

Главные управления  
(Национальные банки)  
Центрального банка  
Российской Федерации

от 26.10.2010 № 141-Т

О Рекомендациях по подходам кредитных организаций к выбору провайдеров и взаимодействию с ними при осуществлении дистанционного банковского обслуживания

В соответствии с Положением Банка России от 16 декабря 2003 года № 242-П «Об организации внутреннего контроля в кредитных организациях и банковских группах», зарегистрированным Министерством юстиции Российской Федерации 27 января 2004 года № 5489, 22 декабря 2004 года № 6222, 20 марта 2009 года № 13547 («Вестник Банка России» от 4 февраля 2004 года № 7, от 31 декабря 2004 года № 74, от 1 апреля 2009 года № 21), одной из целей осуществления внутреннего контроля является принятие мер по поддержанию на не угрожающем финансовой устойчивости кредитной организации и интересам её кредиторов и вкладчиков уровне банковских рисков.

Банк России направляет Рекомендации по подходам кредитных организаций к выбору провайдеров и взаимодействию с ними при осуществлении дистанционного банковского обслуживания, ориентированные на снижение уровней банковских рисков, связанных с использованием кредитными организациями аутсорсинга.

Территориальным учреждениям Банка России довести настоящее письмо до сведения кредитных организаций.

Настоящее письмо подлежит опубликованию в «Вестнике Банка России».

Приложение: на 17 л.

Г.Г. Меликьян

Приложение  
к Письму Банка России от «26» октября 2010 г.  
№ 141-Т «О Рекомендациях по подходам  
кредитных организаций к выбору провайдеров  
и взаимодействию с ними при осуществлении  
дистанционного банковского обслуживания»

## **Рекомендации**

по подходам кредитных организаций  
к выбору провайдеров и взаимодействию с ними  
при осуществлении дистанционного банковского обслуживания

### Раздел 1. Общие положения

1.1. Настоящие Рекомендации по подходам кредитных организаций к выбору провайдеров и взаимодействию с ними при осуществлении дистанционного банковского обслуживания (далее – Рекомендации) разработаны с учётом возможного влияния на банковскую деятельность рисков, связанных с таким обслуживанием, и недостатков в управлении ими в целях обеспечения:

осуществления дистанционного банковского обслуживания (далее – ДБО) в соответствии с требованиями законодательства Российской Федерации, в том числе нормативных актов Банка России, регламентирующих банковскую деятельность и управление банковскими рисками;

надёжности ДБО, отвечающей интересам клиентов кредитной организации в части функций ДБО, информационной безопасности систем ДБО, а также выполняемых в них операций и передаваемых, обрабатываемых и хранимых данных, защищённости информационных систем кредитной организации, включая системы ДБО, от сетевых атак.

1.2. В целях настоящих Рекомендаций используются следующие понятия:

система ДБО – совокупность установленных в кредитной организации (её филиалах, представительствах и внутренних структурных подразделениях) аппаратно-программных средств, с помощью которых осуществляется ДБО;

информационный контур ДБО – совокупность аппаратно-программного обеспечения и технических средств (включая средства связи) кредитной организации и её провайдеров, обеспечивающих удаленное (вне места нахождения кредитной организации и её подразделений) информационное взаимодействие кредитной организации и её клиентов<sup>1</sup>.

доступность ДБО – возможность предоставления клиенту банковских услуг на основании его ордеров, передаваемых через систему ДБО, в интервалы времени, определенные договором на оказание услуг ДБО;

функции ДБО – предоставление банковских услуг в объёме, установленном договором на оказание услуг ДБО;

защищённость систем ДБО – невозможность несанкционированного внесения изменений в их функционирование и получение несанкционированного доступа к массивам данных, хранящимся в информационных системах кредитной организации, подтвержденная наличием документально зафиксированных свидетельств принятия кредитной организацией мер в её обеспечение (полученных, например, по результатам приемо-сдаточных испытаний в кредитной организации по программе и методике их проведения, включавшим имитацию попыток таких действий);

защищённость операций – невозможность несанкционированного изменения их содержания, подтвержденная наличием документально зафиксированных свидетельств принятия кредитной организацией мер в её обеспечение (полученных, например, по результатам приемо-сдаточных

---

<sup>1</sup> Понятия «провайдер» и «ордер клиента» определены в Письме Банка России от 31 марта 2008 года № 36-Т «О рекомендациях по организации управления рисками, возникающими при осуществлении кредитными организациями операций с применением систем интернет-банкинга» («Вестник Банка России» от 09.04.2008 № 16).

испытаний в кредитной организации по программе и методике их проведения, включавшим имитацию попыток таких действий);

защищённость данных (в применении к массивам данных, обрабатываемых и / или хранящихся кредитной организацией) – невозможность их несанкционированного изменения, подтвержденная наличием документально зафиксированных свидетельств (полученных, например, по результатам приемо-сдаточных испытаний в кредитной организации по программе и методике их проведения, включавшим имитацию попыток таких действий);

сетевая информационная технология – информационная технология, реализуемая с помощью информационно-телекоммуникационных сетей;

сетевая атака – воздействие на аппаратно-программное обеспечение кредитной организации и её клиентов с применением сетевых информационных технологий с целью изменения его функционирования, воздействия на выполнение банковских операций или получения несанкционированного доступа к массивам данных, хранящимся в информационных системах кредитной организации.

Понятия «информационные технологии», «информационная система» и «информационно-телекоммуникационная сеть» определены Федеральным законом от 27 июля 2006 года № 149-ФЗ «Об информации, информационных технологиях и о защите информации» (Собрание законодательства Российской Федерации, 2006, № 31, ст. 3448).

## Раздел 2. Принципы определения подходов кредитных организаций к выбору провайдеров и организации работы с ними при оказании услуг дистанционного банковского обслуживания

2.1. При определении подходов, используемых кредитными организациями при выборе провайдеров и организации работы с ними при осуществлении ДБО, целесообразно основываться на анализе сопутствующих ему факторов риска (причин возникновения новых угроз надежности ДБО, которые могут привести к невыполнению кредитной

организацией своих обязательств перед клиентами) и компонентов банковских рисков, под которыми понимаются потенциальные угрозы надежности ДБО и которые возникают вследствие действия этих факторов; указанный анализ проводится исходя из состава провайдеров, требуемых функций и информационного контура ДБО.

2.2. Факторы риска и компоненты банковских рисков, упомянутые в пункте 2.1 настоящих Рекомендаций, рекомендуется описывать во внутреннем документе кредитной организации, регламентирующем управление банковскими рисками, с указанием на его использование в других внутренних документах кредитной организации, касающихся формирования отношений с провайдерами (включая документы, регламентирующие осуществление внутреннего контроля и обеспечение информационной безопасности).

2.3. Описания факторов риска и компонентов банковских рисков, упомянутых в пункте 2.2 настоящих Рекомендаций, рекомендуется излагать по отдельности для провайдеров кредитной организации по каждому виду предоставляемых провайдером услуг (например, доступ к сети Интернет, процессинг (обработка данных), услуги связи, хранение данных и т.д.) с указанием причин возможного возникновения этих факторов и компонентов в связи со спецификой деятельности провайдера (например, использование для связи с провайдером или использование провайдером тех или иных информационных систем, информационно-телекоммуникационных сетей, подверженность новым угрозам надежности ДБО или форс-мажорных обстоятельств, наличие у провайдера контрактов с другими сторонними организациями, от которых зависит его работа и т.д.).

2.4. При определении подходов, указанных в пункте 2.1 настоящих Рекомендаций, целесообразно оценивать возможности получения от провайдеров информации, необходимой кредитной организации для эффективного управления банковскими рисками, сопутствующими ДБО (в том числе о наличии лицензий на используемое программное обеспечение,

на систему обеспечения информационной безопасности провайдера, оборудование связи и т.п.).

### Раздел 3. Банковские риски, сопутствующие осуществлению кредитными организациями дистанционного банковского обслуживания с участием провайдеров

3.1. К банковским рискам, уровни которых могут повышаться в связи с применением кредитной организацией ДБО, относятся: операционный, правовой, стратегический, ликвидности и риск потери деловой репутации (репутационный риск). Кредитным организациям целесообразно учитывать тот факт, что переход к ДБО сопровождается усложнением структур этих рисков за счет возникновения в них новых компонентов, обусловленных не существовавшими ранее угрозами надежности кредитных организаций в связи с изменением характера и условий банковской деятельности.

3.2. Причинами повышения уровня операционного риска при использовании ДБО могут являться:

нарушения функционирования (прерывания взаимодействия между клиентом и кредитной организацией в процессе ДБО, искажения передаваемых данных) используемых для осуществления ДБО информационных систем и информационно-телекоммуникационных сетей провайдеров кредитной организации, связанные с авариями, отказами, сбоями в работе оборудования и программного обеспечения, а также недостаточно надёжной организацией обеспечения прохождения потоков данных;

недостатки в обеспечении информационной безопасности потоков данных, относящихся к информационному взаимодействию между кредитной организацией и её клиентами и проходящих через информационные системы провайдеров;

неправомерный доступ к информационным ресурсам кредитной организации с применением сетевых информационных технологий, в том числе при (для) противоправной деятельности;

недостаточная производительность информационных систем и пропускная способность информационно-телекоммуникационных сетей провайдеров, задействованных в информационном контуре ДБО;

недостатки в функционировании аппаратно-программного обеспечения (включая его низкую надёжность) провайдеров, в том числе по вине разработчиков такого обеспечения;

недостаточная защищённость информационных систем провайдеров от сетевых атак;

невыполнение сторонними поставщиками услуг (исполнителями работ) договорных обязательств перед провайдерами.

3.3. Причинами повышения уровня правового риска при ДБО могут являться:

нарушения провайдерами требований законодательства Российской Федерации, в том числе из-за недостатков в функционировании их аппаратно-программного обеспечения;

несовершенство законодательства Российской Федерации (неурегулированность отдельных вопросов ДБО и ответственности сторон, в том числе при трансграничном оказании банковских услуг с помощью ДБО), а также особенности правоотношений кредитных организаций, использующих услуги провайдеров под юрисдикцией других государств, для осуществления трансграничного информационного взаимодействия;

неправомерный доступ к конфиденциальной информации во время её обработки, передачи и (или) хранения провайдерами кредитной организации;

неэффективная организация правовой работы, приводящая к ошибкам в действиях служащих и органов управления кредитной организации при организации взаимодействия с её провайдерами, в том числе при заключении договоров (контрактов) с провайдерами на оказание услуг по выполнению

функций обработки, передачи, хранения банковской и другой информации, включая вопросы определения ответственности провайдеров при невыполнении обязательств по обеспечению осуществления ДБО, которые могут привести к невыполнению кредитной организацией своих обязательств перед клиентами, невыполнению установленных требований по обеспечению соответствия организации и содержанию банковской деятельности, невозможности предоставления информации правоохранным органам при расследовании противоправной деятельности, а также при заключении с клиентами договоров на ДБО, в том числе определение ответственности сторон при невыполнении соответствующих обязательств;

нахождение филиалов кредитной организации, её клиентов, пользующихся ДБО, и провайдеров под юрисдикцией других государств.

3.4. Причинами повышения уровня стратегического риска при ДБО могут являться возможные убытки вследствие ошибочных решений органов управления кредитной организации в отношении применения технологии ДБО и (или) внедрения, сопровождения и использования систем ДБО, и (или) выбора провайдеров, что может быть обусловлено:

отсутствием или недостатками стратегического плана развития кредитной организации, предусматривающего использование ДБО;

невозможностью достижения стратегических целей, поставленных кредитной организацией, в связи с отсутствием или не обеспечением в полном объеме необходимыми ресурсами (финансовыми, материально-техническими, людскими) и невыполнением организационных мер (управленческих решений) в части ДБО и систем, с помощью которых оно осуществляется, включая информационные системы и информационно-телекоммуникационные сети провайдеров;

ошибками в выборе видов ДБО или реализующих его технических решений, включая информационные системы и информационно-телекоммуникационные сети провайдеров;

чрезмерными затратами на внедрение и сопровождение систем ДБО и (или) их нерентабельностью, а также вынужденным отказом от услуг провайдеров (с учетом как финансовых, так и технических причин) и функционально связанными с ними информационными системами кредитной организации;

ошибками (просчетами) в политике кредитной организации, проводимой в отношении направлений банковской деятельности, связанных с применением ДБО в целом.

3.5. Причинами повышения уровня риска потери деловой репутации (репутационного риска) при ДБО могут являться:

уничтожение, искажение или хищение данных о клиентах кредитной организации, их счетах и банковских операциях и сделках в связи с сетевыми атаками в информационном контуре ДБО (в том числе нарушение банковской тайны, конфиденциальности данных и т.д.);

недоступность для клиентов кредитной организации, пользующихся ДБО, требуемых им функций системы ДБО или нарушение непрерывности функционирования аппаратно-программного обеспечения этой системы и (или) других технических средств, используемых провайдерами, приводящие к невыполнению кредитной организацией своих обязательств перед клиентами;

негативная оценка клиентами кредитной организации качества ДБО, (например, прерывание взаимодействия между клиентом и кредитной организацией в процессе ДБО, длительные задержки реакции на ордера клиентов и пр.) по причинам, связанным с невыполнением провайдерами кредитной организации своих договорных (контрактных) обязательств.

3.6. В условиях ДБО причиной повышения уровня риска ликвидности может стать неплатежеспособность кредитной организации, если своевременное или полное выполнение ею своих финансовых обязательств перед клиентами оказывается невозможно по техническим причинам, не

зависящим от неё. Причинами повышения уровня указанного риска могут являться:

отказы и сбои в компьютерных системах провайдеров (в том числе кредитных организаций-контрагентов), через которые проходит информация, необходимая для осуществления ДБО;

аварии и отказы в информационно-телекоммуникационных сетях, предоставляемых провайдерами, через которые проходит информация в рамках ДБО.

3.7. Во внутренних документах кредитной организации при описании банковских рисков, перечисленных в пункте 3.1 настоящих Рекомендаций, целесообразно отражать их зависимость от провайдеров по каждому виду деятельности в соответствии с пунктом 2.3 настоящих Рекомендаций.

3.8. При использовании кредитной организацией нескольких систем ДБО рекомендуется учитывать возможное взаимное влияние компонентов банковских рисков, сопутствующих применению каждой такой системы, ввиду их проявления в структуре разных рисков (например, сбой в работе аппаратно-программного обеспечения, являющийся причиной возникновения операционного риска, может привести к негативной реакции клиента, проявляющейся в повышении уровня репутационного риска).

3.9. При выборе провайдера целесообразно предусмотреть его информирование о подходах к управлению банковскими рисками, принятых в кредитной организации, в части, относящейся к виду предоставляемых провайдером услуг.

3.10. При необходимости привлечения для осуществления ДБО нескольких провайдеров целесообразно использовать настоящие Рекомендации при выборе каждого из них независимо друг от друга.

#### Раздел 4. Принципы учета факторов риска и компонентов банковских рисков, связанных с использованием услугами провайдеров для осуществления дистанционного банковского обслуживания

4.1. В целях обеспечения эффективности управления банковскими рисками, в состав которых входят компоненты, связанные с использованием услуг провайдеров для осуществления ДБО, органам управления кредитной организации рекомендуется при выборе провайдеров, обоснованном с точки зрения минимизации указанных рисков:

обеспечивать точное соответствие планов внедрения и развития ДБО стратегическим целям кредитной организации с учётом его возможной зависимости от провайдеров;

определить во внутреннем документе кредитной организации подходы, используемые при выборе провайдеров, необходимых в её банковской деятельности, и сопровождения (поддержания) договорных отношений с ними на долгосрочную перспективу;

определить во внутренних документах кредитной организации меры по контролю с её стороны над надёжностью провайдеров в части обеспечения ими осуществления ДБО, которое от них непосредственно зависит, а также обязанность по осуществлению данного контроля конкретным подразделением и ответственными исполнителями самой кредитной организации;

разрабатывать и внедрять процедуры мониторинга функционирования провайдеров кредитной организации и выполнения ими своих обязательств в соответствии с заключёнными с ними договорами (контрактами);

осуществлять контроль ДБО, реализуемого с участием провайдеров кредитной организации, ориентированный на снижение уровней сопутствующих банковских рисков, перечисленных в пункте 3.1 настоящих Рекомендаций;

учитывать в процессе управления банковскими рисками особенности информационного контура ДБО и применения систем ДБО в целом наряду со

специфичными для них факторами риска и компонентами банковских рисков, состав и масштабы банковских операций, осуществляемых в рамках ДБО, виды (информационная, технологическая, техническая) и степень зависимости кредитной организации и её клиентов от качества обслуживания со стороны провайдеров;

внедрять и совершенствовать процессы управления банковскими рисками, связанными с ДБО, на основе своевременного и полного выявления и анализа возможных новых компонентов банковских рисков, связанных с наличием в информационном контуре ДБО провайдеров;

оценивать возможности мониторинга функционирования провайдеров с учётом обязательств, принятых на себя кредитной организацией в отношении её клиентов, и содержания договоров на предоставление услуг, в том числе при добавлении новых банковских услуг, предоставляемых дистанционно или увеличении числа охваченных им клиентов кредитной организации и возникновении необходимости в повышении производительности систем ДБО и пропускной способности каналов справочно-информационного взаимодействия кредитной организации с клиентами;

оценивать возможности использования резервных способов и средств обслуживания клиентов в случае прекращения функционирования провайдеров без предварительного уведомления кредитной организации, а также возможности включения этих способов и средств в планы мероприятий на случай чрезвычайных обстоятельств и проведения регулярных проверок возможности реализации этих планов.

4.2. При организации управления банковскими рисками, указанными в пункте 3.1 настоящих Рекомендаций, и разработке соответствующих внутренних документов кредитной организации рекомендуется учитывать:

фактическую интеграцию технологий, используемых провайдерами, и систем, реализующих эти технологии, в информационный контур ДБО и, как

следствие, возникновение зависимости кредитной организации и её клиентов от указанных технологий и систем;

необходимость совершенствования процессов управления банковской деятельностью (включая управление банковскими рисками) и её информатизацией, внутреннего контроля, обеспечения информационной безопасности с учетом использования провайдеров для обеспечения осуществления банковской деятельности;

необходимость повышения квалификации служащих кредитной организации, отвечающих за выбор провайдеров и взаимодействие с ними.

4.3. Управление банковскими рисками рекомендуется организовывать таким образом, чтобы обеспечить контроль над ДБО в целом, в том числе с учётом возможных обязательств провайдеров относительно функционирования аппаратно-программного обеспечения их систем и соответствующих гарантий в форме документального подтверждения этого, целостности и защищенности массивов данных, образующихся в процессе банковской деятельности кредитной организации, и результатов проведения внешнего аудита работы провайдеров.

4.4. Рекомендуется участие в процессе управления банковскими рисками следующих структурных подразделений, служащих кредитной организации, прямо или косвенно участвующих в организации и обеспечении ДБО (ввиду наличия в его информационном контуре провайдеров):

структурного подразделения, отвечающего за внедрение и применение информационных технологий (информатизацию и автоматизацию банковской деятельности), взаимодействие с провайдерами, а также с поставщиками аппаратно-программного обеспечения информационных систем и разработчиками информационных систем, используемых кредитной организацией и разработанных по её заказу;

структурного подразделения, отвечающего за правовое обеспечение деятельности кредитной организации;

служащего (или структурного подразделения), ответственного за соблюдение правил внутреннего контроля, в том числе осуществляемого в целях противодействия легализации (отмыванию) доходов, полученных преступным путем, и финансированию терроризма;

структурного подразделения, отвечающего за обеспечение информационной безопасности в кредитной организации;

структурного подразделения, отвечающего за управление банковскими рисками;

структурного подразделения, отвечающего за операционную работу с клиентами;

структурного подразделения, отвечающего за справочно-информационное взаимодействие с клиентами;

структурного подразделения, отвечающего за претензионную (рекламационную) работу.

4.5. Работа структурных подразделений и служащих кредитной организации, перечисленных в пункте 4.4 настоящих Рекомендаций, целесообразно организовывать и регламентировать с учетом описаний факторов риска и компонентов банковских рисков, упомянутых в пункте 2.2 настоящих Рекомендаций, с соответствующим отражением во внутренних документах об этих подразделениях и должностных инструкциях их руководителей и сотрудников (служащих).

4.6. В состав структурных подразделений кредитной организации, перечисленных в пункте 4.4 настоящих Рекомендаций, рекомендуется включать служащих, квалификация которых позволяет обеспечивать решение задач по применению и развитию ДБО на основе понимания причин возникновения рисков, связанных с наличием провайдеров кредитной организации в информационном контуре ДБО.

4.7. Определение подчинённости и подотчётности руководителей и ответственных исполнителей кредитной организации в рамках управления банковскими рисками, связанными с ДБО, и взаимодействия с её

провайдерами, рекомендуется организовывать таким образом, чтобы обеспечить непрерывность, своевременность, полноту и адекватность информирования органов управления кредитной организации:

- о текущем состоянии и характеристиках провайдеров, включая их финансовое состояние и технические параметры информационных и иных систем, использование которых предусмотрено договорами (контрактами), а также о перспективах выполнения ими принятых на себя обязательств перед кредитной организацией;

- о выявленных недостатках в функционировании информационного контура ДБО в связи с недостатками в работе провайдеров (несоответствующим качеством предоставляемых услуг);

- о связанных с ДБО факторах риска и компонентах банковских рисков;

- о результатах выполнения принятых решений по управлению банковскими рисками, в том числе в отношении провайдеров кредитной организации;

- о процедурах реагирования на события, которые могут негативно повлиять на безопасность, финансовую устойчивость или деловую репутацию кредитной организации (например, любые существенные нарушения в использовании информационных систем и (или) информационно-телекоммуникационных сетей, инциденты информационной безопасности (данное понятие введено Стандартом Банка России СТО ИББС-1.0-2010 «Обеспечение информационной безопасности организаций банковской системы Российской Федерации. Общие положения»), критическое финансовое состояние провайдера и т.д.) и результатах выполнения этих процедур.

4.8. Кредитной организации в интересах обеспечения экономической эффективности привлечения провайдеров к обеспечению осуществления ею ДБО и снижения уровней сопутствующих ДБО банковских рисков рекомендуется выбирать провайдера для конкретного направления

банковской деятельности на основе открытого или закрытого конкурса, учитывая, в том числе, следующие характеристики провайдера:

опыт в данной области предоставления услуг;

характеристики технического обеспечения предоставления услуг (надежность автоматизированных систем и систем связи, средства обеспечения этой надежности, состояние обеспечения информационной безопасности и защиты информации и пр.);

квалификация персонала, от которого прямо или косвенно зависит выполнение договорных обязательств;

мнение других клиентов (данного провайдера) о качестве предоставляемых услуг;

стоимость и условия предоставления услуг;

возможности мониторинга деятельности провайдера со стороны кредитной организации;

возможность заключения соглашения об уровне сервиса (Service Level Agreement), включая в них обслуживание автоматизированных систем, от которых зависит надежность кредитной организации).

4.9. Кредитной организации целесообразно при выборе провайдера учитывать стратегический план развития, прежде всего, ДБО.

4.10. Кредитной организации рекомендуется оценить возможности выполнения минимально необходимых функций в части мониторинга надёжности информационных систем провайдера, его финансового состояния, а также обеспечения им информационной безопасности потоков данных, передаваемых между кредитной организацией и её клиентами.

4.11. Кредитной организации рекомендуется оценить возможности оказания методологической и консультационной помощи своим клиентам, пользующимся системами ДБО, доведения до них информации о принимаемых ими рисках, связанных с ДБО и возможно связанных с участием в ДБО того или иного провайдера.

4.12. Принятие решений при выборе провайдера кредитной организации, взаимодействие с которым необходимо для осуществления ДБО клиентов, целесообразно основывать на результатах анализа возможных банковских рисков. Рекомендуется предусмотреть резервные варианты ДБО клиентов в случае невозможности выполнения провайдером обязательств перед кредитной организацией.

4.13. В целях минимизации (снижения уровней) банковских рисков, сопутствующих осуществлению кредитными организациями ДБО с участием провайдеров и вызванных недостатками в обеспечении провайдерами информационной безопасности в информационном контуре ДБО, рекомендуется:

на основе описания факторов риска и компонентов банковских рисков определить во внутреннем документе кредитной организации соответствующие требования к обеспечению информационной безопасности (в том числе в зависимости от видов деятельности и технологий, используемых провайдерами);

при формировании требований к обеспечению информационной безопасности систем ДБО учитывать положения Стандарта Банка России СТО БР ИББС-1.0-2010 «Обеспечение информационной безопасности организаций банковской системы Российской Федерации. Общие положения»;

при выборе провайдеров оценивать степень реализации провайдером требований к обеспечению информационной безопасности, определенных кредитной организацией, а также возможность проведения дальнейшего контроля выполнения указанных требований с её стороны, при этом отказ провайдера в осуществлении такого контроля рекомендуется рассматривать как негативный фактор, влияющий на заключение договора (контракта) с ним.

4.14. Кредитной организации рекомендуется при выборе провайдеров оценивать возможность включения в договора (контракты) с ними

требований по обеспечению информационной безопасности, а также по осуществлению как внутреннего, так и внешнего аудита (в том числе – информационной безопасности).

4.15. Кредитной организации рекомендуется оценить возможность использования результатов независимого внешнего аудита провайдера.