создании путем учреждения):** Пакет документов подается в регистрирующий орган по юридическому адресу АО/по месту нахождения исполнительного органа ЮЛ (п. 2 ст. 54 ГК РФ, п. 2 ст. 8 ФЗ «О госрегистрации ЮЛ»). Подать документы можно без посещения инспекции с использованием Единого портала Госуслуг, сервиса на сайте ФНС России – в таких случаях требуется заверить документы УКЭП заявителя (п.п.5, 11 Порядка ФНС 28.12.2022 N ЕД-7-14/1267@). **Срок:** ФНС принимает решение о регистрации **в течение 3 рабочих дней** со дня представления документов (п. 1 ст. 8, п. 3 ст. 13, п. 1 ст. 13.1 ФЗ «О госрегистрации ЮЛ»).		**Документы** (ст. 12 ФЗ «О госрегистрации ЮЛ»: 1. Заявление по форме о форме № Р11001. 2. Устав АО. 3. Решение (Протокол) о создании ООО. 5. Документ об оплате госпошлины. 6. Не обязательно: документ, подтверждающий адрес АО (например, гарантийное письмо на юридический адрес от собственника или арендодателя помещения). **Порядок:** Пакет документов подается в регистрирующий орган по юрид. адресу ООО/по месту нахождения исполнительного	**Документы** (ст. 12 ФЗ «О госрегистрации ЮЛ»: 1. Заявление по форме о форме № Р11001. 2. Устав ПК. 3. Решение (Протокол) о создании ПК. 5. Документ об оплате госпошлины. 6. Не обязательно: документ, подтверждающий адрес АО (например, гарантийное письмо на юридический адрес от собственника или арендодателя помещения). **Порядок** (ст. 6 ФЗ о ПК – в порядке ФЗ «О гос. регистрации ЮЛ и ИП»): Пакет документов подается в ФНС по юр. адресу кооператива, проверяется рег. органом на соответствие формальным критериям и принимается решение. **Срок**: не более трех рабочих дней со дня представления	**Документы:** 1. Устав ассоциации (п. 1 ст. 52 ГК РФ, пп. 1,2 ст. 14 ФЗ об НКО, п. 2 ст. 123.9 ГК РФ). 2. Решение о создании ассоциации (союза) (п. 2 ст. 50.1, п. 1 ст. 123.9 ГК РФ) 3. Протокол ассоциации о ее создании (п. 3 ст. 50.1 ГК РФ). 4. Заявление по форме № Р11001, 5. Документ об оплате госпошлины. **Порядок:** Документы необходимо подать в территориальный орган Минюста в течение трех месяцев со дня принятия решения о создании некоммерческой организации (п. 4 ст.

	Порядок (при создании путем реорганизации из непубличного АО в публичное): Необходимо зарегистрировать в Банке России проспект акций (Указание Банка России от 19.10.2015 № 3824-У, п. 76.1 Положения ЦБ РФ от 19.12.2019 № 706-П). Затем требуется заключить договор с организатором торговли о листинге акций Общества (абз. 2 п. 1 ст. 7.1. Закона об АО). Процедура листинга занимает 1-2 месяца. После этого необходимо внести изменения в Устав общества в рег. органе, указав в наименовании АО, что оно является публичным (п. 1 ст. 97 ГК РФ). **Сроки регистрации проспекта акций**: **15 рабочих дней** Банк России принимает решение о гос. регистрации выпуска ценных бумаг (п. 5 ст. 20 Закон о рынке ценных бумаг).	органа ЮЛ (п. 1.3 ст. 9 Закона о госрегистрации юрлиц). Если регистрирующий орган не выявит оснований для отказа в регистрации ООО, то он принимает решение о госрегистрации и вносит запись в ЕГРЮЛ с указанием ОГРН юрлица (п. 1 ст. 11 Закона о госрегистрации. **Срок:** Срок регистрации ООО при создании составляет не более трех рабочих дней со дня представления документов в регистрирующий орган (п. 3 ст. 13 Закона о госрегистрации).	документов в регистрирующий орган (п. 3 ст. 13 Закона о госрегистрации).	13.1 Закона об НКО). По завершении регистрации ассоциации (союзу) выдается свидетельство о государственной регистрации (п. 8 ст. 13.1 Закона об НКО). **Срок:** Не позднее чем через 14 рабочих дней со дня получения необходимых документов регистрирующий орган принимает решение о госрегистрации некоммерческой организации (если нет оснований для ее приостановления или об отказе в регистрации). После регистрации этот орган передает сведения о созданной организации в регистрирующий орган для их внесения в ЕГРЮЛ (п. 8 ст. 13.1

				Закона о некоммерческих организациях).
Предельная численность участников/ учредителей	Ограничений по численности участников законодательством **не предусмотрено.**	Число участников (учредителей) общества **не должно быть более пятидесяти**. В случае превышения лимита ООО должно преобразоваться в открытое АО или в производственный кооператив, в противном случае, будет принудительная ликвидация (п. 3 ст. 7 Закона об ООО).	Число членов кооператива **не может быть менее чем пять человек** (ст. 4 Закон о ПК) Ограничений по числу пайщиков не предусмотрено, но при этом не менее 75% пайщиков участвуют личным трудовым вкладом (п. 2 ст. 7 Закона о производственных кооперативах).	Число учредителей ассоциации (союза**) не может быть менее двух** (ст. 123.9 ГК РФ). Общее число учредителей (членов) для ассоциации (союза) законом не ограничено.
Кто может выступать учредителем/участником? Существуют ли варианты форм участия?	Учредителями АО являются граждане и (или) юридические лица, принявшие решение о его учреждении (п. 1 ст. 10 Закона об АО). Государственные органы и органы местного самоуправления не могут выступать учредителями АО (п. 1 ст. 10 Закона об АО). Государственные органы и органы местного самоуправления не вправе участвовать **от своего имени** в хозяйственных обществах (п. 6 ст. 66 ГК РФ). Права акционеров АО, доли в уставном капитале которых находятся в собственности РФ осуществляет Правительство РФ (абз. 1 п. 1 ст. 39 Закона о приватизации) Общество не может иметь в качестве единственного учредителя (акционера) другое хозяйственное	Участниками общества могут быть граждане и юридические лица (п.1 ст. 7 Закона об ООО). Общество может быть учреждено одним лицом, которое становится его единственным участником. Государственные органы и органы местного самоуправления не	Членами (участниками) кооператива могут быть граждане Российской Федерации, иностранные граждане, лица без гражданства. Юридическое лицо участвует в деятельности кооператива через своего представителя в соответствии с уставом кооператива. (ст. 4 Закона о производственных кооперативах). **Две формы участия –** личным трудовым вкладом и	Юридические лица и (или) граждане (ст. 11 ФЗ об НКО). Форм участия не предусмотрено – однородные члены союза с равными правами Перечень лиц, которые не могут быть учредителями НКО – иностранные граждане; лица без гражданства в

	общество, состоящее из одного лица (п. 2 ст. 10 Закона об АО). **Формы участия**: 1. Акционеры - владельцы обыкновенных акций общества могут в соответствии с ФЗ об АО и уставом общества участвовать в общем собрании акционеров с правом голоса по всем вопросам его компетенции, а также имеют право на получение дивидендов, а в случае ликвидации общества - право на получение части его имущества (п. 2 ст. 31 Закона об АО). 2. Акционеры - владельцы привилегированных акций общества не имеют права голоса на общем собрании акционеров. Размер дивиденда и ликвидационная стоимость определяются в твердой денежной сумме или в процентах к номинальной стоимости привилегированных акций (ст. 32 Закона об АО).	вправе выступать участниками обществ (п. 2 ст. 7 Закона об ООО). Формы участия отсутствуют, участники имеют равные права. Уставом может быть ограничен максимальный размер доли участника общества, а также возможность изменения соотношения долей участников общества (п. 3 ст. 14 Закона об ООО).	без него (п. 2 ст. 7 Закон о ПК).	отношении которых принято решение о нежелательности их пребывания в РФ; лица, включенные в перечень организаций и физ. лиц причастных к экстремистской деяте-ти, (п. 1.2. ст. 15 Закона об НКО).
Ограничение по целевому характеру деятельности компании	Общество имеет гражданские права и несет обязанности, необходимые для **осуществления любых видов** деятельности, не запрещенных федеральными законами (п. 4 ст. 2 Закона об АО) Вместе с тем, отдельными видами деятельности, перечень которых определяется федеральными законами, общество может заниматься только на основании специального разрешения (лицензии) (п. 4 ст. 2 Закона об АО)	Общество может иметь гражданские права и нести гражданские обязанности, необходимые для осуществления **любых видов деятельности**, не запрещенных федеральными законами, если это не противоречит предмету и целям деятельности, определенно ограниченным уставом	Ограничений по целевому характеру не предусмотрено, но Уставом может быть установлено, что определенная часть принадлежащего кооперативу имущества составляет неделимый фонд кооператива, используемый в целях, определяемых уставом кооператива (п. 1 ст. 10 Закона о ПК)	Ассоциации создаются в целях представления и защиты общих, в том числе профессиональных, интересов, для достижения общественно полезных, а также **иных не противоречащих федеральным законам** и имеющих

		общества (п. 2 ст. 2 Закона об ООО). Ограничения правоспособности (ст. 49 ГК РФ) аналогичны как АО, так и в отношении иных организационно-правовых форм.		некоммерческий характер целей (ст. 11 ФЗ об НКО). НКО может осуществлять предпринимательскую и иную приносящую доход деятельность лишь постольку, поскольку это служит *достижению целей, ради которых она создана* и соответствует указанным целям, при условии, что такая деятельность указана в ее учредительных документах. Такой деятельностью признаются приносящее прибыль производство товаров и услуг, отвечающих целям создания некоммерческой организации, а также приобретение и реализация ценных бумаг, имущественных и неимущественных

					прав, участие в хозяйственных обществах и участие в товариществах на вере в качестве вкладчика (п. 2 ст. 24 Закона об НКО).
Структура органов управления	**Обязательно (ст. 66.3, 67.1, 97 ГК РФ):** **Общее собрание акционеров** (ст. 47 Закона об АО). • Коллегиальный орган управления (наблюдательный **или иной Совет**) (ст. 64 Закона о АО, ч. 3 ст. 97 ГК РФ). Совет директоров (наблюдательный совет) общества осуществляет общее руководство деятельностью общества, за исключением решения вопросов, отнесенных Законом об АО к компетенции общего собрания акционеров (п. 1 ст. 64 Закона об АО). Количественный состав совета директоров (наблюдательного совета) публичного общества составляет **пять членов**,	**Обязательно:** • Общее собрание акционеров. • Единоличный исполнительный орган (Директор, Генеральный директор, председатель и т.п.). **Дополнительно:** • Уставом может быть предусмотрено создание коллегиального исполнительного органа (ст. 70 Закона об АО). Правила для него аналогичны правилам КИО для ПАО. • Создание коллегиального органа управления является не обязательным при наличии условий из ст.	**Обязательно:** • **Общее собрание участников общества** (ст. 33 Закона об ООО) • **Единоличный исполнительный орган** (Директор, Генеральный директор, председатель и т.п.) (ст. 40 Закона об ООО) **Дополнительно:** • Полномочия ЕИО могут быть переданы управляющему по договору на осуществление полномочий (ст. 42 Закона об ООО). • Уставом может быть предусмотрено создание **коллегиального исполнительного**	**Обязательно:** • Общее собрание членов кооператива. • Исполнительные органы – Правление и (или) Председатель кооператива (п 1 ст. 14 Закона о ПК). **Дополнительно**: • В кооперативе с числом членов более пятидесяти может быть создан наблюдательный совет (п. 2 ст. 14 Закона о ПК).	**Обязательно:** • Высший орган ассоциации (союза) с исключительной компетенцией (п. 1 ст. 123.10 ГК РФ). • Единоличный исполнительный орган (председатель, президент). **Дополнительно:** • Постоянно действующие коллегиальные исполнительные органы (совет, правление, президиум и тп) (ст. 123.10 ГК РФ).

	если Уставом не предусмотрено большее количество. **Порядок избрания Совета директоров:** Члены совета директоров (наблюдательного совета) общества избираются общим собранием акционеров в порядке, предусмотренном Законом об АО и уставом общества, на срок до следующего годового общего собрания акционеров (п. 1 ст. 66 Закона об АО). Лица, избранные в состав совета директоров (наблюдательного совета) общества, могут переизбираться неограниченное число раз. По решению общего собрания акционеров полномочия всех членов совета директоров (наблюдательного совета) общества могут быть прекращены досрочно. Членом совета директоров (наблюдательного совета)	64 Закона об АО: в обществе с числом акционеров - владельцев голосующих акций менее пятидесяти устав общества может предусматривать, что функции Совета директоров общества (наблюдательного совета) осуществляет общее собрание акционеров. В этом случае устав общества должен содержать указание об определенном лице или органе общества, к компетенции которого относится решение вопроса о проведении общего собрания акционеров и об утверждении его повестки дня (п. 1 ст. 64 Закона об АО). Количественный состав совета директоров (наблюдательного совета), непубличного общества составляет **три члена**, если	**органа** (КИО, ст. 41 Закона об ООО). **Порядок формирования КИО**: Если уставом общества предусмотрено образование наряду с единоличным исполнительным органом общества также коллегиального исполнительного органа общества (правления, дирекции и других), такой орган избирается общим собранием участников общества в количестве и на срок, которые определены уставом общества. Уставом общества может быть предусмотрено отнесение вопросов образования коллегиального исполнительного органа общества и досрочного прекращения его		

	общества может быть только физическое лицо. Член совета директоров (наблюдательного совета) общества может не быть акционером общества. Выборы членов совета директоров (наблюдательного совета) общества осуществляются **кумулятивным голосованием**. **Компетенция Совета директоров определена в ст. 65 Закона об АО:** - определение приоритетных направлений деятельности общества - утверждение повестки дня общего собрания акционеров - созыв годового и внеочередного общих собраний акционеров - увеличение уставного капитала общества путем размещения обществом дополнительных акций - определение цены (денежной оценки) имущества, цены размещения или порядка ее	Уставом не предусмотрено больше членов (п. 3 ст. 66 Закона об АО). Уставом непубличного общества может быть предусмотрена передача в компетенцию совета директоров (наблюдательного совета) общества вопросов, отнесенных Законом об АО к компетенции общего собрания акционеров, за исключением вопросов внесения изменений в устав общества, реорганизации, ликвидации, утверждения внутренних документов (ст. 48 Закона об АО). В отличие от Совета директоров в кредитных организациях, для корпораций как закрытого (неПАО и ООО), так и открытого	полномочий к компетенции совета директоров (наблюдательного совета) общества. Функции председателя коллегиального исполнительного органа общества выполняет лицо, осуществляющее функции единоличного исполнительного органа общества, за исключением случая, если полномочия единоличного исполнительного органа общества переданы управляющему (п. 1 ст. 41 Закона об ООО). **Полномочия КИО**: Коллегиальный исполнительный орган общества осуществляет полномочия, отнесенные уставом общества к его компетенции (п. 1 ст. 41 Закона об ООО).		

	определения и цены выкупа эмиссионных ценных бумаг и иные. Порядок формирования Совета директоров: Члены совета директоров (наблюдательного совета) общества избираются общим собранием акционеров в порядке, предусмотренном Законом об АО и уставом общества, на срок до следующего годового общего собрания акционеров. Членом совета директоров (наблюдательного совета) общества может быть только физическое лицо. Член совета директоров общества может не быть акционером общества (ст. 66 Закона об АО). Вопросы, отнесенные к компетенции совета директоров (наблюдательного совета) общества, не могут быть переданы на решение исполнительному органу общества (п. 2 ст. 65 Закона об АО).	типа не предусмотрено требований в части: - деловой репутации членов Совета директоров; - обязательности уведомления уполномоченных органов об избрании (освобождении) члена совета директоров. Кроме того, законодательством об отдельных юридических лицах не прописаны конкретные обязанности Совета директоров в части разработки стратегии управления рисками. Такая обязанность Законом об АО предусмотрена только для ПАО, в части иных орг-прав форм существует молчание законодателя и данный вопрос должен быть определён Уставом Общества.	**Порядок деятельности КИО:** Порядок деятельности коллегиального исполнительного органа общества и принятия им решений устанавливается уставом общества и внутренними документами общества (п. 2 ст. 41 Закона об ООО). Уставом общества может быть предусмотрено образование **Совета директоров (наблюдательного совета)** общества (п. 2 ст. 32 Закона об ООО). **<u>Порядок формирования и деятельности Совета Директоров:</u>** Порядок образования и деятельности совета директоров (наблюдательного совета) общества, а		

	Вопросы, отнесенные к компетенции общего собрания акционеров, не могут быть переданы на решение совету директоров (наблюдательному совету) общества (ст. 48 Закона об АО). • **Единоличный исполнительный орган** (ЕИО) - Директор, Генеральный директор, председатель (ст. 69 Закона об АО). К компетенции исполнительного органа общества относятся все вопросы руководства текущей деятельностью общества, за исключением вопросов, отнесенных к компетенции общего собрания акционеров или совета директоров (наблюдательного совета) общества. Права и обязанности единоличного исполнительного органа общества определяются Законом об АО, иными правовыми актами и договором. Заключаемым с Обществом (ст. 69 Закона об АО).		также порядок прекращения полномочий членов совета директоров (наблюдательного совета) общества и компетенция председателя совета директоров (наблюдательного совета) общества определяются уставом общества (п. 2 чт. 32 Закона об ООО). **<u>Полномочия Совета директоров</u>**: - определение основных направлений деятельности общества; - образование исполнительных органов общества и досрочное прекращение их полномочий; - установление размера вознаграждения и денежных компенсаций единоличному исполнительному органу общества,		

	Дополнительно: ПАО и неПАО обязаны избирать ревизионную комиссию, если в Уставе есть положение о ее создании в обществе (п. 1 ст. 85 Закона об АО). • Уставом может быть предусмотрено создание коллегиального исполнительного органа (ст. 70 Закона об АО). **Порядок работы и принятия решений коллегиальным исполнительным органом:** Коллегиальный исполнительный орган общества (правление, дирекция) действует на основании устава общества, а также утверждаемого общим собранием акционеров внутреннего документа общества (положения, регламента или иного документа), в котором устанавливаются сроки и порядок созыва и проведения		членам коллегиального исполнительного органа общества, управляющему; - принятие решения о проведении аудита годовой бухгалтерской (финансовой) отчетности общества, назначение аудиторской организации (индивидуального аудитора) общества и определение размера оплаты ее (его) услуг; - утверждение или принятие документов, регулирующих организацию деятельности общества (внутренних документов общества); - решение вопросов об одобрении сделок, в совершении которых имеется заинтересованность (п. 2.1. ст. 32 Закона об ООО).		

	его заседаний, а также порядок принятия решений (п. 1 ст. 70 Закона об АО). Проведение заседаний коллегиального исполнительного органа общества (правления, дирекции) организует лицо, осуществляющее функции единоличного исполнительного органа общества (п. 2 ст. 70 Закона об АО). Уставом общества, предусматривающим наличие одновременно единоличного и коллегиального исполнительных органов, должна быть определена компетенция коллегиального органа.				
Порядок и простота принятия решений	1. Решения по вопросам, прямо указанным в Законе об АО (ст.48) и ГК РФ (п. 2 ст. 65.3, 67.1) относятся к исключительной компетенции **общего собрания**. Решение на общем собрании акционеров принимается большинством голосов (абз. 1 п. 2, п. 4.2 ст. 49) либо квалифицированным большинством (п. 4 ст. 49 Закона об АО). Решение может быть принято **путем заочного голосования**, т.е. не на заседании (п. 1 ст. 50 Закона об АО)	1. Решения, принимаемые на собрании участников: принимать участие в голосовании могут участники общества или их представители. Также голосовать могут залогодержатель доли в	Общее собрание членов кооператива вправе рассматривать и принимать решение по любому вопросу образования и деятельности кооператива (п. 1 ст. 15 Закон о ПК). Оно правомочно принимать решения, если на нем присутствует более	Большинство решений принимает высший орган союза (как правило, Собрание членов), есть вопросы его исключительной компетенции (п.1 ст.. 123.10 ГК РФ, п. 2 ст. 65.3 ГК РФ).

	В правопорядке существует возможность **отменить принятое на общем собрании Решение**, если такая отмена не имеет признаков злоупотребления правом и совершена до того момента, пока отмененное решение не начало влиять на права и законные интересы третьих (по отношению к участникам собрания) лиц (Определение ВС РФ от 26 апреля 2018 г. N 305-ЭС17-17321). Порядок ведения общего собрания может быть предусмотрен в Уставе АО (п. 5 ст. 49 Закона об АО). *Аспект, осложняющий принятие решений связан* с тем, что общее собрание не вправе принимать решения по вопросам, не включенным в повестку дня собрания, а также изменять повестку дня. Такое требование закона (п. 6 ст. 49 Закона об АО) делает процедуру принятия решений не гибкой, формализованной. Кроме того, всегда высоки риски обжалования принятых решений на собрании ввиду того, что количество акционеров законом не ограничено, а право на обжалование имеется у широкого круга лиц (акционеров, не присутствующих на собрании (п. 7 ст. 49 З об АО), акционеры, голосовавшие против и чьи интересы нарушены и т.д. 2. Единогласным решением участников непубличного общества некоторые вопросы могут быть переданы на рассмотрение **коллегиального органа управления** (пп. 1 п. 3 ст. 66.3 ГК РФ), т.е. Совету директоров.	уставном капитале ООО или доверительный управляющий долей, если по договору они имеют право осуществлять все права участника ООО или право голосовать на собраниях (п. 2 ст. 358.15, п. 1 ст. 1026, п. 1 ст. 1173 ГК РФ, п. 2 ст. 37 Закона об ООО). • Участникам перед проведением ежегодного общего собрания предоставляются отчеты (п. 3 ст. 36, п. 3 ст. 45 Закона об ООО) Решения принимаются большинством не менее двух третей голосов от общего числа голосов участников общества. 2. Решение общего собрания участников общества может быть принято без проведения собрания путем	пятидесяти процентов общего числа членов кооператива. Голосуют простым большинством голосов присутствующих на собрании. Каждый член кооператива **независимо от размера его пая** имеет при принятии решений общим собранием членов кооператива один голос (п. 2 ст. 15 Закон о ПК) Очередное собрание проводится не реже чем 1 раз в год (п. 3 ст. 15), внеочередные созываются Правлением кооператива.	Компетенция органов управления, порядок принимаемых решений, в том числе по вопросам, решения по которым принимаются единогласно или квалифицированным большинством голосов должны содержаться в Уставе союза (п. 2 ст. 123.9 ГК РФ). Решение высшего органа управления некоммерческой организацией может быть принято без проведения собрания или заседания путем проведения **заочного голосования** (опросным путем) (ст. 29 Закона об НКО).

	Ввиду того, что для публичного общества не предусмотрена возможность передать решение вопроса на усмотрение единоличного ИО, порядок принятия решений осложняется. Также, управление акционерным обществом осуществляется его органами, а не просто акционерами. Решения исходят исключительно от органов управления акционерного общества, а не от конкретных лиц. В результате акционеры могут осуществлять свои права на участие в управлении компанией только в рамках тех органов, куда они непосредственно входят.	проведения **заочного голосования** (опросным путем). Такое голосование может быть проведено путем обмена документами посредством почтовой (п. 1 ст. 38 Закона об ООО). 3. В обществе, состоящем из одного участника, решения по вопросам, относящимся к компетенции общего собрания участников общества, принимаются единственным участником общества единолично (ст. 39 Закона об ООО).		
Необходимость одобрения сделок	Общие правила (ст. 79 Закона об АО): Крупные сделки, где речь идет о 25-50% балансовой стоимости активов АО, одобряются Советом директоров (наблюдательным советом). Согласие считается полученным, если решение принято единогласно. Одобрение остальных крупных сделок в АО, а также тех, которые не получили согласия Совета директоров (наблюдательного совета), – компетенция общего собрания акционеров компании.	Совет директоров одобряет крупные сделки и сделки с заинтересованностью (п. 2.1. ст. 32, ст. 45, ст. 46 Закона об ООО). Если не создан Совет директоров, то принятие решения о согласии на совершение сделки	Предусмотрена возможность одобрения сделок кооператива наблюдательным советом или правлением кооператива (п. 4 ст. 17.1 Закон о ПК) – виды сделок, подлежащих одобрению в Законе не конкретизированы, предполагается уточнение в Уставе.	Сделка с заинтересованностью должна быть одобрена органом управления некоммерческой организацией или органом надзора за ее деятельностью (п. 3 ст. 27 Закон об НКО). Иных случаев одобрения Закон об

	Нарушение порядка получения согласия на крупную сделку АО – основание для ее признания недействительной. Оспорить сделку на этом основании могут акционеры (акционер) с 1% и более голосующих акций, член совета директоров и (или) сама компания (п. 6 ст. 79 Закона об АО, ст. 173.1 ГК РФ). Одобрения общего собрания акционеров требуют также сделки с заинтересованностью (ст. 49 Закона об АО). Уставом общества может быть предусмотрена необходимость получения согласия совета директоров (наблюдательного совета) общества или общего собрания акционеров на совершение определенных сделок. При отсутствии такого согласия или последующего одобрения соответствующей сделки она может быть оспорена (п. 2 ст. 69 Закона об АО). Положения уставов хозяйственных обществ, распространяющие порядок одобрения крупных сделок на иные виды сделок, следует рассматривать как **способ установления необходимости получения согласия** совета директоров общества или общего собрания участников (акционеров) на совершение определенных сделок (п. 2 статьи 69 Закона об АО, п.3.1 ст. 40 Закона об ООО) – п. 19 Постановление Пленума Верховного Суда РФ от 26.06.2018 № 27. Сделки, которые совершены за пределами ограничений, предусмотренных как учредительными документами юридического лица, так и иными регулирующими его деятельность документами могут быть признаны	является компетенцией общего собрания участников общества (п. 3 ст. 46 Закона об ООО, п. 4 ст. 45 Закона об ООО). **Уставом** общества может быть предусмотрена необходимость получения согласия Совета директоров (наблюдательного совета) общества или общего собрания участников общества на совершение определенных сделок (п. 3.1 ст. 40 Закона об ООО). **Про сделки с заинтересованностью**: Решение о согласии на совершение сделки, в совершении которой имеется заинтересованность, принимается советом директоров (наблюдательным советом) общества большинством голосов		НКО не предусматривает.

	недействительными. Под иными документами законодатель имеет в виду **внутренние документы ЮЛ** (положения об общем собрании, совете директоров, генеральном директоре) (ст. 174 ГК РФ). В отношении **видов сделок**, особый порядок совершения которых предусмотрен уставом общества, следует отметить, что такие сделки являются существенными для общества и обычно выделяются по следующим параметрам: - исходя из предмета сделки (например, отчуждение недвижимого имущества, основных средств, акций (долей) в уставном капитале других организаций и пр.); - исходя из цены имущества, являющегося предметом сделки, определяемой в соотношении со стоимостью активов хозяйственного общества или в твердой сумме. Кодекс корпоративного управления рекомендует обществам в уставах предусматривать механизмы отнесения к компетенции совета директоров общества вопроса об одобрении сделок, которые не отвечают установленным законодательством критериям крупных сделок, но имеют существенное значение для общества. Например, сделки по продаже акций (долей) подконтрольных обществу юридических лиц, имеющих для него существенное значение, в результате совершения которых общество утрачивает контроль над такими юридическими лицами (п. 307 ККУ).	директоров (если необходимость большего числа голосов не предусмотрена уставом общества), не заинтересованных в ее совершении, или общим собранием участников общества большинством голосов (если необходимость большего числа голосов не предусмотрена уставом общества) от общего числа голосов участников общества, не являющихся заинтересованными в совершении такой сделки или подконтрольными лицам, заинтересованным в ее совершении (п. 4 ст. 45 Закона об ООО).		

	Про сделки с заинтересованностью: В публичном акционерном обществе согласно п. 3 ст. 83 Закона об АО решение о согласии на заключение сделки, в совершении которой имеется заинтересованность, принимается Советом директоров (наблюдательным советом) общества большинством голосов (если необходимость большего числа голосов не предусмотрена уставом общества) директоров, к каждому из которых предъявляются два требования: - директор не должен быть заинтересованным в совершении сделки; - на момент принятия решения и в течение одного года, предшествовавшего его принятию, директор не может являться: 1. лицом, осуществляющим	**Про сделки с заинтересованностью:** В непубличном акционерном обществе решение о согласии на совершение сделки, в совершении которой имеется заинтересованность, принимается советом директоров общества большинством голосов его членов, не заинтересованных в ее совершении (п. 2 ст. 83 Закона об АО). Необходимость большего числа голосов может быть предусмотрена уставом общества. При этом для проведения заседания Совета директоров общества в непубличном акционерном обществе число незаинтересованных директоров должно соответствовать определенному уставом кворуму. Согласно п. 2 ст. 68 Закона об АО кворум не должен составлять менее половины от числа			

	функции единоличного исполнительного органа общества 2. родственником лица, занимающего должности в органах управления управляющей организации общества, управляющей организации общества 3. лицом, контролирующим общество Согласно п. 3.1 ст. 83 Закона об АО для того, чтобы совет директоров публичного акционерного общества мог принимать решение по вопросу о согласовании сделки с заинтересованностью, количество директоров, не заинтересованных в ее совершении и отвечающих требованиям, установленным п. 3 ст. 83, должно быть не менее двух, если большее количество директоров, составляющее кворум для проведения заседания совета директоров публичного общества по	избранных членов совета директоров общества. Пункт 2 ст. 83 Закона об АО устанавливает, что, если количество незаинтересованных директоров составляет менее определенного уставом кворума для проведения заседания совета директоров общества, решение по вопросу о согласовании сделки с заинтересованностью должно приниматься общим собранием акционеров в том же порядке, в каком собрание принимает решение по вопросу о согласовании сделки с заинтересованностью, относящемуся к его компетенции. Уставом непубличного общества может быть установлен отличный от установленного Законом об АО порядка совершения сделок, в совершении которых			

	данному вопросу, не предусмотрено уставом публичного общества. При отсутствии кворума такая сделка потребует согласия общего собрания акционеров на ее совершение.	имеется заинтересованность, либо установлено, что положения главы XI Закона об АО не применяются к этому обществу (п. 8 ст. 83 Закона об АО). **Если в НеПАО отсутствует Совет директоров, то его компетенцию осуществляет Общее собрание акционеров** (ст. 48 Закона об АО, п. 2.1. ст. 48 Закона об АО).			
Раскрытие информации/ Отчетность перед учредителями/ участниками	• Публичное общество обязано раскрывать годовой отчет и бухгалтерскую отчетность, проспект ценных бумаг, сообщение о проведении общего собрания акционеров (п. 1 ст. 92 Закона об АО) • Общество обязано обеспечить акционерам доступ по их требованию к документам, указанным в п. 1 ст. 91 Закона об АО (годовые отчеты, протоколы общих	• Непубличное общество с числом акционеров более пятидесяти обязано раскрывать годовой отчет общества, годовую бухгалтерскую (финансовую) (п.1.1. ст. 92 Закона об АО) • Аналогично, как и в публичных, применяется п. 1 ст. 91 Закона об АО о раскрытии информации перед акционерами • По требованию акционера (акционеров),	• Общество не обязано публиковать отчетность о своей деятельности (ст. 49 Закона об ООО), кроме случая публичного размещения облигаций и иных ценных бумаг • В случае публичного размещения облигаций и иных эмиссионных ценных бумаг общество обязано ежегодно раскрывать годовые отчеты и	• Кооператив обязан обеспечивать членам кооператива доступ к имеющимся у него судебным актам в течение трех дней со дня предъявления соответствующего требования членом кооператива в помещении исполнительного органа кооператива (п. 2 ст. 24 Закон о ПК) • Кооператив ведет бухгалтерский учет и отчетность, а также статистическую отчетность и предоставляет ее органам	• НКО обязаны ежегодно размещать в информационно-телекоммуникационной сети "Интернет" или предоставлять средствам массовой информации для опубликования отчет о своей деятельности в объеме сведений, представляемых в уполномоченный орган или его территориальный

	собраний, списки аффилированных лиц и т.д.) • По требованию акционера (акционеров), владеющего не менее чем 25 процентами голосующих акций общества, общество обязано обеспечить доступ к протоколам заседаний коллегиального исполнительного органа общества и к документам бухгалтерского учета. Уставом Общества может быть предусмотрено меньшее количество акций, необходимых для доступа к указанным документам (п. 5 ст. 91 Закона об АО). В требовании акционера (акционеров), владеющего менее чем 25 процентами голосующих акций общества должна быть указана деловая цель, с которой запрашиваются	владеющего не менее чем одним процентом голосующих акций общества, непубличное общество помимо доступа к информации и документам из п. 2 ст. 91 обязано обеспечить такому акционеру (акционерам) доступ к иным документам, обязанность хранения которых предусмотрена пунктом 1 статьи 89 (Устав Общества, решения Совета директоров, общего собрания) (п. 3 ст. 91 Закона об АО).	годовую бухгалтерскую (финансовую) отчетность (п. 2 ст. 49) • Общество по требованию участника обязано обеспечить ему доступ к следующим документам – п. 2 ст. 50 Закона об ООО (протоколы, док-ты по гос. регистрации и т.д.) • Участники общества вправе участвовать в общем собрании лично или через своих представителей (ст. 37 Закона об ООО).	государственной власти (п.1 ст. 24 Закон о ПК) • Член кооператива имеет право запрашивать информацию от должностных лиц кооператива **по любым вопросам его деятельности** (п. 1 ст. 8 Закон о ПК).	орган (ст. 32 Закон об НКО) • Член ассоциации осуществляет права, предусмотренные Уставом (ст. 123.11 ГК РФ). Согласно п. 34 Приказа Минюста России от 30.06.2023 № 163 «Об утверждении типовых уставов НКО» члены ассоциации вправе получать информацию о деятельности ассоциации (союза) путем направления запроса в Правление.

	документы (п. 4 ст. 91 Закона об АО). • По требованию акционера (акционеров), владеющего не менее чем одним процентом голосующих акций общества, публичное общество обязано обеспечить доступ к следующим информации и документам – информация по сделкам, протоколы заседаний совета директоров, отчеты оценщиков об оценке имущества (п. 2 ст. 91 Закона об АО) • Если стоимость чистых активов общества окажется меньше его уставного капитала более чем на 25 процентов по окончании трех, шести, девяти или двенадцати месяцев отчетного года, следующего за вторым отчетным годом или каждым последующим отчетным годом, по окончании которых стоимость чистых				

	активов общества оказалась меньше его уставного капитала, **общество дважды с периодичностью один раз в месяц обязано поместить в средствах массовой информации уведомление о снижении стоимости чистых активов общества** (п. 7 ст. 35 Закона об АО).				
Контроль за деятельностью компании	Государственный контроль за приобретением акций публичного общества (ст. 84.9 Закона об АО). **Банк России** осуществляет контроль за приобретением ценных бумаг, за их выкупом, за добровольным или обязательным предложением по приобретению бумаг. Локальный контроль за финансово- хозяйственной деятельностью общества осуществляется **ревизионной комиссией** общества в порядке главы XII Закона об АО, путем проверки (ревизии) деятельности компании. **Аудиторская организация** (индивидуальный аудитор) общества проводит аудит годовой бух (финансовой отчетности) в порядке ст. 86 Закона об АО. Совет директоров (наблюдательный совет) публичного общества утверждает внутренние документы общества, определяющие политику общества в области **организации управления рисками и внутреннего контроля** (пп. 9.2 п. 1 ст. 65, п. 1 ст. 87.1 Закона об		Общество для проведения аудита годовой бухгалтерской (финансовой) отчетности общества вправе привлекать **аудиторскую организацию** (ст. 48 Закона об ООО). **Ревизионная комиссия** (ревизор) общества в обязательном порядке проводит проверку годовых отчетов и годовой бухгалтерской (финансовой) отчетности общества до их утверждения общим	В кооперативе с числом членов более пятидесяти может быть создан **наблюдательный совет**, который осуществляет контроль за деятельностью исполнительных органов кооператива (п. 1 ст. 16 Закон о ПК). Решение общего собрания членов кооператива, принятое с нарушением требований Закона и Устава и нарушающее права и (или) законные интересы члена кооператива, может быть признано судом недействительным по заявлению члена	НКО ведет бухгалтерский учет и статистическую отчетность (ст. 32 Закон об НКО). Некоммерческая организация предоставляет информацию о своей деятельности органам государственной статистики и налоговым органам, учредителям и иным лицам (ст. 32 Закон об НКО). Размеры и структура доходов

	АО). Данные документы не относятся к внутренним документам, регулирующим деятельность органов общества (п. 5 Письма Банка России от 15.04.2019 N ИН-06-28/35). Общие принципы и подходы к организации управления рисками и внутреннего контроля, цели и задачи системы управления рисками и внутреннего контроля рекомендуется определить в соответствующем положении (политике) общества (п. 2.2 Рекомендаций от 01.10.2020 N ИН-06-28/143). Иными ключевыми участниками системы управления рисками и внутреннего контроля являются (п. 2.4 Рекомендаций от 01.10.2020 N ИН-06-28/143): • работники и руководители бизнес-подразделений - владельцев рисков, участвующие в бизнес-процессах и управляющие связанными с ними рисками; • работники и руководители структурных подразделений, поддерживающие этих лиц. Например, к ним относятся подразделения по управлению рисками и внутреннему контролю, комплаенс-контролю, охране труда и промышленной безопасности; • работники, осуществляющие внутренний аудит. В неПАО для проведения ревизии финансово-хозяйственной деятельности общества создается **ревизионная комиссия**, за исключением случая, если уставом непубличного общества предусмотрено ее отсутствие (п. 1 ст. 85 Закона об АО). Предполагается,	собранием участников общества (п. 3 ст. 47 Закона об ООО)	кооператива, не принимавшего участия в голосовании или голосовавшего против обжалуемого решения (п. 1 ст. 17.1 Закон о ПК). Ревизионная комиссия или ревизор осуществляют контроль за фин-хоз деятельностью кооператива (п. 1 ст. 18 Закон о ПК).	некоммерческой организации не могут быть предметом коммерческой тайны. НКО обязаны ежегодно представлять в уполномоченный орган документы, содержащие отчет о своей деятельности, о персональном составе руководящих органов и работников, документы о целях расходования денежных средств и использования иного имущества (п. 3 ст. 32 Закон об НКО) + той же нормой предусмотрены внеплановые проверки.

	что именно она отвечает в неПАО за организацию управления рисками. Также, в Законе об АО, в ст. 87.1, также указано на то, что вместе с организацией по управлению рисками ПАО утверждает внутренние документы общества, определяющие политику общества в области организации и осуществления внутреннего аудита. Для неПАО вопрос привлечения **аудиторской организации** также отдается на усмотрение самого Общества и определяется его Уставом (п. 1 ст. 47 Закона об АО), но аудитор также выполняет услуги по управлению рисками и внутреннему контролю (ст. 86 Закона об АО). Кроме того, для неПАО продолжают действовать **рекомендации** п. 258 Кодекса корпоративного управления: для эффективного функционирования системы управления рисками и внутреннего контроля рекомендуется создавать (определить) отдельное структурное подразделение (подразделения) по управлению рисками и внутреннему контролю.			
Формирование имущества компании (капитала)	1. Правоспособность АО в полном объеме возникает не с момента его государственной регистрации, а лишь с момента оплаты 50% акций общества, распределенных среди его учредителей, что установлено п. 3 ст. 2 Закона об АО. 2. Уставный капитал общества составляется из номинальной стоимости акций общества, приобретенных акционерами (ст. 25 Закона об АО). Таким образом, уставный капитал АО **формируется путем первичной эмиссии акций** (первый выпуск	1. Уставный капитал общества составляется из номинальной стоимости долей его участников (п. 1 ст. 14 Закона об ООО). 2. Оплата долей в уставном капитале общества может осуществляться	1. Имущество кооператива образуется за счет паевых взносов членов кооператива, предусмотренных его уставом, прибыли от собственной деятельности, кредитов, имущества, переданного в дар физическими и юридическими лицами, иных	Согласно ст. 26 ФЗ об НКО источниками формирования имущества НКО в денежной и иных формах являются регулярные и единовременные поступления от учредителей (участников, членов);

	после государственной регистрации), т.е. после реализации выпущенных акций первым владельцам. 3. Акции непубличного общества могут быть выпущены в виде цифровых финансовых активов с учетом особенностей и условий, определенных Федеральным законом "О цифровых финансовых активах, цифровой валюте и о внесении изменений в отдельные законодательные акты Российской Федерации" (ст. 25 Закона об АО). 4.Решение об учреждении общества, утверждении его устава и утверждении денежной оценки ценных бумаг, других вещей или имущественных прав либо иных прав, имеющих денежную оценку, вносимых учредителем в оплату акций общества, принимается учредителями единогласно (п. 3 ст. 9 Закона об АО). 5. Если иное не установлено уставом общества, оплата акций при их приобретении осуществляется деньгами (п. 4 ст. 72 Закона об АО). Устав общества может содержать ограничения на виды имущества, которым могут быть оплачены акции общества **(п. 2 ст. 34 Закона об АО)** При оплате дополнительных акций неденежными средствами денежная оценка имущества, вносимого в оплату акций, производится Советом директоров (наблюдательным советом) общества с привлечением оценщика (п. 3 ст. 34 Закона об АО). 6. Уставом непубличного общества могут быть установлены ограничения количества акций, принадлежащих одному акционеру, и их суммарной номинальной стоимости, а также максимального числа голосов, предоставляемых одному акционеру (ст. 11 Закона об АО). 7. Внесение в устав общества изменений и дополнений, связанных с увеличением (уменьшением)	деньгами, ценными бумагами, другими вещами или имущественными правами либо иными имеющими денежную оценку правами (п. 1 ст. 15 Закона об ООО). Уставом общества могут быть установлены виды имущества, которое не может быть внесено для оплаты долей в уставном капитале общества. 3. Общество имеет в собственности обособленное имущество, учитываемое на его самостоятельном балансе, может от своего имени приобретать и осуществлять имущественные и личные неимущественные права (п. 2 ст. 2 Закона об ООО). 4. Уставом общества может быть	допускаемых законодательством источников (ст. 9 Закона о ПК) 2. Имущество, находящееся в собственности кооператива, делится на паи его членов в соответствии с уставом кооператива. 3. Пай члена кооператива состоит из паевого взноса члена кооператива и соответствующей части чистых активов кооператива (за исключением неделимого фонда) (ст. 9 Закон о ПК). 4. Паевым взносом члена кооператива могут быть деньги, ценные бумаги, иное имущество, в том числе и имущественные права, а также иные объекты гражданских прав (п. 2 ст. 9 Закон о ПК). Уставом кооператива может быть установлено, что определенная часть принадлежащего кооперативу имущества составляет неделимый фонд кооператива, используемый в целях, определяемых уставом кооператива. Имущество,	добровольные имущественные взносы и пожертвования; выручка от реализации товаров, работ, услуг; дивиденды (доходы, проценты), получаемые по акциям, облигациям, другим ценным бумагам и вкладам; доходы, получаемые от собственности некоммерческой организации. Имущество, которое передано ассоциации или союзу его учредителями (участниками), является собственностью самого объединения (ассоциации и союза). Такой же режим установлен законом и в отношении имущества, приобретенного ассоциацией (союзом)

	номинальной стоимости акций общества, в том числе изменений, связанных с увеличением (уменьшением) уставного капитала общества, консолидацией или дроблением акций общества, осуществляется на основании решения, принятого общим собранием акционеров, и зарегистрированных изменений, внесенных в решение о выпуске акций общества, а в случаях, предусмотренных законодательством РФ о несостоятельности (банкротстве), зарегистрированного отчета об итогах выпуска акций общества (п. 2 ст. 12 Закона об АО). 8. Акции общества, распределенные при его учреждении, **должны быть полностью оплачены в течение года** с момента государственной регистрации общества, если меньший срок не предусмотрен договором о создании общества. Не менее 50 процентов акций общества, распределенных при его учреждении, должно быть оплачено в течение трех месяцев с момента государственной регистрации общества (п. 1 ст. 34 Закона об АО).		ограничен максимальный размер доли участника общества. Уставом общества может быть ограничена возможность изменения соотношения долей участников общества (п. 3 ст. 14 Закона об ООО).	составляющее неделимый фонд кооператива, не включается в паи членов кооператива.	по иным основаниям (п. 3 ст. 213 ГК, п. 1 ст. 24 Закон об НКО).
Минимальный размер капитала	Минимальный размер уставного капитала ПАО составляет 100 тыс. руб. (ст. 26 Закона об АО).	Минимальный уставный капитал непубличного общества должен составлять десять тысяч рублей (ст. 26 Закона об АО).	Размер уставного капитала общества должен быть не менее чем десять тысяч рублей (п. 1 ст. 14 ФЗ об ООО).	Паевой фонд кооператива определяет минимальный размер имущества кооператива, гарантирующего интересы его кредиторов. Паевой фонд должен быть полностью сформирован в течение первого года деятельности кооператива (п. 3 ст. 10 Закона о ПК) – конкретный размер не установлен.	Не менее минимального размера уставного капитала, предусмотренного для обществ с ограниченной ответственностью (п. 5 ст. 50 ГК РФ) – т.е. не менее десяти тысяч рублей.

Существует ли возможность уменьшения/ увеличения капитала?	Уставный капитал общества может быть **увеличен** путем увеличения номинальной стоимости акций или размещения дополнительных акций (п. 1 ст. 28 Закона об АО). Общество вправе, а в случаях, предусмотренных Законом об АО, обязано **уменьшить** свой уставный капитал (ст. 29 Закона об АО). Например, после того как общество приобрело размещенные им акции, оно должно их реализовать по цене не ниже их рыночной стоимости не позднее одного года с даты их приобретения. Если реализовать не получилось, общее собрание акционеров обязано принять решение об уменьшении уставного капитала путем погашения указанных акций (п. 3 ст. 72, п. 6 ст. 76, п. 1 ст. 34 Закона об АО). Аналогичные правила предусмотрены ст. 100 ГК РФ.	Общее собрание участников общества может принять решение об **увеличении уставного капитала** общества за счет внесения дополнительных вкладов участниками общества (ст. 17, п. 1 ст. 19 Закона об ООО). При увеличении уставного капитала общества пропорционально увеличивается номинальная стоимость долей всех участников общества без изменения размеров их долей (п. 3 ст. 18). **Уменьшение уставного капитала** общества может осуществляться путем уменьшения номинальной стоимости долей всех участников общества в уставном капитале	Общее собрание членов кооператива обязано объявить **об уменьшении размера паевого фонда** кооператива, если по окончании второго или каждого последующего года стоимость чистых активов окажется меньше стоимости паевого фонда кооператива, и зарегистрировать это уменьшение в установленном порядке (п. 4 ст. 10 Закон о ПК).	Прямого указания в законодательстве не имеется. Исходя из того, что в НКО природа уставного капитала **– членский взнос**, возможность увеличения его или уменьшения в том понимании, что это имеет место быть в коммерческих организациях, отсутствует.

			общества и (или) погашения долей, принадлежащих обществу (ст. 20 Закона об ООО). Общество вправе, а в случаях, предусмотренных настоящим Федеральным законом, обязано уменьшить свой уставный капитал.		
Порядок приобретения/ отчуждение/ обмена доли/ акции	**Приобретение и отчуждение:** Свободная продажа акций третьим лицам без чьего-либо согласия (ст. 7 Закона об АО, п. 5 ст. 97 ГК РФ). Публичное общество вправе проводить размещение акций и эмиссионных ценных бумаг, конвертируемых в его акции, посредством открытой подписки (п. 2 ст. 7 Закона об АО). Для ПАО существует **обязательное или добровольное предложение о приобретении акций**	**Приобретение**: Акции непубличного общества и эмиссионные ценные бумаги, конвертируемые в его акции, не могут размещаться посредством открытой подписки или иным образом предлагаться для приобретения неограниченному кругу лиц (п. 2 ст. 7 Закона об АО). **Отчуждение**: Акционер, намеренный осуществить отчуждение своих акций третьему лицу, обязан известить об этом непубличное	**Приобретение:** Каждый учредитель общества должен оплатить полностью свою долю в уставном капитале. Освобождение его от этой обязанности не допускается (ст. 16). В случае неполной оплаты доли в уставном капитале общества в течение 4 месяцев с момента государственной регистрации общества, неоплаченная часть доли переходит к обществу (п. 3 ст. 16 Закона об ООО).	**Приобретение и отчуждение:** Член кооператива вправе передать свой пай или его часть другому члену кооператива. Передача пая влечет за собой прекращение членства в кооперативе. Порядок передачи закрепляется в Уставе. Применяются правила о преимущественном праве и получении согласия иных членов кооператива при передаче пая лицу, не входящему в кооператив (ст. 9 Закон о ПК).	**Отчуждение**: Членство в ассоциации (союзе) **неотчуждаемо** (п. 3 ст. 123.11 ГК РФ). Член ассоциации (союза) вправе выйти из нее по своему усмотрению в любое время. В случае выхода из состава учредителей и (или) участников последнего либо единственного учредителя и (или) участника он обязан до направления сведений о своем выходе в рег. орган

	публичного общества (ст. 84.1 и 84.2 Закона об АО), когда лицо, намеревающееся приобрести или которое уже приобрело более 30 процентов общего количества акций публичного общества, принадлежащих этому лицу и его аффилированным лицам, в течение 35 дней с момента внесения соответствующей приходной записи по лицевому счету (счету депо) или с момента, когда это лицо узнало или должно было узнать о том, что оно самостоятельно или совместно с его аффилированными лицами владеет указанным количеством таких акций, **обязано** (или **вправе**, если только намеревается приобрести) направить акционерам - владельцам остальных акций соответствующих категорий (типов) и	общество, устав которого предусматривает преимущественное право приобретения отчуждаемых акций (п. 4 ст. 7 Закона об АО). **Соответственно, если Устав не предусматривает преимущественного права, то уведомлять никого не нужно.** В течение 2 дней об этом уведомляются все акционеры. Акционер вправе осуществить отчуждение акций третьему лицу при условии, что другие акционеры общества и (или) общество не воспользуются преимущественным правом приобретения всех отчуждаемых акций в течение двух месяцев со дня получения извещения обществом. Если отчуждение акций осуществляется по договору купли-продажи,	**Отчуждение:** Участник общества вправе продать или осуществить отчуждение иным образом своей доли или части доли в уставном капитале общества одному или нескольким участникам данного общества. Доля участника общества может быть отчуждена до полной ее оплаты только в части, в которой она оплачена. Перед продажей участник обязан известить остальных участников о своем намерении, чтобы у них была возможность реализовать преимущественное право (п. 5 ст. 21 Закона об ООО). В случае выхода участника Общество обязано выплатить ему действительную	Выход или исключение из кооператива не являются основанием для одностороннего прекращения или изменения взаимоотношений члена кооператива и кооператива по поводу переданного имущества, если иное не предусмотрено соглашением сторон (п. 5 ст. 9 Закон о ПК). Лицу, прекратившему членство в кооперативе, **выплачивается стоимость пая или выдается имущество**, - это и для ООО нужно прописать, там эта часть отсутствует… соответствующее его паю, а также производятся другие выплаты, предусмотренные уставом кооператива (п. 7 ст. 22 Закон о ПК). **Исключение из кооператива**: В уставе кооператива должны определяться основания и порядок исключения из членов кооператива (п. 2 ст. 5 Закона о ПК)	передать свои права учредителя и (или) участника другому лицу в соответствии с федеральным законом и уставом юридического лица (п. 3 ст. 15 Закона об НКО). **Приобретение**: Устав некоммерческой организации должен предусматривать порядок вступления (принятия) членов (участников) в состав некоммерческой организации (п. 3 ст. 14 Закона об НКО). **Исключение из Ассоциации**: К исключительной компетенции высшего органа управления некоммерческой организацией относится определение порядка исключения из состава ее

	владельцам эмиссионных ценных бумаг, конвертируемых в такие акции**, публичную оферту о приобретении у них таких ценных бумаг.** **Обмен**: **Уставом** непубличного общества в отношении определенных категорий (типов) акций могут быть предусмотрены порядок их обмена на доли участников в уставном капитале общества с ограниченной ответственностью, доли или вклады в складочном капитале хозяйственного товарищества либо паи членов производственного кооператива, создаваемых в результате реорганизации общества. **Исключение акционера**: Нельзя исключить акционера из ПАО (п. 1 ст. 67 ГК РФ)	такое отчуждение должно осуществляться по цене и на условиях, которые сообщены обществу. Срок осуществления преимущественного права, предусмотренный уставом общества, не может быть менее чем 10 дней со дня получения извещения обществом. **Исключение акционера**: В непубличных обществах участник вправе требовать **исключения другого участника из общества** в судебном порядке с выплатой ему действительной стоимости его доли участия, если такой участник своими действиями (бездействием) причинил существенный вред обществу либо иным образом существенно затрудняет его деятельность и достижение целей, ради которых оно создавалось, в том числе грубо нарушая свои	стоимость его доли или части доли в уставном капитале общества либо выдать ему в натуре имущество такой же стоимости в течение трех месяцев со дня возникновения соответствующей обязанности, если иной срок или порядок выплаты действительной стоимости доли или части доли не предусмотрен уставом общества (п. 6 ст. 23 Закона об ООО). **Обмен долей**: Общее собрание участников общества принимает решение о реорганизации и о порядке обмена долей (п. 2 ст. 56 Закона об ООО). **Исключение участника**:	Член правления кооператива может быть исключен из кооператива по решению общего собрания в связи с членством в аналогичном кооперативе. Член кооператива, исключенный из него, имеет право на получение пая и других выплат, предусмотренных уставом кооператива (п. 2 ст. 106.5 ГК РФ).	учредителей (участников, членов) (п. 3 ст. 29 Закона об НКО).

		обязанности, предусмотренные законом или учредительными документами общества (п. 1 ст. 67 ГК РФ).	Допускается исключение участника, если он причинил существенный вред товариществу или обществу либо иным образом существенно затрудняет его деятельность и достижение целей, ради которых оно создавалось, в том числе грубо нарушая свои обязанности, предусмотренные законом или учредительными документами товарищества или общества (п. 1 ст. 67 ГК РФ).		
	Порядок обмена акций в акционерных обществах устанавливается в Уставе (ст. 15,20 Закона об АО)- обычно, решение о конвертации в акции другого общества или порядок обмена на доли участников в уставном капитале ООО принимается общим собранием акционеров.				
Преимущественное право выкупа доли/ акции	В ПАО **акционерам не может быть предоставлено преимущественное право** приобретения акций, отчуждаемых акционером третьим лицам (п. 5 ст. 97 ГК РФ).	Уставом непубличного общества **<u>может быть предусмотрено</u> преимущественное право приобретения** его акционерами акций, отчуждаемых по возмездным сделкам другими акционерами или самим Обществом, по цене предложения третьему лицу или по	Участники общества **пользуются преимущественным правом** покупки доли или части доли участника общества по цене предложения третьему лицу или по отличной от цены предложения третьему лицу и заранее	Члены кооператива пользуются преимущественным правом покупки такого пая (его части) (п. 4 ст. 9 Закон о ПК).	Не предусмотрено законодательством.

		цене, порядок определения которой установлены уставом общества (ст. 7 Закона об АО). При отчуждении акций непубличного общества с нарушением преимущественного права акционеры, имеющие такое преимущественное право, либо само общество, если его уставом предусмотрено преимущественное право приобретения им акций, в течение трех месяцев со дня, когда акционер общества либо общество узнали или должны были узнать о данном нарушении, вправе потребовать в судебном порядке перевода на них прав и обязанностей приобретателя.	определенной уставом общества цене пропорционально размерам своих долей, , **если уставом общества не предусмотрен иной порядок** осуществления преимущественного права покупки доли или части доли. (п. 4 ст. 21 Закона об ООО).		
Обязательность согласия	Уставом ПАО не может быть предусмотрена необходимость получения	Уставом непубличного общества может быть предусмотрена	Участник общества вправе продать или осуществить	Передача пая (его части) гражданину, не являющемуся членом	Физические и (или) юридические лица вправе войти в состав

участников на отчуждение/ приобретение доли/ акции	чьего-либо согласия на отчуждение акций этого общества (п. 5 ст. 97 ГК РФ).	необходимость получения согласия акционеров на отчуждение акций третьим лицам (ст. 41 Закона об АО, ст. 7 Закона об АО).	отчуждение иным образом своей доли или части доли в уставном капитале общества одному или нескольким участникам данного общества. **Согласие других участников общества или общества на совершение такой сделки не требуется**, если иное не предусмотрено уставом общества (п. 2 ст. 21 Закона об ООО). **Уставом** общества может быть предусмотрена необходимость согласия участников на продажу долей **третьим лицам,** на принятие в состав участников наследников (правопреемников) (п. 3, 6 ст. 93 ГК РФ).	кооператива, допускается лишь с согласия кооператива (п. 4 ст. 9 Закон о ПК), т.е. **Общего собрания членов** кооператива (п. 3 ст. 106.5 ГК РФ).	учредителей (участников) некоммерческой корпорации **с согласия других учредителей и (или) участников** (п. 4 ст. Закона об НКО), если иное не предусмотрено Уставом НКО.
Право выкупа компанией	Общество вправе приобретать размещенные им акции по решению общего собрания акционеров об уменьшении уставного капитала общества путем приобретения части размещенных акций в целях		Общество не вправе приобретать доли или части долей в своем уставном капитале, за	Право выкупа отсутствует. Член кооператива может на договорных началах	Не предусмотрено законодательством, так как собственником

собственных долей/ акций	сокращения их общего количества, если это предусмотрено уставом общества (п. 1 ст. 72 Закона об АО). Акционеры - владельцы голосующих акций вправе требовать выкупа обществом всех или части принадлежащих им акций (ст. 75 Закона об АО) в случаях, указанных в статье (принятие решения о реорганизации, согласия и одобрения сделки и тд).	исключением случаев, предусмотренных настоящим ФЗ (п. 1 ст. 23 Закона об ООО). Общество может стать владельцем доли в отдельных случаях (п. 3 ст. 15, п. 3 ст. 16, п. 4 ст. 23 Закона об ООО). Например, в случае прекращения у общества права пользования имуществом до истечения срока, на который такое имущество было передано в пользование обществу для оплаты доли, участник общества, передавший имущество, обязан предоставить обществу по его требованию денежную компенсацию. В случае непредоставления в установленный срок компенсации доля или часть доли в уставном капитале общества, пропорциональные неоплаченной сумме	передавать принадлежащие ему материальные ценности и иные средства **кооперативу** (П. 5 ст. 9 Закона о ПК). При отказе бывшего члена кооператива выплатить задолженность добровольно кооператив вправе взыскать ее в установленном порядке (п. 2 ст. 22 Закон о ПК).	членских взносов и так является сама ассоциация (союз).

		(стоимости) компенсации, переходят к обществу (п. 3 ст. 15 Закона об ООО). Или же в случае неполной оплаты доли в уставном капитале общества в течение 4 месяцев с момента гос. регистрации общества, неоплаченная часть доли переходит к обществу. В случае, если уставом общества отчуждение доли или части доли, принадлежащих участнику общества, третьим лицам запрещено и другие участники общества отказались от их приобретения либо не получено согласие на отчуждение доли или части доли участнику общества или третьему лицу при условии, что необходимость получить такое согласие предусмотрена уставом		

		общества, **общество обязано приобрести по требованию участника общества принадлежащие ему долю или часть доли** (п. 2 ст. 23 Закона об ООО). Участник, желающий выйти из ООО, вправе потребовать приобретения Обществом его доли (п. 3, 6 ст. 93 ГК РФ). Цена приобретения обществом доли будет равна действительной стоимости доли участника в уставном капитале общества, определенную на основании данных бухгалтерской отчетности общества за последний отчетный период, предшествующий дню обращения участника общества с соответствующим требованием, или с согласия участника общества выдать ему в		

			натуре имущество такой же стоимости (п. 2 ст. 23 Закона об ООО).		
Права и обязанности участников/ учредителей компании	**Не допускается возлагать на акционеров дополнительные обязанности**, помимо тех, что предусмотрены ГК РФ (п. 7 ст. 7 Закона об АО). **Права акционеров** владельцев обыкновенных и привилегированных акций общества перечислены в ст. 31, 32 Закона об АО. **Права акционеров-владельцев обыкновенных акций общества**: Каждая обыкновенная акция общества предоставляет акционеру - ее владельцу одинаковый объем прав. Акционеры - владельцы обыкновенных акций общества могут в соответствии с Законом об АО и уставом общества участвовать в общем собрании акционеров с правом голоса по всем вопросам его компетенции, а также имеют право на	Допускается возложение на акционеров **дополнительных обязанностей**, помимо тех, что предусмотрены ГК РФ для всех участников хозяйственных обществ (п. 7 ст. 7 Закона об АО). Права участников НеПАО предусмотрены ст. 65.2 ГК РФ, ст. 65.3 ГК РФ, ст. 31 Закона об АО и должны содержаться также в его уставе: - право на участие в высшем органе управления НеПАО - общем собрании акционеров НеПАО (п. 1 ст. 65.2 ГК РФ) - право быть избранным в состав совета директоров (наблюдательного совета) НеПАО, в том	**Права участников** (ст. 8 Закона об ООО): - участвовать в управлении делами общества; - получать информацию о деятельности ООО и знакомиться с его документами бухгалтерского учета и иной документацией - принимать участие в распределении прибыли - продать или осуществить отчуждение иным образом своей доли или части доли в уставном капитале общества одному или нескольким участникам данного общества либо другому лицу - получить в случае ликвидации общества часть имущества, оставшегося после расчетов с	**Права членов кооператива**: - передавать свой пай другому члену или третьему лицу с согласия иных членов (п. 4 ст. 9 Закон о ПК) - член кооператива, права и интересы которого нарушены решением общего собрания членов кооператива, вправе обжаловать это решение в суд; - член кооператива вправе по своему усмотрению выйти из него, предупредив в письменной форме председателя (правление) кооператива не позднее чем за две недели. **Член кооператива обязан** внести к моменту государственной регистрации кооператива не менее чем десять процентов паевого взноса (п. 1 ст. 10 Закон о ПК).	**Член союза осуществляет корпоративные права**, предусмотренные п. 1 ст. 65.2 ГК РФ, а также имеет право на равных началах с другими членами пользоваться безвозмездно оказываемыми ассоциацией услугами (ст. 123.11 ГК РФ). Член ассоциации (союза) вправе выйти из нее по своему усмотрению в любое время. **Члены союза обязаны** уплачивать предусмотренные уставом членские взносы и по решению высшего органа ассоциации (союза)

	получение дивидендов, а в случае ликвидации общества - право на получение части его имущества. **Права акционеров-владельцев привилегированных акций общества**: Акционеры - владельцы привилегированных акций общества не имеют права голоса на общем собрании акционеров. Акционеры - владельцы привилегированных акций участвуют в общем собрании акционеров с правом голоса при решении вопросов о реорганизации и ликвидации общества, о внесении в устав изменений, исключающих указание на то, что общество является публичным, а также вопросов, решение по которым принимается единогласно всеми акционерами общества. **Акционерным соглашением** признается договор об осуществлении прав, удостоверенных акциями, и (или) об	числе в случаях, когда уставом предусмотрено образование совета директоров в НеПАО с числом акционеров менее пятидесяти - Отметим, что п. 2 ст. 31 Закона об АО также предусмотрено, что акционеры - владельцы обыкновенных акций общества могут в соответствии с данным Законом и уставом общества участвовать в общем собрании акционеров с правом голоса по всем вопросам его компетенции.	кредиторами, или его стоимость - выйти из общества путем отчуждения своей доли обществу, если такая возможность предусмотрена уставом общества, или потребовать приобретения обществом доли. **Обязанности участников** (ст. 9 Закона об ООО) - оплачивать доли в уставном капитале общества - не разглашать информацию о деятельности общества, в отношении которой установлено требование об обеспечении ее конфиденциальности. Помимо прав, предусмотренных Законом об ООО, устав общества может предусматривать **иные права**	Для членов кооперативов **законодательством априори возложены дополнительные обязанности**, к числу которым относится обязанность лично участвовать в трудовой деятельности кооператива (п. 2 ст. 8 Закон о ПК).	вносить дополнительные имущественные взносы в имущество ассоциации (союза) (ст. 123.11 ГК РФ).

	особенностях осуществления прав на акции (п. 2 ст. 32.1 Закона об АО).		**(дополнительные права**) участника (участников) общества (п. 2 ст. 8 Закона об ООО). Учредители (участники) вправе заключить **Договор об осуществлении прав участников** общества, по которому они обязуются осуществлять определенным образом свои права и (или) воздерживаться (отказываться) от осуществления указанных прав (п. 3 ст. 8 Закона об ООО). Устав может предусматривать дополнительные обязанности участников (п. 2 ст. 9 Закона об ООО).		
	! Учредители общества могут заключить **корпоративный договор**, в котором они конкретизируют, в том числе, свои собственные права и обязанности (п. 5 ст. 9 Закона об АО)				

Распределение прибыли	Между акционерами прибыль распределяется в виде **дивидендов** (п. 3 ст. 42 Закона об АО). Решение о выплате (объявлении) дивидендов принимается общим собранием акционеров. **Указанным решением должны быть определены** размер дивидендов по акциям каждой категории (типа), форма их выплаты, порядок выплаты дивидендов в неденежной форме, дата, на которую определяются лица, имеющие право на получение дивидендов. В свою очередь в **Уставе общества изначально должны быть определены** размер дивиденда и (или) стоимость, выплачиваемая при ликвидации общества (ликвидационная стоимость) по привилегированным акциям каждого типа.	В непубличных АО решение о выплате промежуточных дивидендов может принимать Совет директоров при наличии соответствующих полномочий в Уставе. (п. 2.1 ст. 48 Закона об АО). Если в НеПАО отсутствует Совет директоров, то решение принимает общее собрание акционеров (пп.11.1) п. 1 ст. 48 Закона об АО, п. 2.1. ст. 48 Закона об АО).	Прибыль распределяется между участниками пропорционально доле в уставном капитале общества (п. 2 ст. 28 Закона об ООО). В ООО Уставом общества или корпоративным договором может быть предусмотрен иной порядок распределения прибыли – не пропорционально доле участия в уставном капитале (п. 1 ст. 66 ГК РФ, ст. 28 Закона об ООО).	Прибыль кооператива распределяется между его членами в соответствии с их личным трудовым и (или) иным участием, размером паевого взноса, а между членами кооператива, не принимающими личного трудового участия в деятельности кооператива, соответственно размеру их паевого взноса. По решению общего собрания членов кооператива часть прибыли кооператива может распределяться между его наемными работниками (п. 1 ст. 12 ФЗ о ПК). Но данное правило не императивно, Уставом кооператива может предусматриваться иной порядок распределения прибыли вне зависимости от трудового участия (п. 3 ст. 106.3 ГК РФ).	Полученная некоммерческой организацией прибыль не подлежит распределению между участниками (членами) некоммерческой организации (п. 3 ст. 26 Закона об НКО).
Ответственность участников/ учредителей по	Акционеры не отвечают по обязательствам общества и несут риск убытков, связанных с его деятельностью, в пределах стоимости принадлежащих им акций (п. 1 ст. 2 Закона об АО).		Участники общества не отвечают по его обязательствам и несут риск убытков, связанных с деятельностью	Субсидиарная ответственность членов кооператива по обязательствам кооператива определяется в порядке, предусмотренном уставом	Члены ассоциации (союза) не отвечают по ее обязательствам, за исключением случаев, если законом или уставом

долгам компании	Акционеры, не полностью оплатившие акции, несут солидарную ответственность по обязательствам общества в пределах неоплаченной части стоимости принадлежащих им акций (ст. 96 ГК РФ). Если несостоятельность (банкротство) общества вызвана действиями (бездействием) его акционеров или других лиц, которые имеют право давать обязательные для общества указания либо иным образом имеют возможность определять его действия, то на указанных акционеров или других лиц в случае недостаточности имущества общества может быть возложена субсидиарная ответственность по его обязательствам. (п. 3 ст. 3 Закона об АО).	общества, в пределах стоимости принадлежащих им долей в уставном капитале общества (п. 1 ст. 2 Закона об ООО). Участники не отвечают по долгам общества, **за исключением случаев:** - по вине контролирующего участника общество доведено до банкротства (абз. 2 п. 3 ст. 6 Закона о банкротстве); -ответственность участника общества по сделкам общества, совершенным во исполнение указаний участника (абз. 2 п. 3 ст. 6 Закона об ООО, абз. 2 п. 2 ст. 67.3 ГК РФ); - ответственность участников за неполную оплату уставного капитала (п. 4 ст. 66.2 ГК РФ, п. 1 ст. 2 Закона об ООО).	кооператива (ст. 13 Закон о ПК). Обращение взыскания на пай члена кооператива по его личным долгам допускается лишь при недостатке иного имущества для покрытия таких долгов в порядке, предусмотренном уставом кооператива. Уставом кооператива должна быть предусмотрена ответственность члена кооператива за нарушение им обязательства по внесению паевого взноса (п. 2 ст. 10 Закон о ПК). ! Член производственного кооператива, **который внес дополнительный паевой** взнос, тем самым компенсировал кооперативу свое "неучастие" личным трудом в деятельности кооператива, **не освобождается от субсидиарной ответственности** по долгам кооператива (п. 2 ст. 8 Закон о ПК).	ассоциации (союза) предусмотрена субсидиарная ответственность ее членов (ст. 123.8 ГК РФ). Члены ассоциации (союза) несут субсидиарную ответственность по обязательствам этой ассоциации (союза) в размере и в порядке, предусмотренных ее учредительными документами (п. 4 ст. 11 Закона об НКО).

		В случае оплаты долей в уставном капитале общества неденежными средствами участники общества и независимый оценщик солидарно несут при недостаточности имущества общества субсидиарную ответственность по его обязательствам в размере завышения стоимости имущества, внесенного для оплаты долей в уставном капитале общества в течение трех лет с момента государственной регистрации общества (ст. 15 Закона об ООО).		
Обязанность участников/ учредителей по докапитализации	В АО существует **инситут вкладов в имущество общества**. Акционеры на основании договора с обществом имеют право в целях финансирования и поддержания деятельности общества в любое время вносить в имущество общества безвозмездные вклады в денежной или иной форме, которые не увеличивают уставный капитал общества и не изменяют номинальную стоимость акций (ст. 32.2 Закона об АО). Уставом непубличного общества может быть предусмотрено, что решением общего собрания	Участники общества обязаны, если это предусмотрено уставом общества, по решению общего собрания вносить вклады в имущество общества (ст. 27 Закона об ООО). Вклады в имущество общества вносятся	Член кооператива может на договорных началах передавать принадлежащие ему материальные ценности и иные средства кооперативу. Выход или исключение из кооператива не являются основанием для одностороннего прекращения или изменения взаимоотношений члена	Члены ассоциации (союза) обязаны уплачивать предусмотренные уставом членские взносы и по решению высшего органа ассоциации (союза) вносить **дополнительные** имущественные

	акционеров непубличного общества на акционеров общества **может быть возложена обязанность по внесению вкладов в имущество общества**, а также могут быть предусмотрены порядок, основания и условия внесения вкладов в имущество общества (п. 3 ст. 32.2 Закона об АО). Уставом непубличного общества может быть предусмотрено, что по решению общего собрания акционеров допускается возложение обязанности по внесению вкладов в имущество непубличного общества только на акционеров - **владельцев акций определенной категории (типа).**	всеми участниками общества пропорционально их долям в уставном капитале общества (ст. 27 Закона об ООО).	кооператива и кооператива по поводу переданного имущества, если иное не предусмотрено соглашением сторон (п. 5 ст. 9 Закон о ПК).	взносы в имущество ассоциации (союза) (п. 2 ст. 123.11 ГК РФ). Предусмотрена экономическая поддержка НКО в различных формах (ст. 31 Закона об НКО).