СТАНДАРТ БАНКА РОССИИ

СТО БР ИББС-1.4-2018

ОБЕСПЕЧЕНИЕ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ ОРГАНИЗАЦИЙ БАНКОВСКОЙ СИСТЕМЫ РОССИЙСКОЙ ФЕДЕРАЦИИ

УПРАВЛЕНИЕ РИСКОМ НАРУШЕНИЯ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ ПРИ АУТСОРСИНГЕ

Дата введения: 2018-07-01

Издание официальное

Москва
2018

Предисловие

ПРИНЯТ И ВВЕДЕН в действие приказом Банка России от 6 марта 2018 года № ОД-568.

Содержание

Введение

В настоящее время в деятельности отдельных организаций банковской системы (БС) Российской Федерации (РФ) отмечается тенденция и экономическая потребность на передачу выполнения отдельных собственных бизнес-функций на основании договорных отношений сторонним (внешним) организациям, специализирующимся на предоставлении соответствующих услуг, – поставщикам услуг.

Основными причинами и целями передачи выполнения бизнес-функций организаций БС РФ поставщикам услуг (целями аутсорсинга), как правило, являются:

- содействие оптимизации и повышению эффективности деятельности организации БС РФ;
- оптимизация затрат и повышение эффективности деятельности организаций БС РФ, в том числе связанных с выполнением непрофильных (вспомогательных) бизнес-функций;
- повышение прозрачности бизнеса для уточнения его стоимости при совершении сделок с акциями (долями);
- привлечение внешних специалистов, обладающих необходимой квалификацией, компетенцией, знаниями и опытом работы в областях, которые являются вспомогательными или непрофильными для организаций БС РФ;
- снижение зависимости от ресурсных ограничений, в первую очередь финансовых и кадровых, для выполнения вспомогательных или непрофильных бизнес-функций.

Одними из основных видов бизнес-функций, которые рассматриваются организациями БС РФ в качестве приоритетных для возможной передачи на аутсорсинг, являются:

- функции, связанные с применением информационных технологий, обслуживанием и администрированием средств вычислительной техники (далее – СВТ), серверного и телекоммуникационного оборудования, устройств самообслуживания, с разработкой программного обеспечения;
- административные функции, включая функции, связанные с финансовой деятельностью, функционалом back-офиса, call-центра, организационным и административным обеспечением;
- функции, связанные с хранением и обработкой информации, в том числе на внешних центрах обработки данных и облачных сервисах (облачных службах);
- функции обеспечения информационной безопасности (ИБ) организации БС РФ;
- административно-хозяйственные функции.

Несмотря на то что привлечение поставщиков услуг для аутсорсинга призвано способствовать повышению эффективности реализации бизнес-функций при сокращении затрат на их реализацию, в большинстве случаев передача выполнения бизнес-функций приводит к появлению новых рисков в деятельности организаций БС РФ, включая риски нарушения ИБ. Передача выполнения бизнес-функций на аутсорсинг не снимает обязанности и не переносит ответственности организаций БС РФ, включая вопросы обеспечения ИБ, предусмотренные законодательством РФ, в том числе нормативно-правовыми актами РФ, нормативными актами Банка России (далее при совместном упоминании – законодательство РФ).

Основными факторами нового риска нарушения ИБ при аутсорсинге являются:

- возникновение зависимости процессов обеспечения ИБ от деятельности поставщика услуг;
- возникновение зависимости устойчивости (непрерывности) выполнения бизнес-функций организации БС РФ от возможных сбоев и отказа объектов информационной инфраструктуры поставщика услуг в результате реализации угроз ИБ;
- недостаточный уровень организации поставщиком услуг систем обеспечения ИБ;
- неверная оценка ресурсов, возможностей (кадровых, финансовых, технических) и потенциала поставщика услуг, необходимых для выполнения взятых на себя обязательств по обеспечению ИБ при реализации бизнес-функций организаций БС РФ;
- наличие в соглашении об аутсорсинге положений, реализация которых приведет к возникновению ограничений в деятельности организаций БС РФ;
- возникновение зависимости выполнения бизнес-функций организации БС РФ от эффективности деятельности поставщика услуг и добросовестности выполнения соглашения об уровне услуг (SLA).

Указанные факторы порождают риск нарушения ИБ, к которому относятся следующие риски:

- риск бесконтрольного несанкционированного доступа к защищаемой информации при реализации бизнес-функций лицами, не являющимися работниками организаций БС РФ;
- риск несанкционированного проведения операций, имеющих финансовые последствия как для организаций БС РФ, так для их клиентов и контрагентов;
- риск потери контроля над реализацией и уровнем зрелости процессов обеспечения ИБ и как следствие – риск потери контроля над уровнем обеспечения ИБ и киберустойчивости [1];
- риск нарушения бесперебойности бизнес-функций;

– риск несоблюдения требований законодательства РФ в области обеспечения ИБ, в том числе в части обеспечения режимов защиты банковской тайны и персональных данных (ПДн).

Указанные риски нарушения ИБ могут реализоваться в виде инцидентов ИБ, имеющих значимые финансовые или репутационные последствия, например:

– прерывание организациями БС РФ предоставления финансовых услуг[1] на неприемлемый для организации период времени;
– несанкционированные переводы денежных средств, в том числе в крупных объемах;
– несоблюдение требований законодательства РФ в области обработки информации ограниченного доступа [2], в том числе ПДн и информации, составляющей банковскую тайну, инсайдерскую информацию, коммерческую тайну и другие виды тайн (далее – защищаемая информация).

Организациям БС РФ необходимо учитывать, что в ряде случаев ущерб от реализации указанных рисков не может быть компенсирован поставщиком услуг в рамках заключенных договорных отношений. В частности, ущерб от несанкционированного перевода денежных средств может составлять остаток на корреспондентском счете организации БС РФ, открытом в расчетном центре платежной системы, который в ряде случаев сопоставим с капиталом организации БС РФ.

В связи с этим организациям БС РФ при привлечении для аутсорсинга поставщиков услуг следует обеспечить реализацию механизмов управления и контроля риска нарушения ИБ, создающую основу для обеспечения соответствия уровня риска нарушения ИБ при передаче бизнес-функций на аутсорсинг уровню риска, принятому самостоятельно организацией БС РФ.

Для достижения цели управления и контроля риска нарушения ИБ при аутсорсинге настоящий стандарт устанавливает базовые требования к управлению риском нарушения ИБ, включая требования:

– к содержанию задач и зоне ответственности руководства организаций БС РФ при реализации управления и контроля риска нарушения ИБ при аутсорсинге;
– к оценке риска нарушения ИБ при аутсорсинге существенных функций, в том числе при принятии решения о передаче бизнес-функций на аутсорсинг;
– к оценке возможности поставщика услуг обеспечить должный уровень ИБ при выполнении бизнес-функций и наличию внутренней компетенции организации БС РФ для проведения такого рода оценки;
– к содержанию соглашений о передаче выполнения бизнес-функций на аутсорсинг;
– к содержанию мероприятий по контролю обеспечения непрерывности деятельности поставщиком услуг при реализации бизнес-функций организаций БС РФ в части обеспечения ИБ;
– к содержанию мероприятий по постоянному мониторингу и контролю рисков нарушения ИБ при аутсорсинге;
– к составу и содержанию мероприятий по проведению периодического внешнего аудита обеспечения ИБ при аутсорсинге существенных функций;
– к организации аутсорсинга процессов обеспечения ИБ.

[1] В частности, прерывание услуг по переводу денежных средств на период более двух часов или незавершение выполнения расчетов в течение рабочего дня.

СТО БР ИББС-1.4-2018

СТАНДАРТ БАНКА РОССИИ

ОБЕСПЕЧЕНИЕ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ ОРГАНИЗАЦИЙ БАНКОВСКОЙ СИСТЕМЫ РОССИЙСКОЙ ФЕДЕРАЦИИ

УПРАВЛЕНИЕ РИСКАМИ НАРУШЕНИЯ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ ПРИ АУТСОРСИНГЕ

Дата введения: 2018-07-01

1. Область применения

Настоящий стандарт распространяется на организации БС РФ, передающие на постоянной (непрерывной) основе на длительный срок выполнение следующих бизнес-функций (процессов) сторонним (внешним) организациям – поставщикам услуг, в рамках которых возникает новый риск нарушения ИБ:

– при выполнении которых осуществляется обработка информации, защищаемой в соответствии с требованиями законодательства РФ [2–4], несанкционированный доступ к которой, раскрытие (распространение), несанкционированное (неавторизованное) изменение, уничтожение (потеря) и (или) хищение создают условия для возникновения убытков организации БС РФ, ее клиентов или контрагентов, в том числе условия для совершения финансовых операций от имени клиентов;
– ненадлежащее выполнение которых поставщиком услуг создает условия для реализации или реализует инциденты ИБ.

Настоящий стандарт среди прочего распространяется на случай аутсорсинга, при котором:

– поставщик услуг является поднадзорной Банку России организацией или не является таковой;
– поставщику услуг передаются функции, связанные с обеспечением ИБ, выполнение которых регулируется и контролируется Банком России в зоне его компетенции, определенной законодательством РФ.

Целью стандарта является установление требований к управлению и контролю риска нарушения ИБ при аутсорсинге, выполнение которых создает основу для обеспечения соответствия уровня риска нарушения ИБ при передаче бизнес-функций на аутсорсинг уровню риска нарушения ИБ, принятому самостоятельно организацией БС РФ, а также основу для уменьшения такого риска.

Настоящий стандарт рекомендован для применения путем включения ссылок на него и (или) прямого использования устанавливаемых в нем положений во внутренних документах организаций БС РФ, а также в соглашениях (контрактах, пакетах договорных документов) с поставщиками услуг.

Настоящий стандарт не распространяется на случаи:

– разовой передачи организацией БС РФ выполнения своих бизнес-функций сторонним (внешним) организациям – поставщикам услуг;
– привлечения организацией БС РФ сторонних (внешних) организаций – поставщиков услуг для обслуживания организации БС РФ, в том числе направленного на повышение качества услуг и (или) расширение перечня услуг, сопутствующих банковским операциям, осуществляемым организацией БС РФ для своих клиентов (например, привлечение удостоверяющих центров, платежных агентов).

Положения настоящего стандарта носят рекомендательный характер, если только обязательность применения отдельных из них не установлена законодательством РФ.

Обязательность применения настоящего стандарта может быть установлена договорами и соглашениями, заключенными организациями БС РФ, или решением организаций БС РФ о присоединении к настоящему стандарту.

Положения настоящего стандарта предназначены и могут быть использованы кредитными организациями, некредитными финансовыми организациями, указанными в части первой статьи 76.1 Федерально-

го закона “О Центральном банке Российской Федерации (Банке России)”, а также субъектами национальной платежной системы.

2. Нормативные ссылки

В настоящем стандарте использованы нормативные ссылки на стандарт Банка России “Обеспечение информационной безопасности организаций банковской системы Российской Федерации. Общие положения” СТО БР ИББС-1.0-2014.

3. Термины и определения

Аутсорсинг – передача организацией БС РФ на основании договора на длительный срок сторонней (внешней) организации – поставщику услуг выполнения бизнес-функций организации БС РФ, которые являются необходимыми для ее деятельности и которые в обычных условиях (без привлечения поставщика услуг) осуществлялось бы организацией БС РФ самостоятельно.

Примечание: отличительными характеристиками аутсорсинга, рассматриваемыми в настоящем стандарте, которые отличают аутсорсинг от других форм оказания услуг, являются:

– передача полностью выполнения бизнес-функций поставщику услуг без участия в реализации указанных бизнес-функций работников организации БС РФ;
– передача поставщику услуг выполнения бизнес-функций на постоянной (непрерывной) основе на длительный период времени (например, не менее 1 года).

При этом под аутсорсингом не понимается привлечение организацией БС РФ сторонних (внешних) организаций – поставщиков услуг в следующих случаях:

– разовой передачи организацией БС РФ выполнения своих бизнес-функций сторонним (внешним) организациям – поставщикам услуг;
– привлечения организацией БС РФ сторонних (внешних) организаций – поставщиков услуг для обслуживания организации БС РФ, в том числе направленного на повышение качества услуг и (или) расширение перечня услуг, сопутствующих банковским операциям, осуществляемым организацией БС РФ для своих клиентов (например, привлечение удостоверяющих центров, платежных агентов).

Поставщик услуг – обслуживающая организация, специализирующаяся на предоставлении услуг, которой организации БС РФ передают выполнение своих бизнес-функций на аутсорсинг.

Примечание: поставщиком услуг может выступать как аффилированное в пределах банковской группы юридическое лицо, так и юридическое лицо, которое является внешним по отношению к банковской группе, привлекаемым для выполнения на постоянной (непрерывной) основе определенных бизнес-функций организации БС РФ, выполнение которых в обычных условиях (без привлечения поставщика услуг) осуществлялось бы организацией БС РФ самостоятельно.

Услуга – деятельность поставщика услуг по выполнению бизнес-функций организаций БС РФ, переданных на аутсорсинг.

Существенные функции в части ИБ; существенные функции – бизнес-функции организации БС РФ:

1) при выполнении которых осуществляется обработка защищаемой информации, несанкционированный доступ к которой, раскрытие (распространение), несанкционированное (неавторизованное) изменение, уничтожение (потеря) и (или) хищение создают условия для возникновения убытков организации БС РФ, ее клиентов или контрагентов, в том числе условия для совершения финансовых операций от имени клиентов (далее – обработка защищаемой информации);

2) невыполнение или ненадлежащее выполнение которых поставщиком услуг создают условия для реализации или реализуют инциденты ИБ, связанные:

– с нарушением непрерывности предоставления организацией БС РФ финансовых услуг[2] (далее – нарушение непрерывности предоставления финансовых услуг);
– с утечкой защищаемой информации; с совершением операций, имеющих финансовые последствия, в том числе переводов денежных средств, лицами, не обладающими соответствующими правами;
– с несоблюдением организациями БС РФ требований к обеспечению ИБ, установленных законодательством РФ.

Аутсорсинг существенных функций в части ИБ; аутсорсинг существенных функций – аутсорсинг бизнес-функций, которые отнесены к существенным.

---

[2] В частности, прерывание предоставления услуг по переводу денежных средств на период более двух часов или незавершение выполнения расчетов в течение рабочего дня.

Соглашение об уровне услуг (SLA, Service Level Agreement) – соглашение между организацией БС РФ и поставщиком услуг, описывающее определенные полномочия и услугу, а также целевые показатели уровня услуги, зоны ответственности сторон – организации БС РФ и поставщика услуг.

4. Обозначения и сокращения

РФ – Российская Федерация;
БС – банковская система;
ИБ – информационная безопасность;
ИТ – информационные технологии;
ПДн – персональные данные;
СВТ – средства вычислительной техники;
СВР – степень возможности реализации риска нарушения ИБ;
СТП – степень тяжести последствий от реализации риска нарушения ИБ;
SLA – соглашение об уровне услуг (Service Level Agreement);
НСД – несанкционированный доступ.

5. Риск нарушения информационной безопасности при аутсорсинге существенных функций

5.1. Организациям БС РФ при аутсорсинге существенных функций следует рассматривать следующие факторы нового риска нарушения ИБ:

- возникновение зависимости процессов обеспечения ИБ от деятельности поставщика услуг;
- возникновение зависимости устойчивости (непрерывности) выполнения бизнес-функций организаций БС РФ от возможных сбоев и отказа объектов информационной инфраструктуры поставщика услуг в результате реализации угроз ИБ;
- ненадлежащий уровень организации поставщиком услуг систем обеспечения ИБ;
- неверная оценка ресурсов, возможностей (кадровых, финансовых, технических) и потенциала поставщика услуг, необходимых для выполнения взятых на себя обязательств по обеспечению ИБ при реализации бизнес-функций организаций БС РФ;
- возникновение зависимости выполнения бизнес-функций организаций БС РФ от эффективности деятельности поставщика услуг и добросовестности выполнения соглашения об уровне услуг (SLA);
- наличие в соглашении об аутсорсинге положений, реализация которых приведет к возникновению ограничений в деятельности организаций БС РФ, которые в том числе могут быть связаны:
  - с досрочным односторонним прекращением поставщиком услуг обеспечения дополнительного уровня ИБ при предоставлении услуг аутсорсинга;
  - с ограничением возможности контроля деятельности поставщика услуг и получения необходимой информации для контроля риска нарушения ИБ;
  - с недостаточным уровнем обеспечения ИБ и ненадлежащим управлением риском нарушения ИБ в случае недостаточной детализации в соглашении обязанностей поставщика услуг;
  - с зависимостью реализации обеспечения ИБ от содержания и качества деятельности лиц, не являющихся работниками организаций БС РФ;
  - с расширением состава внутренних нарушителей безопасности информации, обладающих легально предоставленными правами логического и (или) физического доступа.

5.2. При аутсорсинге существенных функций факторы, указанные в пункте 5.1 настоящего стандарта, создают новый риск нарушения ИБ, который должен управляться и контролироваться организацией БС РФ.

Основные виды риска нарушения ИБ организаций БС РФ, связанные с аутсорсингом существенных функций, и возможные последствия от его реализации приведены в таблице 1.

Таблица 1. Виды операционных рисков и возможные последствия для организаций БС РФ от их реализации при аутсорсинге существенных функций

Вид риска организаций БС РФ	Последствия для организаций БС РФ от реализации риска
Операционный риск, связанный с несоблюдением требований законодательства РФ (правовой риск)	Несоблюдение требований законодательства РФ в области обработки защищаемой информации; несоблюдение законодательства РФ в области обеспечения защиты информации; несоблюдение законодательства РФ в обеспечении непрерывности предоставления финансовых услуг в результате реализации угроз ИБ; возникновение ограничений на способность организации БС РФ предоставить необходимую и достоверную информацию Банку России и уполномоченным органам исполнительной власти в рамках выполнения надзорных (контрольных) мероприятий в области обеспечения защиты информации
Операционный риск, связанный с потерей (невозможностью) контроля обеспечения ИБ поставщиком услуг	Политика обеспечения ИБ поставщика услуг может не совпадать с политикой обеспечения ИБ организации БС РФ, а деятельность поставщика услуг в части обеспечения ИБ может осуществляться с учетом собственных интересов; потеря организацией БС РФ контроля над уровнем риска нарушения ИБ и уровнем зрелости реализации поставщиком услуг процессов обеспечения ИБ; отсутствие возможности и необходимой компетенции у организации БС РФ обеспечить надлежащий контроль деятельности поставщика услуг в части обеспечения ИБ при аутсорсинге существенных функций
Операционный риск, связанный с возможностью прерывания деятельности организации БС РФ в результате реализации угроз ИБ	Нарушение непрерывности предоставления финансовых услуг в случае реализации сбоев и отказа в работе информационной инфраструктуры поставщика услуг или в работе информационной инфраструктуры организации БС РФ в результате деятельности поставщика услуг; нарушение непрерывности предоставления финансовых услуг в случае реализации сбоев и отказа в обслуживании технических средств и систем защиты информации в результате действий поставщика услуг; возникновение уязвимостей защиты информации в результате действий поставщика услуг
Операционный риск, связанный с реализацией инцидентов ИБ, имеющих последствия для организации БС РФ	Нарушение непрерывности предоставления финансовых услуг; утечка информации конфиденциального характера; хищение материальных носителей, содержащих объекты интеллектуальной собственности; совершение несанкционированных операций, имеющих финансовые последствия, в том числе переводов денежных средств, лицами, не обладающими соответствующими правами
Операционный риск, связанный с возникновением зависимости от поставщика услуг	Отказ поставщика услуг от выполнения своих обязательств по обеспечению ИБ перед организацией БС РФ, в том числе предусмотренных соглашением об аутсорсинге существенных функций; возникновение неприемлемых финансовых затрат у организации БС РФ в случае отказа поставщика услуг от своих обязательств; утрата у работников организации БС РФ необходимых компетенций, знаний и навыков, необходимых для обеспечения ИБ при возврате выполнения существенных функций с использованием собственных ресурсов; невозможность обеспечить необходимый уровень ИБ при возврате выполнения бизнес-функций в течение периода времени, приемлемого для организации БС РФ; увеличение временных затрат на выполнение бизнес-функций, связанное с территориальной удаленностью поставщика услуг (при нахождении на большом расстоянии от организации БС РФ или в другом часовом поясе); снижение гибкости в обеспечении ИБ при выполнении бизнес-функций, связанное с выполнением поставщиком услуг только тех требований, которые установлены соглашением об аутсорсинге
Операционный риск, связанный со снижением качества услуг по обеспечению ИБ, предоставляемых поставщиком услуг	Снижение лояльности и удовлетворенности клиентов и контрагентов организации БС РФ; снижение лояльности, удовлетворенности и продуктивности сотрудников организации БС РФ

6. Основные требования к управлению риском нарушения информационной безопасности при аутсорсинге существенных функций

6.1. Настоящий стандарт определяет ряд основных требований, основанных на положениях документа Базельского комитета по банковскому надзору при Банке международных расчетов “Аутсорсинг в сфере финансовых услуг” [5], адаптированных для цели управления риском нарушения ИБ и контроля над ним при аутсорсинге существенных функций.

Реализация указанных ниже основных требований с учетом дальнейших положений настоящего стандарта способствует применению взвешенного подхода к передаче организациями БС РФ выполнения бизнес-функций поставщикам услуг на основе оценке объема потенциального риска нарушения ИБ.

При определении основных требований к управлению риском нарушения ИБ в настоящем стандарте предполагается, что аутсорсинг существенных функций может привести к повышению общего отраслевого системного риска нарушения ИБ, который может оказать существенное влияние не только на деятельность отдельной организации БС РФ, но и на стабильность функционирования БС РФ в целом.

На аутсорсинг не могут передаваться функции, связанные с выбором требуемого уровня защищенности, а также функции, связанные с принятием рисков нарушения ИБ.

6.2. Основное требование 1. В случае планирования передачи выполнения бизнес-функций поставщикам услуг на аутсорсинг организации БС РФ следует установить политику в отношении аутсорсинга существенных функций (далее – политика аутсорсинга).

Политика аутсорсинга должна среди прочего однозначно определять:

– возможность аутсорсинга бизнес-функций, при выполнении которых осуществляется обработка защищаемой информации;
– возможность аутсорсинга бизнес-функций, невыполнение или ненадлежащее выполнение которых поставщиком услуг создает условия для реализации или реализует инциденты ИБ;
– возможность аутсорсинга только в случае соблюдения требований законодательства РФ в области обработки ПДн и информации, составляющей банковскую тайну, в частности возможность аутсорсинга в случае надлежащего получения соглашения субъектов ПДн [4];
– возможность аутсорсинга только в случае соблюдения требований законодательства РФ в области защиты информации;
– возможность аутсорсинга только в случае отсутствия прямых или косвенных ограничений на реализацию полномочий Банка России и уполномоченных органов исполнительной власти в рамках выполнения надзорных (контрольных) мероприятий в части вопросов защиты информации;
– возможность аутсорсинга только в случае реализации организацией БС РФ надлежащего управления риском нарушения ИБ и контроля над ним.

Политика аутсорсинга существенных функций должна быть принята советом директоров (наблюдательным советом) организации БС РФ, а в случае его отсутствия – исполнительным органом организации БС РФ.

В отношении аутсорсинга существенных функций организация БС РФ должна реализовать процедуры внутреннего контроля соответствия принятой политики аутсорсинга, результаты которого должны рассматриваться советом директоров (наблюдательным советом) организации БС РФ.

6.3. Основное требование 2. Организация БС РФ должна разработать, применять и обеспечить контроль программы аутсорсинга, предусматривающей вопросы управления риском нарушения ИБ (далее – программа аутсорсинга).

Программа аутсорсинга должна определять:

– состав и содержание мероприятий по управлению риском нарушения ИБ при аутсорсинге существенных функций;
– состав и содержание мероприятий по мониторингу и контролю деятельности поставщика услуг по обеспечению ИБ при аутсорсинге существенных функций;
– возможность привлечения поставщиком услуг субподрядчиков при оказании услуг аутсорсинга, а также требования к таким субподрядчикам.

В части мероприятий по управлению риском нарушения ИБ и контролю над ним программа аутсорсинга должна определять:

– задачи и зоны ответственности исполнительного органа организации БС РФ для цели реализации управления риском нарушения ИБ и контроля над ним при аутсорсинге;
– требования к составу и содержанию мероприятий по оценке организацией БС РФ риска нарушения ИБ при принятии решения о передаче бизнес-функций на аутсорсинг;
– требования к составу и содержанию мероприятий по оценке организацией БС РФ возможности поставщика услуг обеспечить должный уровень ИБ при аутсорсинге существенных функций и по обеспечению наличия внутренней компетенции организации БС РФ для проведения такого рода оценки;

– требования к содержанию соглашений, связанных с передачей выполнения бизнес-функций на аутсорсинг.

В части состава и содержания мероприятий по мониторингу и контролю деятельности поставщика услуг программа аутсорсинга должна определять:

– требования к составу и содержанию мероприятий по контролю обеспечения непрерывности деятельности поставщиков услуг при реализации бизнес-функций организации БС РФ в части обеспечения ИБ;
– требования к составу и содержанию мероприятий по постоянному мониторингу и контролю риска нарушения ИБ при аутсорсинге.

Организация БС РФ должна реализовать контроль выполнения программы аутсорсинга, в том числе со стороны службы ИБ и службы внутреннего контроля, а также контроль со стороны исполнительного органа организации БС РФ.

6.4. Основное требование 3. Организация БС РФ должна обеспечить выполнение своих обязательств перед клиентами и контрагентами, а также возможность проведения эффективного контроля выполнения требований в области защиты информации со стороны Банка России и уполномоченных органов исполнительной власти в рамках выполнения надзорных (контрольных) мероприятий в области защиты информации.

Организации БС РФ рекомендуется реализовать:

– регламентацию и применение организационных мер и технических средств, реализующих контроль доступа работников поставщика услуг и иных лиц к защищаемой информации, а также информационным (автоматизированным) обрабатывающим ее системам;
– обязательное сохранение за организацией БС РФ функций управления предоставлением доступа к защищаемой информации, а при технической невозможности (например, при использовании облачных вычислений по модели SaaS) – контроль выполнения функций по управлению предоставлением доступа к защищаемой информации поставщиком услуг.

Привлечение поставщиков услуг для выполнения работ не должно оказывать влияния на законодательно закрепленные права клиентов по отношению к организации БС РФ, включая право на возврат денежных средств при использовании электронного средства платежа без согласия клиента, установленное статьей 9 Федерального закона от 27 июня 2011 года № 161-ФЗ “О национальной платежной системе” [3].

6.5. Основное требование 4. Исполнительный орган организации БС РФ должен определить критерии, в том числе основанные на законодательстве РФ о лицензировании отдельных видов деятельности [6–8], которые должны использоваться для оценки способности и потенциала поставщика услуг эффективно и качественно обеспечить ИБ при предоставлении услуги по аутсорсингу существенных функций, в том числе обеспечить защиту информации в соответствии с требованиями законодательства РФ.

В случае несоответствия поставщика услуг соответствующим критериям ему не могут передаваться на выполнение существенные функции.

6.6. Основное требование 5. Организации БС РФ следует привлекать поставщиков услуг для аутсорсинга существенных функций только после принятия поставщиком услуг всех необходимых мер по обеспечению ИБ и заключения соглашения, определяющего детальные условия и разграничение ответственности по обеспечению ИБ.

Детализация условий по обеспечению ИБ в соглашении должна обеспечивать возможность проведения оперативных мероприятий по мониторингу и контролю со стороны организации БС РФ деятельности поставщика услуг в части обеспечения ИБ.

Детальные требования к содержанию соглашения об аутсорсинге существенных функций установлены в разделе 9 настоящего стандарта, а примерный перечень вопросов, которые могут использоваться для оценки поставщика услуг в части обеспечения ИБ, приведен в Приложении 2.

При заключении соглашения с поставщиками услуг на осуществление аутсорсинга существенных функций организации БС РФ следует обеспечить наличие следующих условий по обеспечению ИБ:

– обязанность поставщика услуг обеспечить соблюдение требований к защите информации, установленных для организации БС РФ, в том числе требований, установленных в рамках законодательства о национальной платежной системе [3, 9, 10], а также в области защиты персональных данных [4, 11, 12];
– составление перечня защищаемой информации, передаваемой на обработку и (или) хранение поставщику услуг;
– разграничение ответственности между организацией БС РФ и поставщиком услуг в части обеспечения ИБ;
– наличие у поставщика услуг лицензий по оказываемым видам деятельности в соответствии с законодательством о лицензировании отдельных видов деятельности [6–8];
– наличие у поставщика услуг, связанных с обработкой данных платежных карт, свидетельства о соответствии требованиям стандарта PCI DSS;

– сохранение права организации БС РФ на контроль выполнения организацией БС РФ самостоятельно или с привлечением внешнего аудитора, определяемого организацией БС РФ, условий соглашения в части выполнения обязанностей по обеспечению ИБ, соблюдение порядка и (или) процедуры выполнения указанного контроля;
– обязанность поставщиков услуг уведомлять организации БС РФ об инцидентах, связанных с обеспечением ИБ, соблюдение порядка и (или) процедуры выполнения указанного уведомления.

6.7. Основное требование 6. В программе аутсорсинга исполнительный орган организации БС РФ должен определить требования к проведению мероприятий, связанных с обеспечением непрерывности деятельности поставщиков услуг при аутсорсинге бизнес-функций организаций БС РФ в части обеспечения ИБ.

Организации БС РФ следует учитывать, что наличие и использование ограниченного числа поставщиков услуг, предоставляющих услуги аутсорсинга многим организациям БС РФ, реализует концентрацию операционного риска, что является системной угрозой для БС РФ в целом. С целью своевременного выявления концентрации операционного риска, связанного с передачей многими организациями БС РФ выполнения существенных бизнес-функций ограниченной группе поставщиков услуг, Банк России рекомендует организациям БС РФ уведомлять ФинЦЕРТ Банка России (info_fincert@cbr.ru) о планируемой передаче выполнения бизнес-функций. Информирование осуществляется в форме электронных сообщений.

6.8. Основное требование 7. Организация БС РФ должна рассматривать бизнес-функции, передаваемые на аутсорсинг поставщику услуг, в качестве неотъемлемой части своей деятельности, в том числе подпадающей под регулирование в части защиты информации со стороны уполномоченных органов исполнительной власти РФ и Банка России.

При аутсорсинге существенных функций организация БС РФ должна обеспечить выполнение своих обязательств по предоставлению возможности контроля соблюдения требований к защите информации, установленных в рамках законодательства о национальной платежной системе [3, 9, 10], персональных данных [4, 11, 12] и безопасности критической информационной инфраструктуры [13], со стороны уполномоченных органов исполнительной власти РФ и Банка России (в пределах их полномочий, установленных законодательством РФ), в том числе обеспечить доступ к информации, связанной с деятельностью поставщика услуг.

6.9. Основное требование 8. Организации БС РФ при принятии решения об аутсорсинге существенных функций, при котором предполагается трансграничная передача защищаемой информации, следует убедиться в соблюдении требований:
– законодательства РФ, регулирующего вопросы трансграничной передачи персональных данных [14];
– законодательства РФ, устанавливающего обязанность обработки и хранения персональных данных на территории РФ [15];
– нормативных актов Банка России, устанавливающих обязанность кредитных организаций создавать и передавать Банку России резервные копии электронных баз данных, а также размещать резервные копии электронных баз данных на территории РФ [16];
– законодательства РФ, регулирующего вопросы лицензирования отдельных видов деятельности [6–8];
– законодательства РФ, регулирующего вопросы обеспечения безопасности критической информационной инфраструктуры [13].

В случае наличия у поставщика услуг подразделений и (или) дочерних предприятий за пределами РФ, а также при использовании самим поставщиком услуг аутсорсинга поставщик услуг должен предоставить организации БС РФ информацию о таких подразделениях, предприятиях или аутсорсинговых субподрядчиках (если они участвуют в оказании услуг аутсорсинга), выполняемых ими работах, часовых поясах и странах, в которых находятся их штаб-квартиры и из которых они ведут свою деятельность в целях выполнения соглашения об аутсорсинге для организации БС РФ. Необходимо учитывать возможность существования своих законодательных требований и ограничений, а также используемых разговорных языках и возможных культурных и религиозных особенностях в области обеспечения ИБ в юрисдикциях, в которых находятся поставщики услуг, их подразделения, дочерние предприятия и субподрядчики.

Трансграничная передача информации, составляющей банковскую тайну, допускается в обезличенной обобщенной (агрегированной) форме, за исключением случаев, установленных законодательством РФ.

7. Оценка риска нарушения информационной безопасности при аутсорсинге существенных функций

7.1. Аутсорсинг существенных функций организации БС РФ должен сопровождаться оценкой, надлежащим управлением и контролем организации БС РФ в отношении риска нарушения ИБ, реализуемыми в соответствии с политикой аутсорсинга.

7.2. Реализация организацией БС РФ программы аутсорсинга должна предусматривать следующие мероприятия:

– идентификация потенциального риска нарушения ИБ при аутсорсинге существенных функций, в том числе из видов риска, определенных в разделе 5 настоящего стандарта;
– оценка потенциального риска нарушения ИБ при аутсорсинге существенных функций;
– принятие решения о возможности аутсорсинга на основе результатов оценки риска нарушения ИБ;
– реализация последующего постоянного мониторинга и контроля уровня риска нарушения ИБ.

Ключевым фактором для реализации программ аутсорсинга является оценка потенциального риска нарушения ИБ, а также обеспечение возможности последующего мониторинга и контроля его уровня.

Идентификацию риска нарушения ИБ следует проводить на основе анализа состава бизнес-функций, планируемых к передаче на аутсорсинг, а также на основе анализа факторов нового риска нарушения ИБ, определенных в разделе 5 настоящего стандарта.

7.3. Для оценки потенциального риска нарушения ИБ и обеспечения возможности мониторинга и контроля его уровня организации БС РФ следует определить состав и проводить оценку (в том числе периодическую) показателей (метрик), характеризующих:

– степень возможности реализации риска нарушения ИБ (далее – СВР) в результате наличия факторов нового риска, приведенного в разделе 5 настоящего стандарта;
– степень тяжести последствий от реализации риска нарушения ИБ (далее – СТП) для реализации бизнес-функций организации БС РФ, переданных на аутсорсинг.

7.4. В качестве показателей (метрик), характеризующих СВР, организации БС РФ рекомендуется (среди прочих) рассмотреть использование следующих:

– оценка соблюдения требований законодательства РФ в области:
  • обеспечения защиты информации, обработки ПДн и информации, содержащей банковскую тайну;
  • обеспечения непрерывности предоставления финансовых услуг;
  • обеспечения возможности организации БС РФ предоставить необходимую и достоверную информацию в рамках выполнения Банком России и уполномоченными органами исполнительной власти их надзорных (контрольных) функций;
– характеристика достижения целей обеспечения ИБ организации БС РФ;
– характеристика потенциала организации БС РФ, необходимого для контроля риска нарушения ИБ при аутсорсинге существенных функций;
– характеристика, определяющая требования к непрерывности предоставления финансовых услуг;
– характеристика, определяющая необходимый уровень защиты информации в соответствии с требованиями, установленными законодательством РФ;
– характеристика, определяющая наличие и функциональность системы обеспечения ИБ поставщика услуг;
– характеристика потенциала организации БС РФ, необходимого для обеспечения ИБ существенных функций после прекращения действия соглашения с поставщиком услуг или в случае отказа поставщика услуг от выполнения своих обязательств.

7.5. В качестве показателей (метрик), характеризующих СТП, организации БС РФ следует (среди прочих) рассмотреть использование следующих:

– общая сумма операций по переводу денежных средств, включая электронные денежные средства, осуществляемых через организацию БС РФ с использованием электронных технологий, связанных с бизнес-функцией, переданной на аутсорсинг;
– среднеквартальный остаток денежных средств, находящихся на корреспондентских счетах организации БС РФ, открытых в расчетных центрах платежных систем, в том числе в платежной системе Банка России;
– характеристика, определяющая уровень операционных расходов:
  • операционные расходы (убытки) организации БС РФ, связанные с нарушением непрерывности предоставления финансовых услуг в результате НСД к ее информационной инфраструктуре или информационной инфраструктуре поставщика услуг;
  • операционные расходы (убытки), связанные с совершением операций, имеющих финансовые последствия, в том числе переводов денежных средств, лицами, не обладающими соответствующими правами;
  • операционные расходы (убытки) организации БС РФ в результате НСД к объектам ее информационной инфраструктуры, используемой для осуществления переводов денежных средств, или в результате использования электронных средств платежа без согласия клиентов;
  • неприемлемые финансовые затраты организации БС РФ в случае отказа поставщика услуг от своих обязательств;

- невозможность организовать должный уровень обеспечения ИБ в случае необходимости возврата выполнения существенных функций в течение периода времени, приемлемого для организации БС РФ.

7.6. В качестве источников данных для показателя СВР могут быть использованы следующие оценки:

– собственная (экспертная) оценка организации БС РФ, выполненная ее работниками, обладающими необходимыми знаниями, опытом и компетенцией;
– оценка, выполненная аудиторской или консалтинговой организацией (независимой от поставщика услуг), обладающей необходимым опытом и компетенцией;
– оценка, выполненная на основе результатов проведения поставщиком услуг внешнего независимого аудита на соответствие применимым документам в области стандартизации, в первую очередь национальным стандартам РФ, разрабатываемым Банком России, отраслевым стандартам Банка России или иным применимым национальным стандартам РФ и международным стандартам, гармонизированным в установленном порядке в РФ (в том числе в соответствии с ГОСТ 57580.1-2017 “Безопасность финансовых (банковских) операций. Защита информации финансовых организаций. Базовый набор организационных и технических мер” [17]).

7.7. Организации БС РФ следует выбирать те источники данных для оценки показателей СВР и СТП, которые смогут обеспечить наиболее достоверную и полную информацию для оценки риска нарушения ИБ при аутсорсинге существенных функций.

Выбор указанных показателей и источников их получения должен обеспечить возможность оценки наличия правовой возможности и экономической целесообразности при принятии решения об аутсорсинге существенных функций, а также возможности осуществления деятельности по должному мониторингу и контролю риска нарушения ИБ при аутсорсинге существенных функций.

Организации БС РФ следует учитывать, что определение показателей (факторов), характеризующих СВР и СТП, является ключевым элементом оценки, управления и контроля в отношении риска нарушения ИБ.

В качестве основы для выработки подходов к оценке риска нарушения ИБ может быть рекомендован подход, определенный в таблице 2.

Таблица 2. Рекомендации по определению и использованию показателей (факторов) риска нарушения ИБ при аутсорсинге существенных функций
(методика оценки риска определяется организацией БС РФ самостоятельно на основе Рекомендаций в области стандартизации Банка России (РС БР ИББС-2.2-2009) "Обеспечение информационной безопасности организаций банковской системы Российской Федерации. Методика оценки рисков нарушения информационной безопасности")

Тип операционного риска	Возможная характеристика СВР	Возможный источник получения оценки СВР	Возможная характеристика СТП	Принятие решения о возможности аутсорсинга
Связанный с несоблюдением требований законодательства РФ (правовой)	Оценка соблюдения требований законодательства РФ в области: – обеспечения защиты информации, обработки ПДн и информации, содержащей банковскую тайну; – обеспечения непрерывности предоставления финансовых услуг; – обеспечения возможности организации БС РФ предоставить необходимую и достоверную информацию в рамках выполнения Банком России и уполномоченными органами исполнительной власти их надзорных (контрольных) функций в области защиты информации	Собственная оценка организации БС РФ, выполненная ее работниками; оценка, выполняемая консалтинговой организацией (независимой от поставщика услуг)	Наличие риска несоблюдения законодательства РФ	Однозначная невозможность передачи выполнения существенных функций на аутсорсинг; аутсорсинг существенных функций невозможен
Связанный с потерей (невозможностью) контроля обеспечения ИБ поставщиком услуг	Оценка достижения целей обеспечения ИБ организации БС РФ; оценка потенциала организации БС РФ обеспечить контроль риска нарушения ИБ при аутсорсинге существенных функций	Собственная оценка организации БС РФ, выполненная ее работниками; оценка, выполняемая аудиторской или консалтинговой организацией (независимой от поставщика услуг)	Общая сумма операций по переводу денежных средств, включая электронные денежные средства, осуществляемых через организацию БС РФ с использованием электронных технологий; среднеквартальный остаток денежных средств, находящихся на корреспондентских счетах организации БС РФ, открытых в расчетных центрах платежных систем, в том числе в платежной системе Банка России; операционные расходы (убытки) организации БС РФ, связанные с нарушением непрерывности предоставления финансовых услуг в результате НСД к ее информационной инфраструктуре или информационной инфраструктуре поставщика услуг	Принимается самостоятельно организацией БС РФ на основании анализа показателей экономической целесообразности и уровня оцененного риска

Тип операционного риска	Возможная характеристика СВР	Возможный источник получения оценки СВР	Возможная характеристика СТП	Принятие решения о возможности аутсорсинга
Связанный с возможностью прерывания деятельности в результате реализации угроз ИБ	Оценка уровня соблюдения требования к непрерывности предоставления финансовых услуг; оценка уровня защиты информации в соответствии с требованием законодательства РФ	Оценка выполняется на основе результатов прохождения поставщиком услуг внешнего независимого аудита	Операционные расходы (убытки) организации БС РФ, связанные с нарушением непрерывности предоставления финансовых услуг в результате НСД к ее информационной инфраструктуре или информационной инфраструктуре поставщика услуг	Принимается самостоятельно организацией БС РФ на основании анализа показателей экономической целесообразности и уровня оцененного риска
Связанный с реализацией инцидентов ИБ	Оценка уровня защиты информации в соответствии с требованием законодательства РФ; оценка потенциала организации БС РФ обеспечить контроль уровня обеспечения ИБ после заключения соглашения с поставщиком услуг	Оценка выполняется на основе результатов прохождения поставщиком услуг внешнего независимого аудита	Общая сумма операций по переводу денежных средств, включая электронные денежные средства, осуществляемых через организацию БС РФ с использованием электронных технологий; среднеквартальный остаток денежных средств, находящихся на корреспондентских счетах организации БС РФ, открытых в расчетных центрах платежных систем, в том числе в платежной системе Банка России; операционные расходы (убытки) организации БС РФ, связанные с нарушением непрерывности предоставления финансовых услуг в результате НСД к ее информационной инфраструктуре или информационной инфраструктуре поставщика услуг	Принимается самостоятельно организацией БС РФ на основании анализа показателей экономической целесообразности и уровня оцененного риска
Связанный с возникновением зависимости от поставщика услуг	Оценка потенциала организации БС РФ обеспечить ИБ в случае отказа поставщика услуг от выполнения своих обязательств	Собственная оценка организации БС РФ, выполненная ее работниками; оценка, выполняемая аудиторской или консалтинговой организацией (независимой от поставщика услуг)	Утрата организациями БС РФ необходимых компетенций, знаний и навыков, необходимых для обеспечения ИБ при необходимости возврата выполнения существенных функций с использованием собственных ресурсов; неприемлемые финансовые затраты организаций БС РФ на обеспечение должного уровня ИБ в случае отказа поставщика услуг от своих обязательств; невозможность обеспечить должный уровень ИБ при возврате выполнения существенных функций в течение периода времени, приемлемого для организаций БС РФ	Принимается самостоятельно организацией БС РФ на основании анализа показателей экономической целесообразности и уровня оцененного риска; однозначная невозможность передачи выполнения существенных функций на аутсорсинг в случае отсутствия у организации БС РФ стратегии “выхода”

8. Содержание задач и зона ответственности руководства организации банковской системы Российской Федерации при аутсорсинге существенных функций

8.1. Деятельность руководства организации БС РФ является ключевым фактором обеспечения должного уровня управления и контроля в отношении риска нарушения ИБ при аутсорсинге существенных функций. Одним из основных аспектов является наличие полного осознания руководством БС РФ, что передача при аутсорсинге поставщику услуг выполнения бизнес-функций не переносит на поставщика услуг ответственность, обязанности по обеспечению ИБ и риски нарушения ИБ организации БС РФ.

8.2. Основным содержанием задач руководства организации БС РФ при аутсорсинге, определенным в настоящем стандарте, является:

- установление политики и программы аутсорсинга существенных функций в соответствии с требованиями к их содержанию, определенными в настоящем стандарте, и реализация контроля за их выполнением;
- установление механизмов управления и контроля в отношении уровня риска нарушения ИБ в рамках заключения соглашений с поставщиком услуг;
- контроль над реализацией и выполнением деятельности по управлению риском нарушения ИБ;
- принятие решения о возможности аутсорсинга только на основании оценки риска нарушения ИБ;
- обеспечение наличия плана действий организации БС РФ в случае отказа поставщика услуг от выполнения своих обязательств, реализация которого позволит обеспечить необходимый уровень ИБ для продолжения выполнения бизнес-функций в течение периода времени, приемлемого для организации БС РФ (далее – стратегия “выхода”).

8.3. В зону компетенции совета директоров (наблюдательного совета) организации БС РФ рекомендуется включить:

- определение политики аутсорсинга в соответствии с положениями раздела 6 настоящего стандарта, предполагающей оценку (мониторинг) риска нарушения ИБ в рамках всех действующих и возможных соглашений об аутсорсинге существенных функций;
- установление показателей уровня риска нарушения ИБ, связанного с аутсорсингом, приемлемого для организации БС РФ (риск-аппетита);
- обеспечение контроля соблюдения политики аутсорсинга и уровня риска нарушения ИБ, связанного с аутсорсингом;
- определение лиц из числа членов исполнительного органа организации БС РФ, в компетенцию которых входит принятие решений о возможности аутсорсинга в соответствии с требованиями политики аутсорсинга на основании оценки и установленного показателя уровня приемлемого риска нарушения ИБ (риск-аппетита);
- обеспечение контроля установления исполнительным органом организации БС РФ программы аутсорсинга в соответствии с принятой политикой аутсорсинга;
- рассмотрение вопросов финансирования регулярного аудита поставщика услуг с целью подтверждения качества предоставления услуг в части обеспечения ИБ и создания условий непрерывности предоставления финансовых услуг.

8.4. В зону компетенции исполнительного органа организации БС РФ входит:

- определение методики оценки и уровня риска при аутсорсинге;
- определение показателей (метрик), характеризующих риск нарушения ИБ при аутсорсинге существенных функций, в том числе на основе положений раздела 7 настоящего стандарта;
- определение и контроль выполнения программы аутсорсинга, соответствующей политике аутсорсинга, установленной в соответствии с разделом 6 настоящего стандарта;
- принятие решения о возможности аутсорсинга и последующий выбор поставщика услуг;
- обеспечение оперативного мониторинга и контроля уровня риска нарушения ИБ, связанного с аутсорсингом существенных функции, на основе разработанных показателей (метрик), характеризующих риск нарушения ИБ, в рамках всех действующих соглашений об аутсорсинге;
- обеспечение наличия стратегии (плана действий) на случай отказа поставщика услуг от выполнения своих обязательств перед организациями БС РФ (стратегии “выхода”);
- обеспечение контрольных мероприятий в рамках выполнения программы аутсорсинга, связанных с мониторингом и контролем риска нарушения ИБ. К таким мероприятиям могут относиться:
  - организация проведения и использования результатов внешних аудитов обеспечения ИБ и обеспечения непрерывности предоставления финансовых услуг;
  - организация проведения и использования результатов мониторинга и контроля обеспечения ИБ, выполненного самостоятельно организацией БС РФ или с привлечением аудиторской или консалтинговой организации;

- обеспечение надлежащих и корректирующих действий, направленных на поддержание уровня риска нарушения ИБ при аутсорсинге существенных функций на приемлемом уровне, установленном политикой аутсорсинга.

9. Требования к проведению оценки поставщика услуг при аутсорсинге существенных функций

9.1. Одним из основных элементов успешной реализации управления риском нарушения ИБ при аутсорсинге существенных функций является всесторонняя оценка потенциала поставщика услуг выполнить свои обязательства в соответствии с требованиями по управлению риском нарушения ИБ, применяемыми организацией БС РФ.

Оценку поставщика услуг рекомендуется проводить перед заключением с ним соглашения об аутсорсинге, а также на периодической (регулярной) основе.

9.2. Основными целями оценки поставщика услуг являются:

– оценка ресурсов, потенциала и возможностей поставщика услуг обеспечить необходимый уровень ИБ при выполнении своих обязательств в рамках заключенного соглашения;
– оценка опыта и репутации поставщика услуг;
– оценка показателей деятельности поставщика услуг на основе метрик СВР, принятых организацией БС РФ для контроля и мониторинга риска нарушения ИБ при аутсорсинге существенных функций;
– оценка возможностей поставщика услуг обеспечивать выполнение обязательств организации БС РФ перед клиентами и контрагентами, а также Банком России и уполномоченными органами исполнительной власти в рамках выполнения надзорных (контрольных) мероприятий в области защиты информации, как если бы бизнес-функции, переданные на аутсорсинг, выполнялись самостоятельно организацией БС РФ.

9.3. При оценке ресурсов, потенциала и возможностей поставщика услуг организации БС РФ необходимо учитывать следующие показатели:

– финансовое состояние поставщика услуг, наличие финансовых ресурсов, необходимых и достаточных для обеспечения ИБ при предоставлении организации БС РФ услуг аутсорсинга на протяжении всего срока действия соглашения. Для оценки финансового состояния поставщика услуг организацией БС РФ могут использоваться методы, аналогичные применяемым при оценке финансового состояния и потенциала кредиторов и иных контрагентов в организации БС РФ, результаты анализа или аудита финансового состояния (отчетности);
– наличие в штате поставщика услуг персонала в необходимом количестве и с достаточной квалификацией, реализация поставщиком услуг программ повышения квалификации персонала и реализации проведения аттестации персонала в соответствии с применимыми отечественными и международными системами аттестации (см. Приложение 1);
– наличие у поставщика услуг системы обеспечения ИБ;
– реализация политики обеспечения доверия к персоналу, которая должна соответствовать политике обеспечения доверия к персоналу, применяемой в организации БС РФ. В составе реализации такой политики необходимо рассматривать:
  - определение, выполнение и регистрацию процедуры контроля деятельности работников, обладающих совокупностью полномочий, определяемых их ролями, позволяющими получить доступ к защищаемой информации организации БС РФ;
  - определение, выполнение и регистрацию процедуры приема на работу, реализующие принцип “знать своего работника”, включающие проверку подлинности предоставленных документов, заявляемой квалификации, точности и полноты биографических фактов, а также проверку в части профессиональных навыков и оценку профессиональной пригодности;
  - получение письменного обязательства работников поставщика услуг о соблюдении конфиденциальности, приверженности правилам корпоративной этики, включая требования по недопущению конфликта интересов;
  - включение обязанности персонала поставщика услуг по выполнению требований к обеспечению ИБ, обработке ПДн, обеспечению сохранности защищаемой информации в трудовые контракты (соглашения, договоры) и (или) должностные инструкции;
– наличие у поставщика услуг необходимых лицензий, предусмотренных законодательством о лицензировании отдельных видов деятельности [6–8];
– показатели, характеризующие политику аутсорсинга поставщика услуг в части обеспечения ИБ.

Для оценки политики поставщика услуг может быть рекомендован перечень вопросов, представленный в Приложении 2.

9.4. В составе метрик СВР, характеризующих деятельность поставщика услуг, могут использоваться следующие:

– оценка уровня защиты информации, реализованного поставщиком услуг в соответствии с требованием законодательства РФ (в том числе в соответствии с ГОСТ 57580.1-2017 [17]);
– оценка уровня соблюдения требования к непрерывности предоставления финансовых услуг, реализованного поставщиком услуг;
– оценка потенциала организации БС РФ обеспечить контроль уровня обеспечения ИБ после заключения соглашения с поставщиком услуг;
– наличие у поставщика услуг необходимого технического и (или) технологического обеспечения.

9.5. Важным фактором при выборе поставщика услуг является оценка его репутации:

– наличие положительной деловой репутации в области выполнения аутсорсинга существенных функций для организаций БС РФ;
– наличие опыта разработки, реализации и поддержки решений по аутсорсингу существенных функций;
– наличие известных инцидентов ИБ.

9.6. При оценке возможности поставщика услуг обеспечить выполнение обязательств организации БС РФ следует рассмотреть следующие показатели:

– соблюдение требований к обеспечению ИБ, установленных для организации БС РФ законодательством РФ по защите информации (в том числе в соответствии с ГОСТ 57580.1-2017 [17]);
– возможность получения информации, необходимой для предоставления Банку России и уполномоченным органам исполнительной власти в рамках выполнения надзорных (контрольных) мероприятий в области защиты информации;
– возможность осуществления организацией БС РФ деятельности по мониторингу и контролю риска нарушения ИБ;
– возможность организации БС РФ получать информацию о результатах проведения внешних аудитов обеспечения ИБ и внешних аудитов обеспечения непрерывности деятельности.

9.7. Организация БС РФ может выполнить оценку поставщика услуг следующими способами:

– самостоятельно работниками организации БС РФ;
– с привлечением аудиторской или консалтинговой организации (независимой от поставщика услуг), обладающей необходимым опытом и компетенцией для проведения оценки поставщика услуг.

9.8. В качестве основного фактора при оценке поставщика услуг организацией БС РФ следует рассматривать соблюдение законодательства РФ в области трансграничной передачи защищаемой информации в соответствии с положением пункта 6.9 настоящего стандарта.

9.9. В качестве дополнительного фактора при оценке поставщика услуг организацией БС РФ следует рассматривать:

– зависимость деятельности поставщика услуг от субподрядчиков;
– результаты взаимодействия поставщика услуг с субподрядчиками;
– наличие у поставщика услуг страхования рисков, связанных с эксплуатацией его информационной инфраструктуры.

9.10. Организации БС РФ, выполняющей функции оператора по переводу денежных средств, признанной Банком России значимой на рынке платежных услуг, рекомендуется заранее уведомлять ФинЦЕРТ Банка России (info_fincert@cbr.ru) о планируемой передаче выполнения существенных функций на аутсорсинг.

9.11. Оценка поставщика услуг должна носить периодический характер и входить в состав мониторинга и контроля риска нарушения ИБ при аутсорсинге существенных функций, установленный разделом 11 настоящего стандарта. Оценку поставщика услуг рекомендуется проводить не реже одного раза в два года. Конкретные интервалы проведения оценки организация БС РФ определяет самостоятельно.

10. Требования к содержанию соглашений об аутсорсинге существенных функций

10.1. Заключение с поставщиком услуг соглашения (контракта, пакета договорных документов) об аутсорсинге является одним из основных элементов управления и контроля в отношении риска нарушения ИБ при аутсорсинге существенных функций.

10.2. Содержание соглашения об аутсорсинге должно создать правовые условия для возможности обеспечения организацией БС РФ:

– контроля и мониторинга уровня риска нарушения ИБ;
– выполнения своих обязательств перед клиентами и контрагентами, а также перед Банком России и уполномоченными органами исполнительной власти в рамках выполнения надзорных (контрольных) мероприятий в области защиты информации.

10.3. Содержание соглашения об аутсорсинге должно однозначно среди прочего определять:

– перечень существенных функций, связанных с обработкой защищаемой информации или обеспечением ИБ (реализацией процессов обеспечения ИБ), передаваемых на аутсорсинг поставщику услуг;
– обязанности и разделение зоны ответственности поставщика услуг и организации БС РФ в обеспечении ИБ при аутсорсинге существенных функций;
– требования к показателям качества деятельности поставщика услуг, определяемым на основе метрик управления риском нарушения ИБ организацией БС РФ в рамках процедур управления риском;
– требования к уровню и качеству предоставления услуг в части обеспечения ИБ и создания условий непрерывности предоставления финансовых услуг (требования к SLA) и к инструментам по мониторингу этого уровня;
– требования к гарантиям поставщика услуг (в том числе финансовым) в случае наступления риска нарушения ИБ;
– требования к инфраструктуре оказания услуг, включая инфраструктуру обеспечения ИБ и обеспечения непрерывности выполнения бизнес-функций и их восстановления после инцидентов ИБ;
– обязанность поставщика услуг обеспечить возможность проведения организацией БС РФ или привлекаемой организацией БС РФ консалтинговой или аудиторской организацией контрольных мероприятий в рамках мониторинга риска нарушения ИБ;
– обязанность по обеспечению сторонами конфиденциальности информации;
– обязанность поставщика услуг проходить периодический аудит с целью подтверждения качества предоставления услуг в части обеспечения ИБ и создания условий непрерывности предоставления финансовых услуг;
– обязанность поставщика услуг информировать организацию БС РФ об инцидентах ИБ, включая НСД к защищаемой информации, в течение 3-х часов после выявления инцидента ИБ, а также о мерах, предпринятых для управления наступившими инцидентами;
– порядок разбора конфликтов в случае нарушения поставщиком услуг условий оказания услуг, а также в случае несогласия поставщика услуг признавать факт реализации риска нарушения ИБ или инцидента ИБ;
– обязанность поставщика услуг информировать организацию БС РФ обо всех факторах, связанных с возникновением риска нарушения ИБ при аутсорсинге существенных функций, включая тип событий и обстоятельства их реализации;
– обязанность поставщика услуг передавать всю необходимую информацию организации БС РФ для выполнения своих обязательств перед Банком России и уполномоченными органами исполнительной власти в рамках выполнения надзорных (контрольных) мероприятий в области защиты информации;
– возможность пересмотра и изменения условий соглашения по инициативе организации БС РФ в следующих случаях:
  • наличие у организации БС РФ необходимости сохранить надлежащий уровень контроля и управления в отношении риска нарушения ИБ при аутсорсинге существенных функций;
  • наличие у организации БС РФ необходимости принять соответствующие меры для выполнения своих обязательств перед клиентами и контрагентами, а также перед Банком России и уполномоченными органами исполнительной власти;
  • возможность проведения регулярных (не реже одного раза в квартал) встреч представителей организации БС РФ и поставщика услуг для обсуждения статуса выполнения соглашения об аутсорсинге в части вопросов обеспечения ИБ;
– рекомендуемые основания для отказа организаций БС РФ от исполнения соглашения с поставщиком услуг в одностороннем внесудебном порядке в случае:
  • смены владельцев (участников) поставщика услуг;
  • изменения финансового состояния поставщика услуг, его потенциала, ресурсов и возможностей в отношении выполнения услуг аутсорсинга существенных функций;
  • нарушения поставщиком услуг требований к уровню и качеству предоставления услуг в части обеспечения ИБ и создания условий непрерывности предоставления финансовых услуг (требования к SLA);
  • препятствия (отказа) со стороны поставщика услуг реализации мониторинга и контроля риска нарушения ИБ со стороны организации БС РФ или со стороны независимой аудиторской организации;
  • возникновения риска нарушения ИБ, превышающего уровень, определенный организацией БС РФ в качестве приемлемого;
  • возникновения инцидентов нарушения ИБ;
– минимальный срок выполнения условий расторжения соглашения об аутсорсинге существенных функций, необходимый организации БС РФ для возобновления выполнения бизнес-функций собственными

ресурсами или с привлечением иного поставщика услуг в случаях расторжения действующего соглашения;

– условия привлечения поставщиком услуг субподрядчиков, предусматривающие:
  - право организации БС РФ сохранить способность мониторинга и контроля риска нарушения ИБ при аутсорсинге существенных функций в случаях привлечения поставщиком услуг субподрядчиков;
  - ограничения на передачу субподрядчику обработки защищаемой информации;
  - ответственность поставщика услуг за все действия субподрядчика в части вопросов обеспечения ИБ, в том числе ответственность за соблюдение законодательства РФ;
  - обязанность поставщика услуг обеспечить уведомление и получать предварительное согласование организации БС РФ при привлечении субподрядчиков для выполнения существенных функций организации БС РФ;
  - обязанность поставщика услуг предоставить организации БС РФ документы (в том числе политики, стандарты), разработанные поставщиком услуг для обеспечения ИБ;
– обязанность поставщика услуг обеспечить соблюдение требований к защите информации, установленных для организации БС РФ, в том числе:
  - в рамках законодательства о национальной платежной системе [3, 9, 10];
  - в области защиты информации ограниченного доступа, включая защиту ПДн [4, 11, 12];
  - в области безопасности критической информационной инфраструктуры [13];
  - в области лицензирования отдельных видов деятельности [6–8];
  - нормативных актов Банка России, устанавливающих обязанность кредитных организаций по созданию и передаче Банку России резервных копий электронных баз данных, а также размещению их на территории РФ [16];
– политику предоставления поставщику услуг доступа к защищаемой информации и инфраструктуре организации БС РФ;
– описание контактных данных лица, ответственного за реализацию соглашения об аутсорсинге со стороны поставщика услуг, а также процедур эскалации возможных конфликтов при оказании услуг аутсорсинга;
– требования к работникам поставщика услуг, задействованным в обеспечении ИБ.

10.4. Целесообразно указать услуги (сервисы), которые будут поддерживаться поставщиком услуг в случае возникновения инцидентов ИБ.

10.5. При составлении соглашения об аутсорсинге необходимо привлекать представителей службы ИБ организации БС РФ, подразделений управления рисками, операционных подразделений, юридической службы, службы управления закупками, а также подразделений информатизации.

11. Мониторинг и контроль риска нарушения информационной безопасности при аутсорсинге существенных функций

11.1. Осуществление надлежащего мониторинга и контроля риска нарушения ИБ при аутсорсинге существенных функций входит в зону компетенции исполнительного органа организации БС РФ.

Для выполнения указанных функций исполнительный орган БС РФ должен обеспечить наличие регистра риска, содержащего:
– информацию обо всех соглашениях аутсорсинга существенных функций;
– показатели (метрики), характеризующие риск нарушения ИБ при аутсорсинге существенных функций, определенные в соответствии с разделом 7 настоящего стандарта. Показатели (метрики) должны рассматриваться исполнительным органом независимо для каждого заключенного соглашения об аутсорсинге;
– оценку значений показателей (метрик) риска нарушения ИБ, обновляемую в соответствии с установленной периодичностью, но не реже одного раза в год.

11.2. Исполнительный орган обязан организовать мониторинг следующих видов рисков:
– операционный риск, связанный с потерей (невозможностью) контроля обеспечения ИБ поставщиком услуг;
– операционный риск, связанный с возможностью прерывания деятельности в результате реализации угроз ИБ;
– операционный риск, связанный с реализацией инцидентов ИБ;
– операционный риск, связанный с возникновением зависимости от поставщика услуг.

Для выполнения мониторинга указанных видов рисков организацией БС РФ может быть рассмотрен подход, использованный в таблице 3.

Таблица 3. Рекомендуемый подход к мониторингу риска нарушения ИБ при аутсорсинге существенных функций

Тип риска	Характеристика мониторинга (метрика)	Способ мониторинга (периодичность)
Операционный риск, связанный с потерей (невозможностью) контроля обеспечения ИБ поставщиком услуг	Характеристика достижения целей обеспечения ИБ организацией БС РФ; потенциал организации БС РФ обеспечить контроль риска нарушения ИБ при аутсорсинге существенных функций	Самостоятельная оценка организацией БС РФ выполнения своих показателей; рекомендуемая периодичность – ежегодно
Операционный риск, связанный с возможностью прерывания деятельности	Операционные расходы (убытки) организации БС РФ, связанные с нарушением непрерывности предоставления финансовых услуг в результате НСД к ее информационной инфраструктуре или информационной инфраструктуре поставщика услуг	Самостоятельная оценка организацией БС РФ операционных расходов (убытков) в результате нарушения непрерывности предоставления финансовых услуг; рекомендуемая периодичность – ежеквартально
Операционный риск, связанный с реализацией инцидентов ИБ	Операционные расходы (убытки), связанные с совершением финансовых операций, имеющих финансовые последствия, в том числе переводов денежных средств, без согласия клиентов; операционные расходы (убытки) организации БС РФ в результате НСД к объектам ее информационной инфраструктуры, используемой для осуществления переводов денежных средств или в результате использования электронных средств платежа без согласия клиентов	Самостоятельная оценка организацией БС РФ операционных расходов (убытков) в результате перевода денежных средств без согласия клиентов, а также в результате НСД к объектам информационной инфраструктуры организации БС РФ; рекомендуемая периодичность – ежеквартально
Операционный риск, связанный с возникновением зависимости от поставщика услуг	Характеристика потенциала организации БС РФ обеспечить ИБ существенных функций после заключения соглашения с поставщиком услуг или в случае отказа поставщика услуг от выполнения своих обязательств	Самостоятельная оценка организацией БС РФ или с привлечением аудиторской или консалтинговой организации (независимой от поставщика услуг) возможности реализовать стратегию “выхода” в случае отказа поставщика услуг от выполнения своих обязательств; рекомендуемая периодичность – ежегодно

11.3. Для проведения оценки показателей (метрик) риска нарушения ИБ при аутсорсинге существенных функций исполнительному органу следует обеспечить привлечение представителей службы ИБ организации БС РФ, подразделений управления рисками, операционных подразделений, юридической службы, а также при необходимости подразделений информатизации для:

– подготовки данных по определенному перечню показателей (метрик) риска нарушения ИБ;
– своевременного предоставления актуальной информации о значениях показателей (метрик) исполнительному органу организации БС РФ, а также обеспечения их достоверности.

Дополнительным видом мониторинга и контроля риска нарушения ИБ при аутсорсинге существенных функций является деятельность службы внутреннего контроля организации БС РФ, направленная на оценку полноты, адекватности и актуальности данных о показателях (метриках) нарушения ИБ, предоставляемых исполнительными органами организации БС РФ.

11.4. В случае возникновения риска нарушения ИБ, связанного с аутсорсингом существенных функций, превышающего принятый приемлемый риск (риск-аппетит), организации БС РФ следует совершить оперативные корректирующие действия, направленные на обработку указанного риска:

– корректировка (пересмотр) соглашения;
– рассмотрение целесообразности расторжения соглашения и последующая реализация стратегии “выхода”.

Организация БС РФ должна предусмотреть механизмы принятия оперативного решения, в случае если уровень риска нарушения ИБ выходит за рамки допустимых значений. В таких случаях должен быть предусмотрен внеплановый аудит поставщика услуг для подтверждения способности выполнять аутсорсинг существенных функций организации БС РФ.

Рассмотрение вопросов о фактах выявления неприемлемых рисков при аутсорсинге существенных функций, а также принятие решения по таким случаям должно входить в компетенцию совета директоров (наблюдательного органа) организации БС РФ.

В случае выявления рисков и принятия решения о корректировке соглашения необходимо проведение надлежащей переоценки риска нарушения ИБ в объеме, определяемом содержанием предполагаемых корректировок.

11.5. Важной частью мониторинга и контроля риска нарушения ИБ при аутсорсинге существенных функций является прохождение поставщиком услуг регулярного аудита.

Организация БС РФ должна обеспечить анализ результатов проведения периодического аудита с целью:

– обновления (уточнения) перечня существенных функций, связанных с обработкой защищаемой информации или обеспечением ИБ, передаваемых на аутсорсинг поставщику услуг;
– контроля надлежащего и своевременного предоставления поставщиком услуг отчетности в части аутсорсинга существенных функций;
– оценки показателей качества деятельности поставщика услуг, определенных на основе показателей (метрик) управления риском нарушения ИБ;
– соблюдения поставщиком услуг установленных соглашением параметров уровня и качества предоставления услуг в части обеспечения ИБ и создания условий непрерывности предоставления финансовых услуг (требований к SLA).

Поставщик услуг должен проходить периодический аудит с целью подтверждения качества предоставления услуг в части:

– защиты информации в соответствии с требованием законодательства РФ;
– создания условий непрерывности предоставления финансовых услуг организации БС РФ.

11.6. Основные требования, предъявляемые к организациям, проводящим аудит информационной безопасности:

– независимость аудиторской организации от выполнения бизнес-функций организации БС РФ и поставщика услуг;
– обладание необходимой компетенцией и навыками выполнения аудиторских проверок, определенных в первую очередь опытом проведения проверок;
– использование передовых отечественных и международных практик аудиторских проверок;
– наличие рекомендаций Банка России о возможности привлечения аудиторской организации.

11.7. Минимальный срок хранения аудиторских заключений деятельности поставщика услуг – 5 лет.

12. Особенности аутсорсинга процессов информационной безопасности

12.1. В настоящее время у организаций БС РФ отмечается потребность в передаче отдельных процессов системы обеспечения ИБ (далее – СОИБ) на аутсорсинг поставщикам услуг. Организации доверяют поставщикам услуг реализацию процессов обеспечения ИБ для оптимизации расходов, повышения эффективности деятельности и поддержания необходимого уровня ИБ.

Аутсорсинг ИБ рассматривается в качестве альтернативы реализации, поддержки и улучшения СОИБ силами работников организации БС РФ, ответственных за обеспечение ИБ.

Целью организации БС РФ при аутсорсинге процессов СОИБ является привлечение квалифицированного персонала и получение готовых процессов и развитой методологии, а также средств, систем и технологий обеспечения ИБ, необходимых для организации и эксплуатации СОИБ.

Поставщик услуг аутсорсинга ИБ может использовать уже применяемые организацией БС РФ средства и системы обеспечения ИБ – принимать их на эксплуатацию и (или) администрирование.

12.2. Основными целями использования аутсорсинга ИБ организацией БС РФ является:

– кадровое обеспечение:
  - необходимость обеспечения ИБ при отсутствии у организации БС РФ собственных кадров в необходимом количестве и (или) требуемой квалификации;
  - необходимость высвобождения ключевых специалистов организации БС РФ для выполнения приоритетных проектов и задач;
– экономическая эффективность:
  - предсказуемость и прозрачность финансовых расходов на обеспечение ИБ при использовании аутсорсинга ИБ;
  - оптимизация финансовых расходов на организацию и эксплуатацию СОИБ организации БС РФ;
– техническое и технологическое обеспечение:
  - повышение общего уровня ИБ за счет использования современных средств, систем и технологий обеспечения ИБ;
  - поддержка реализации критичных процессов СОИБ в режиме 24×7;
  - возможность быстрых реализаций и совершенствования отдельных процессов СОИБ.

12.3. В общем случае поставщик услуг аутсорсинга ИБ может предоставлять следующие сервисы ИБ:

– эксплуатация средств и систем обеспечения ИБ, используемых организацией БС РФ;
– эксплуатация средств и систем обеспечения ИБ, предоставляемых поставщиком услуг аутсорсинга;
– реализация отдельных целостных процессов СОИБ или их частей.

12.4. Организации БС РФ стоит ориентироваться на один из следующих подходов к аутсорсингу ИБ:

– долговременное сотрудничество. На аутсорсинг передаются непрофильные и (или) сложные процессы ИБ (например, мониторинг событий и реагирование на инциденты ИБ);
– среднесрочное сотрудничество. На аутсорсинг временно передаются сложные технологические процессы СОИБ до момента реализации соответствующего процесса самостоятельно организацией БС РФ. Например, процесс мониторинга событий ИБ может быть передан на аутсорсинг на время построения собственного Центра мониторинга и реагирования;
– кратковременное сотрудничество. Усиление СОИБ услугами аутсорсинга на время проведения крупных мероприятий, характерных увеличением рисков ИБ (например, политические саммиты, выборы, спортивные соревнования, международные конкурсы).

12.5. Организации БС РФ целесообразно рассматривать возможность аутсорсинга следующих процессов СОИБ:

– выявление компьютерных атак на информационную инфраструктуру организации БС РФ, в том числе с использованием информации, получаемой от Центра мониторинга и реагирования на компьютерные атаки в кредитно-финансовой сфере (ФинЦЕРТ);
– управление средствами защиты информации организации БС РФ, в том числе системами обнаружения вторжений (IDS/IPS);
– управление межсетевыми экранами (в том числе и на прикладном уровне по 7-уровневой стандартной модели взаимодействия открытых систем, определенной в ГОСТ 28906-91), средствами антивирусной защиты и другими решениями по обеспечению ИБ;
– анализ безопасности кода приложений;
– мониторинг и анализ событий ИБ (Security Operation Center);
– анализ защищенности и контроль конфигурации сетевого оборудования и операционных систем;
– проведение тестирования на проникновение;
– анализ защищенности информационной инфраструктуры;
– обеспечение безопасности веб-доступа и электронной почты;
– организация управления инцидентами ИБ;
– оповещение о новых угрозах и признаках атак (Treat Intelligence);
– повышение осведомленности по вопросам ИБ и проведение киберучений.

12.6. Организации БС РФ следует применять соглашения об уровне предоставления сервиса ИБ (SLA) для контроля качества услуг аутсорсинга ИБ. SLA – это дополнение к соглашению об аутсорсинге между организацией БС РФ и поставщиком услуг, определяющее предоставление сервиса с заданным уровнем качества.

Общий состав SLA должен среди прочего определять:

– описание состава предоставляемых поставщиком услуг сервисов ИБ;
– согласованный уровень качества сервиса ИБ (перечень ключевых параметров качества), содержащий:
  • описание расчета ключевых параметров качества сервиса и периодичность предоставления поставщиком услуг отчетов о параметрах качества;
  • методы и средства контроля ключевых параметров качества;
  • описание методов контроля исполнения SLA;
  • установление обязанности и описание процедуры предоставления поставщиком услуг информации о нарушениях SLA и условиях эскалации инцидентов, связанных с нарушением SLA (далее – инцидент SLA);
  • описание процедур восстановления работы в случаях прерывания предоставляемых сервисов ИБ, или отказа в обслуживании, или нарушения SLA;
  • описание процедуры внесения изменений в SLA.

12.7. Контрольные ключевые параметры качества сервиса ИБ, вносимые в соглашение, должны быть измеримыми и представляться в виде числовых показателей (метрик). Состав ключевых показателей (метрик) качества определяется в зависимости от состава предоставляемых сервисов ИБ. Ключевыми показателями (метриками) качества сервиса ИБ могут выступать среди прочих:

– временные показатели (метрики):
  • время реакции на обращение организации БС РФ – время, прошедшее с момента поступления и регистрации запроса на обслуживание (сообщение организации БС РФ об инциденте) до фактического начала работ по факту обращения;
  • время закрытия инцидента SLA – время, прошедшее с момента фактического начала работ над инцидентом SLA до его фактического закрытия;
  • время решения инцидента SLA – суммарное время, прошедшее с момента поступления и регистрации обращения до закрытия заявки на обслуживание;
  • максимальное время реакции поставщика услуг – максимальное время, необходимое поставщику услуг при аварийных ситуациях для устранения их последствий;
  • время устранения уязвимости – время, прошедшее с момента обнаружения уязвимости до ее устранения;
– качественные характеристики:
  • число предотвращенных утечек информации по отношению к общему числу реализованных и предотвращенных утечек информации;
  • число предотвращенных фишинговых атак по отношению к общему числу реализованных и предотвращенных фишинговых атак;
  • соотношение числа запросов на обслуживание (сообщение организации БС РФ об инциденте) к числу инцидентов SLA;
  • число повторных инцидентов SLA определенного типа;
  • соотношение найденных и устраненных уязвимостей;
– качественные метрики:
  • уровень брака – это количественное или процентное выражение количества инцидентов SLA за определенный (отчетный) период времени;
  • техническое качество – уровень технического качества программно-аппаратного комплекса, используемого для предоставления сервисов ИБ и обеспечивающего гарантию непрерывности предоставления финансовых услуг;
  • удовлетворенность качеством обслуживания – степень соответствия реализации сервиса ИБ потребности организации БС РФ, определяемой на основании опросов, проводимых самостоятельно организацией БС РФ и (или) с привлечением независимой организации;
– метрики доступности и непрерывности сервисов ИБ:
  • доступность сервисов ИБ организации БС РФ – количество времени или временной промежуток, в котором сервисы ИБ, выполняемые поставщиком услуг, остаются доступными;
  • время восстановления сервисов ИБ в случае прерывания (RTO, Recovery time objective).

Количество метрик, включаемых в SLA, должно быть достаточным для проведения объективной оценки качества предоставления сервисов ИБ поставщиком услуг.

Приложение 1

Международная сертификация по информационной безопасности

Сертификация международной ассоциации ISACA (Information Systems Audit and Control Association):

- Certified Information Systems Auditor (CISA) – сертифицированный аудитор информационной безопасности;
- Certified Information Security Manager (CISM) – сертифицированный руководитель службы информационной безопасности.

Сертификация международного консорциума по информационной безопасности ISC² (International Information Systems Security Certifications Consortium, Inc.):

- Certified Information Systems Security Professional (CISSP) – сертифицированный профессионал в области информационной безопасности.

Приложение 2

Перечень вопросов для оценки политики поставщика услуг в части обеспечения информационной безопасности

1. Вопросы организации защиты данных
- Как данные организации БС РФ, включая защищаемую информацию, отделены от данных других клиентов?
- Где хранятся данные организации БС РФ, включая защищаемую информацию?
- Как обеспечивается конфиденциальность и целостность данных организации БС РФ, включая защищаемую информацию?
- Как осуществляется контроль доступа к данным организации БС РФ, включая защищаемую информацию?
- Как защищаются данные организации БС РФ в процессе их передачи поставщику услуг?
- Как защищаются данные организации БС РФ в процессе их передачи между различными подразделениями поставщика услуг, в том числе в процессе их передачи между различными центрами обработки данных, включая облачные?
- Как защищаются данные организации БС РФ в процессе их передачи субподрядчикам поставщика услуг?
- Реализованы ли меры по контролю утечек данных организации БС РФ?
- Может ли третья сторона, в том числе правоохранительные органы, операторы связи, хостинг-провайдеры, получить доступ к данным организации БС РФ? Какие правила и механизмы доступа должны применяться?
- Все ли данные организации БС РФ уничтожаются по завершении договора на оказание услуг аутсорсинга?

2. Вопросы анализа защищенности
- Как часто проводится анализ защищенности сети и приложений поставщика услуг и его субподрядчиков?
- Может ли организация БС РФ провести собственный анализ защищенности поставщика услуг аутсорсинга? Какова процедура проведения анализа защищенности?
- Каков процесс устранения обнаруженных уязвимостей?
- Существуют ли результаты анализа защищенности инфраструктуры поставщика услуг со стороны третьих фирм?

3. Вопросы управления доступом
- Возможна ли интеграция с каталогом учетных записей организации БС РФ?
- Как осуществляется управление учетными записями в информационных системах поставщика услуг?
- Поддерживается ли Single Sign-On (SSO)? Какой стандарт применяется для реализации SSO?
- Поддерживается ли федеративная система аутентификации? Какой стандарт применяется?

4. Вопросы охраны и персонала
- В каком режиме обеспечивается контроль доступа на территорию поставщика услуг и его субподрядчиков (8×5 или 24×7)?
- Поставщик услуг и его субподрядчики пользуются выделенной инфраструктурой, включая помещения, или разделяют ее с другими организациями?
- Регистрируется ли доступ персонала поставщика услуг и субподрядчиков к данным, включая защищаемую информацию, организации БС РФ?
- Какова процедура набора персонала поставщиком услуг и его субподрядчиками?

5. Вопросы доступности и производительности
- Каков обеспечиваемый поставщиком услуг и его субподрядчиками уровень качества обслуживания (SLA)?
- Какие меры обеспечения доступности используются поставщиком услуг и его субподрядчиками (например, резервные каналы связи, защита от DDoS)?

- Какие инструменты контроля доступности инфраструктуры поставщика услуг предоставляются организации БС РФ?
- Существует ли у поставщика услуг план действий на время нарушения доступности инфраструктуры?

6. Вопросы безопасности приложений
- Существует ли у поставщика услуг процесс тестирования внешних приложений и исходного кода?
- Использует ли поставщик услуг или его субподрядчики приложения третьих фирм при оказании услуг аутсорсинга?
- Каковы используемые меры защиты приложений (например, WAF, защита БД)
- Внедрен ли поставщиком услуг и его субподрядчиками процесс безопасного программирования (SDLC) при разработке приложений?

7. Вопросы управления инцидентами
- Согласовано ли понятие инцидента ИБ и их перечень между организацией БС РФ и поставщиком услуг?
- Существует ли у поставщика услуг и его субподрядчиков план реагирования на инциденты?
- Каков процесс реагирования на инциденты?

8. Вопросы обеспечения сохранности защищаемой информации
- Какие данные собираются поставщиком услуг или его субподрядчиками об организации БС РФ? Где и как долго они хранятся?
- Каковы условия передачи данных организации БС РФ третьим лицам?
- Каковы гарантии поставщика услуг относительно нераскрытия защищаемой информации организации БС РФ третьим лицам и третьими лицами?
- Существует ли у поставщика услуг процесс обезличивания защищаемой информации и предоставления к ней доступа только авторизованному персоналу?

9. Вопросы обеспечения непрерывности бизнеса и восстановления после инцидентов ИБ
- Существует ли у поставщика услуг и его субподрядчиков план обеспечения непрерывности бизнеса и восстановления после катастроф?
- Существует ли у поставщика услуг и его субподрядчиков резервная инфраструктура, включая центр обработки данных?
- Проходил ли поставщик услуг внешний аудит по непрерывности бизнеса и восстановлению после катастроф?

10. Вопросы регистрации событий безопасности
- Как поставщиком услуг и его субподрядчиками обеспечивается регистрация событий безопасности и сбор доказательств по инцидентам ИБ?
- Как долго хранятся журналы регистрации событий? Какова периодичность ротации журналов регистрации? Возможно ли увеличение этого срока?
- Можно ли организовать хранение журналов регистрации событий во внешнем хранилище?

11. Вопросы соответствия требованиям
- Подчиняется ли поставщик услуг или его субподрядчики локальным, национальным или международным нормативным требованиям? Каким?
- Проходил ли поставщик услуг или его субподрядчики внешний аудит на требования обеспечения ИБ?
- Проводит ли поставщик услуг регулярную оценку рисков нарушения выполнения требований заказчиков, в том числе организации БС РФ?
- Внедрены ли средства контроля, обеспечивающие полное, точное и своевременное оказание услуг, снижающие выявленные риски?

12. Вопросы финансовых гарантий
- Существует ли компенсация в случае инцидента безопасности или нарушения соглашения о качестве обслуживания (SLA)?

13. Вопросы завершения договорных обязательств
- Какова процедура завершения договорных обязательств?
- Как осуществляется возврат защищаемой информации и в каком виде (формате)?
- В течение какого срока по окончании договорных обязательств поставщик услуг возвратит все данные организации БС РФ?
- Каков процесс уничтожения всех резервных и иных копий данных организации БС РФ?

14. Вопросы интеллектуальной собственности
- Кому принадлежат права на данные, переданные организацией БС РФ поставщику услуг? Кому принадлежат права на данные, полученные в процессе оказания услуг аутсорсинга организации БС РФ поставщиком услуг (в том числе журналы регистрации, резервные копии, репликации БД, базы инцидентов)?

Приложение 3

Примеры бизнес-функций, которые могут быть переданы на аутсорсинг

1. ИТ-аутсорсинг:
- аутсорсинг офисной печати;
- аутсорсинг центров обработки данных;
- облачные вычисления (по модели предоставления сервиса SaaS, PaaS, IaaS);
- обслуживание информационных (автоматизированных) систем организации БС РФ;
- разработка программного обеспечения.

2. Аутсорсинг в финансовой сфере:
- инвентаризационный аудит;
- обеспечение взаиморасчетов с персоналом.

3. Аутсорсинг в сфере управления персоналом:
- использование внештатного персонала (аутстаффинг);
- аутсорсинг обучения и повышения осведомленности.

4. Аутсорсинг в сфере безопасности:
- аутсорсинг инкассации;
- аутсорсинг информационной безопасности.

5. Аутсорсинг в сфере маркетинговых коммуникаций:
- телемаркетинг;
- аутсорсинг центров обработки вызовов.

6. Аутсорсинг в административно-хозяйственной сфере:
- аутсорсинг питания.

7. Аутсорсинг в сфере документооборота:
- аутсорсинг архивного хранения документов;
- аутсорсинг уничтожения документов на физических носителях.

Библиография

1. Committee on Payments and Market Infrastructures Board of the International Organization of Securities Commissions Guidance on cyber resilience for financial market infrastructures. URL: http://www.iosco.org/library/pubdocs/pdf/IOSCOPD535.pdf (дата обращения: 05.06.2017).

2. Федеральный закон от 27 июля 2006 года № 149-ФЗ “Об информации, информационных технологиях и о защите информации”.

3. Федеральный закон от 27 июня 2011 года № 161-ФЗ “О национальной платежной системе”.

4. Федеральный закон от 27 июля 2006 года № 152-ФЗ “О персональных данных”.

5. Outsourcing in Financial Services. URL: https://www.bis.org/publ/joint12.htm (дата обращения: 10.04.2017).

6. Постановление Правительства Российской Федерации от 3 февраля 2012 года № 79 “О лицензировании деятельности по технической защите конфиденциальной информации”.

7. Постановление Правительства Российской Федерации от 18 февраля 2005 года № 87 “Об утверждении перечня наименований услуг связи, вносимых в лицензии, и перечней лицензионных условий”.

8. Постановление Правительства Российской Федерации от 16 апреля 2012 года № 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)”.

9. Положение Банка России от 9 июня 2012 года № 382-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”.

10. Постановление Правительства Российской Федерации от 13 июня 2012 года № 584 “Об утверждении Положения о защите информации в платежной системе”.

11. Постановление Правительства Российской Федерации от 1 ноября 2012 года № 1119 “Об утверждении требований к защите персональных данных при их обработке в информационных системах персональных данных”.

12. Приказ Федеральной службы по техническому и экспортному контролю от 18 февраля 2013 года № 21 “Об утверждении Состава и содержания организационных и технических мер по обеспечению безопасности персональных данных при их обработке в информационных системах персональных данных”.

13. Федеральный закон от 26 июля 2017 года № 187-ФЗ “О безопасности критической информационной инфраструктуры Российской Федерации”.

14. Федеральный закон от 27 июля 2006 года № 152-ФЗ “О персональных данных”, ст. 12 “Трансграничная передача персональных данных”.

15. Федеральный закон от 21 июля 2014 года № 242-ФЗ “О внесении изменений в отдельные законодательные акты Российской Федерации в части уточнения порядка обработки персональных данных в информационно-телекоммуникационных сетях”.

16. Положение Банка России от 21 февраля 2013 года № 397-П “О порядке создания, ведения и хранения баз данных на электронных носителях”.

17. ГОСТ Р 57580.1-2017 “Безопасность финансовых (банковских) операций. Защита информации финансовых организаций. Базовый набор организационных и технических мер”.