ЦЕНТРАЛЬНЫЙ БАНК РОССИЙСКОЙ ФЕДЕРАЦИИ

ПИСЬМО
от 31 марта 2008 г. N 36-Т

О РЕКОМЕНДАЦИЯХ ПО ОРГАНИЗАЦИИ УПРАВЛЕНИЯ РИСКАМИ, ВОЗНИКАЮЩИМИ ПРИ ОСУЩЕСТВЛЕНИИ КРЕДИТНЫМИ ОРГАНИЗАЦИЯМИ ОПЕРАЦИЙ С ПРИМЕНЕНИЕМ СИСТЕМ ИНТЕРНЕТ-БАНКИНГА

В соответствии с Положением Банка России от 16 декабря 2003 года N 242-П "Об организации внутреннего контроля в кредитных организациях и банковских группах", зарегистрированным Министерством юстиции Российской Федерации 27 января 2004 года N 5489, 22 декабря 2004 года N 6222 ("Вестник Банка России" от 4 февраля 2004 года N 7, от 31 декабря 2004 года N 74) одной из целей внутреннего контроля является обеспечение эффективного управления банковскими рисками.

Банком России направляются для использования в работе Рекомендации по организации управления рисками, возникающими при осуществлении кредитными организациями операций с применением систем интернет-банкинга.

Настоящее Письмо подлежит опубликованию в "Вестнике Банка России".

Первый заместитель Председателя
Центрального банка
Российской Федерации
Г.Г.МЕЛИКЬЯН

Приложение
к Письму Банка России
от 31 марта 2008 г. N 36-Т
"О Рекомендациях по организации
управления рисками, возникающими
при осуществлении кредитными
организациями операций
с применением систем
интернет-банкинга"

РЕКОМЕНДАЦИИ
ПО ОРГАНИЗАЦИИ УПРАВЛЕНИЯ РИСКАМИ, ВОЗНИКАЮЩИМИ ПРИ ОСУЩЕСТВЛЕНИИ КРЕДИТНЫМИ ОРГАНИЗАЦИЯМИ ОПЕРАЦИЙ С ПРИМЕНЕНИЕМ СИСТЕМ ИНТЕРНЕТ-БАНКИНГА

Раздел 1. Общие положения

1.1. Для целей настоящих Рекомендаций используются следующие понятия:

Интернет-банкинг - способ дистанционного банковского обслуживания клиентов, осуществляемого кредитными организациями в сети Интернет (в том числе через WEB-сайт(ы) в сети Интернет <*>) и включающего информационное и операционное взаимодействие с ними.

<*> Определения понятий "WEB-сайт", "WEB-сервер" содержатся в Рекомендациях по информационному содержанию и организации WEB-сайтов кредитных организаций в сети Интернет (приложение к Указанию оперативного характера Банка России от 03.02.2004 N 16-Т "О Рекомендациях по информационному содержанию и организации WEB-сайтов кредитных организаций в сети Интернет", "Вестник Банка России" от 11 февраля 2004 года N 11).

Информационный контур интернет-банкинга - совокупность взаимосвязанных компьютерных систем, устройств и каналов связи, используемых при обслуживании клиента (передаче информации от кредитной организации к клиенту и обратно с использованием сети Интернет, а также при обработке и хранении

данной информации).

Провайдер - организация, предоставляющая кредитным организациям услуги по выполнению функций обработки, передачи, хранения банковской и другой информации, а также обеспечивающая доступ к информационно-телекоммуникационным сетям.

Система интернет-банкинга - информационная система, используемая кредитной организацией для обслуживания клиентов в сети Интернет.

Риски интернет-банкинга - риски, возникающие при осуществлении кредитными организациями операций с применением систем интернет-банкинга.

Ордер клиента - любое дистанционное обращение клиента кредитной организации с помощью системы интернет-банкинга за оказанием банковских услуг (получение выписки со счета, осуществление банковской операции и так далее).

1.2. Настоящие Рекомендации разработаны в целях обеспечения:

надежного дистанционного банковского обслуживания с применением систем интернет-банкинга, отвечающего требованиям клиентов кредитной организации в части доступности, функциональности и защищенности операций и данных интернет-банкинга;

соответствия дистанционного банковского обслуживания с применением систем интернет-банкинга требованиям законодательства Российской Федерации, в том числе нормативных актов Банка России, по вопросам банковской деятельности и управления банковскими рисками;

информационной безопасности систем интернет-банкинга, в том числе защиты информационных ресурсов кредитной организации от неправомерного доступа с применением интернет-технологий;

контроля за банковскими операциями, осуществляемыми клиентами с применением систем интернет-банкинга, в рамках системы внутреннего контроля кредитной организации;

противодействия легализации (отмыванию) доходов, полученных преступным путем, и финансированию терроризма, а также исключению вовлечения кредитной организации в противоправную деятельность при использовании дистанционного банковского обслуживания с применением систем интернет-банкинга;

достоверности, полноты и своевременности учета данных об осуществлении банковских операций с применением систем интернет-банкинга;

поддержания уровней банковских рисков, связанных с дистанционным банковским обслуживанием с применением систем интернет-банкинга, в пределах, установленных кредитной организацией.

Раздел 2. Банковские риски, возникающие при осуществлении кредитными организациями операций с применением систем интернет-банкинга

2.1. К банковским рискам, связанным с применением систем интернет-банкинга, относятся: операционный, правовой, стратегический риски, риск потери деловой репутации (репутационный риск) и риск ликвидности.

2.2. Причинами возникновения операционного риска при применении систем интернет-банкинга могут являться:

ненадлежащая организация информационных потоков, внутрибанковских процессов и процедур, а также обеспечения информационной безопасности как в самой кредитной организации, так и у провайдеров;

нарушения режимов функционирования используемых для интернет-банкинга информационных систем кредитной организации, связанные с авариями, отказами, сбоями оборудования и программного обеспечения самой кредитной организации или ее провайдеров;

ошибки и (или) сбои в работе аппаратно-программного обеспечения применяемых кредитной организацией систем интернет-банкинга, которые могут привести к нарушениям целостности данных в информационном контуре интернет-банкинга;

действия в отношении кредитной организации в виде неправомерного доступа с применением интернет-технологий к ее информационным ресурсам, в том числе при (для) совершении(я) преступных действий;

недостаточная производительность и защищенность информационных систем и информационно-телекоммуникационных сетей как кредитной организации, так и провайдеров, задействованных в информационном контуре интернет-банкинга (с учетом возможного неправомерного доступа с применением интернет-технологий);

ошибки служащих кредитной организации, ее клиентов или провайдеров (в том числе разработчиков программного обеспечения систем интернет-банкинга и устройств, входящих в информационный контур интернет-банкинга), а также недостаточный уровень контроля (в том числе программного) за возможностью их совершения;

невыполнение поставщиками услуг (исполнителями работ) договорных обязательств перед кредитной организацией;

невыполнение кредитной организацией обязательств перед клиентами из-за ненадлежащего качества аппаратно-программного обеспечения систем интернет-банкинга;

хищения денежных средств путем неправомерного использования ключа электронной цифровой подписи.

2.3. Причинами возникновения правового риска при применении систем интернет-банкинга могут являться:

нарушения кредитной организацией требований законодательства Российской Федерации, в том числе нормативных актов Банка России, из-за недостатков (ошибок) в аппаратно-программном обеспечении систем интернет-банкинга, результатом чего является возникновение оснований для применения мер за нарушения валютного законодательства Российской Федерации, банковской тайны, порядка организации и осуществления внутреннего контроля, в том числе в целях противодействия легализации (отмыванию) доходов, полученных преступным путем, и финансированию терроризма, правил осуществления банковских операций, правил бухгалтерского учета, представления недостоверной отчетности;

несовершенство правовой системы (неурегулированность отдельных вопросов дистанционного банковского обслуживания с применением систем интернет-банкинга и ответственности сторон, в том числе при трансграничном оказании банковских услуг);

неправомерный доступ к конфиденциальной информации во время ее обработки, передачи или хранения как в самой кредитной организации, так и у провайдеров, с которыми кредитной организацией заключены договоры на обслуживание;

несоответствие внутренних документов кредитной организации законодательству Российской Федерации, в том числе нормативным, а также иным актам Банка России, и (или) неспособность кредитной организации своевременно приводить свою деятельность и внутренние документы в соответствие с изменениями законодательства;

неэффективная организация правовой работы, приводящая к ошибкам в действиях служащих и органов управления кредитной организации при разработке и внедрении новых интернет-технологий;

недостаточность проработки кредитной организацией правовых вопросов при заключении договоров с провайдерами на оказание услуг по выполнению функций обработки, передачи, хранения банковской и другой информации, в том числе определение ответственности провайдеров при невыполнении обязательств по обслуживанию в рамках интернет-банкинга;

недостаточность проработки кредитной организацией правовых вопросов при заключении договоров с клиентами на оказание услуг интернет-банкинга, в том числе определение ответственности сторон при невыполнении обязательств;

нахождение филиалов кредитной организации, ее клиентов, пользующихся услугами интернет-банкинга, и провайдеров под юрисдикцией различных государств;

нарушения условий договоров со стороны как кредитной организации, так и ее клиентов и контрагентов.

2.4. Причинами возникновения стратегического риска при применении систем интернет-банкинга могут являться возможные убытки вследствие ошибочных решений органов управления кредитной организации в отношении внедрения, сопровождения и развития систем интернет-банкинга, что может быть обусловлено:

отсутствием или недостатками стратегического плана развития, предусматривающего применение систем интернет-банкинга;

невозможностью достижения стратегических целей, поставленных кредитной организацией, в связи с отсутствием или необеспечением в полном объеме необходимыми ресурсами (финансовыми, материально-техническими, людскими) и невыполнением организационных мер (управленческих решений) в области предоставления услуг интернет-банкинга;

чрезмерными затратами на внедрение и сопровождение систем интернет-банкинга и (или) их нерентабельностью, а также вынужденным отказом от использования уже внедренных в эксплуатацию технологий банковского обслуживания и соответствующих информационных систем кредитной организации;

ошибками в выборе видов услуг интернет-банкинга или реализующих его технических решений;

ошибками в политике кредитной организации по тем или иным направлениям банковской деятельности, связанным с применением систем интернет-банкинга.

2.5. Причинами возникновения риска потери деловой репутации (репутационного риска) при применении систем интернет-банкинга могут являться:

уничтожение данных о клиентах кредитной организации, их счетах и вкладах в связи с отказами оборудования, входящего в информационный контур интернет-банкинга, как в самой кредитной организации, так и у провайдеров;

утечка из кредитной организации конфиденциальной информации, в том числе нарушение банковской тайны (из-за сетевых атак в условиях дистанционного банковского обслуживания с применением систем интернет-банкинга, неправомерного доступа к информационным ресурсам кредитной организации и т.п.);

вовлечение кредитной организации в противоправную деятельность с применением систем интернет-банкинга из-за ненадлежащего исполнения обязанностей по идентификации клиентов, установления и идентификации выгодоприобретателей и установления личности лица (лиц), уполномоченного (уполномоченных) распоряжаться денежными средствами, находящимися на счете, используя аналог собственноручной подписи, коды, пароли и иные средства, подтверждающие наличие указанных полномочий, а также ошибок в сообщениях об авторизации и аутентификации при осуществлении банковских операций;

неправомерные воздействия на информацию, размещенную на WEB-сайте, используемом кредитной организацией, и (или) размещение на нем недостоверной, неполной или нежелательной для кредитной организации информации, негативно влияющей на ее деловую репутацию;

возникновение у кредитной организации конфликта интересов с учредителями (участниками), клиентами и контрагентами, а также другими заинтересованными лицами при осуществлении операций с применением систем интернет-банкинга;

негативная оценка клиентами качества предоставляемого дистанционного банковского обслуживания с применением систем интернет-банкинга;

нарушения непрерывности функционирования систем интернет-банкинга.

2.6. Причинами возникновения риска ликвидности при применении систем интернет-банкинга могут являться:

недостатки при управлении ликвидностью в условиях применения систем интернет-банкинга, препятствующие своевременному и полному выполнению кредитной организацией своих обязательств перед клиентами;

негативное влияние на выполнение обязательств кредитной организации нарушений в функционировании информационно-телекоммуникационных сетей, используемых для работы систем интернет-банкинга;

невозможность реализации высоколиквидных активов по причине сбоев в системах интернет-банкинга (а также в системах и комплексах провайдеров);

нарушения непрерывности функционирования систем интернет-банкинга;

использование систем интернет-банкинга для противоправных действий, наносящих ущерб клиентам кредитной организации или ей самой.

2.7. При использовании кредитной организацией нескольких систем интернет-банкинга рекомендуется учитывать возможное взаимное влияние источников (факторов) банковских рисков, сопутствующих каждой из этих систем.

Раздел 3. Принципы управления рисками интернет-банкинга

3.1. Управление рисками интернет-банкинга рекомендуется организовывать таким образом, чтобы обеспечить контроль за данным видом дистанционного банковского обслуживания в целом, в том числе в рамках функционирования аппаратно-программного обеспечения систем интернет-банкинга, осуществления отдельных операций и используемых при этом массивов банковских данных.

3.2. При организации управления рисками интернет-банкинга и принятии внутренних документов кредитной организации рекомендуется учитывать:

высокие темпы инновационных процессов в технологиях интернет-банкинга;

рост зависимости кредитной организации от информационных технологий в целом и от эффективности построения внутрибанковских автоматизированных систем;

интеграцию новых интернет-технологий в действующие внутрибанковские автоматизированные системы;

повышенную степень риска при осуществлении операций с применением систем интернет-банкинга ввиду возможности легализации (отмывания) доходов, полученных преступным путем, и финансирования терроризма;

необходимость совершенствования процессов управления банковской деятельностью и внутреннего контроля с учетом применения интернет-технологий;

необходимость повышения квалификации служащих кредитной организации и совершенствования управления рисками интернет-банкинга.

3.3. В целях обеспечения эффективности управления рисками, возникающими при осуществлении кредитными организациями операций с применением систем интернет-банкинга, органам управления кредитной организации (совету директоров (наблюдательному совету), единоличному и коллегиальному исполнительным органам) рекомендуется:

обеспечивать точное соответствие планов внедрения и развития обслуживания клиентов с помощью систем интернет-банкинга стратегическим целям;

разрабатывать и внедрять процедуры мониторинга банковских операций, осуществляемых с применением систем интернет-банкинга;

осуществлять контроль за дистанционным банковским обслуживанием с применением систем интернет-банкинга, ориентированный на снижение сопутствующих рисков;

внедрять и совершенствовать процессы управления рисками интернет-банкинга на основе своевременного и адекватного выявления, анализа и мониторинга возможных новых источников (факторов) рисков, связанных с усложнением внутрибанковских автоматизированных систем и появлением в информационном контуре интернет-банкинга новых участников, например, провайдеров;

учитывать в процессе управления банковскими рисками особенности применения систем интернет-банкинга и интернет-технологий в целом наряду со специфичными для них источниками (факторами) рисков, виды и масштабы банковских операций, осуществляемых в рамках интернет-банкинга, применяемые способы анализа, контроля и обработки ордеров клиентов, состав клиентской базы в целом (с учетом возможностей легализации (отмывания) доходов, полученных преступным путем, и финансирования терроризма), а также структуру кредитной организации и распределение функций, имеющих отношение к работе в рамках интернет-банкинга;

осуществлять мониторинг процессов управления интернет-технологиями в целом, разработку и внедрение процедур, реализующих данный процесс управления, наряду с созданием дополнительных средств контроля в целях управления рисками интернет-банкинга;

организовывать мониторинг и обеспечивать своевременное (упреждающее) повышение производительности внутрибанковских автоматизированных систем, с помощью которых осуществляется обслуживание в рамках интернет-банкинга, по мере расширения его клиентской базы, развития предоставляемых с его помощью банковских услуг и расширения потребностей клиентов;

предусматривать способы и средства обслуживания клиентов в случае неожиданного прекращения функционирования провайдеров и (или) систем интернет-банкинга, разрабатывать планы необходимых мероприятий на случай чрезвычайных обстоятельств и проводить регулярные проверки возможности их реализации;

устанавливать порядок (правила) применения систем интернет-банкинга (разработка, приобретение, документирование, ввод в эксплуатацию, эксплуатация, модернизация, вывод из эксплуатации) и выполнения реализуемых ими процедур предоставления банковских услуг.

3.4. Рекомендуется участие в процессе управления рисками интернет-банкинга следующих структурных подразделений (служб, служащих кредитной организации), прямо или косвенно участвующих в интернет-банкинге (в случае наличия):

структурного подразделения, отвечающего за внедрение и применение информационных технологий (информатизацию и автоматизацию банковской деятельности), в том числе интернет-технологий, функционирование систем интернет-банкинга, а также за взаимодействие с провайдерами и поставщиками аппаратно-программного обеспечения систем интернет-банкинга;

структурного подразделения, отвечающего за ведение бухгалтерского учета в кредитной организации (реализацию учетной политики), практическую реализацию алгоритмов учета в компьютерных программах, управляющих работой внутрибанковских автоматизированных систем, связанных с системами интернет-банкинга, и подготовку банковской отчетности;

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

структурного подразделения, отвечающего за правовое обеспечение деятельности кредитной организации;

структурного подразделения, отвечающего за операционную работу с клиентами;

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

структурного подразделения, осуществляющего справочно-информационное взаимодействие с клиентами.

3.5. В состав структурных подразделений кредитной организации, участвующих в процессе дистанционного банковского обслуживания с применением систем интернет-банкинга, службах внутреннего контроля (внутреннего аудита) и информационной безопасности, а также структурных подразделений, осуществляющих мониторинг и оценку рисков интернет-банкинга, рекомендуется включать служащих, удовлетворяющих квалификационным требованиям, позволяющим обеспечивать решение задач по применению и развитию интернет-банкинга, а также понимание причин возникновения рисков интернет-банкинга.

3.6. При организации управления рисками интернет-банкинга целесообразно обеспечить

разграничение общего руководства таким образом, чтобы поддерживать:

непрерывность управления (передачи управленческих функций в организационной структуре кредитной организации) с охватом всех процессов и процедур, необходимых для осуществления обслуживания клиентов в рамках интернет-банкинга и обеспечения его надежности за счет удержания уровней банковских рисков в допустимых пределах;

доступность систем интернет-банкинга и выполнение всех функций, указанных в договорах с клиентами, а также защищенность операций и данных интернет-банкинга за счет создания и поддержания в кредитной организации необходимых для этого условий, включая надлежащее организационно-техническое обеспечение интернет-банкинга;

адекватный характеру и масштабам банковских операций с применением систем интернет-банкинга порядок согласования (утверждения) внутренних документов по вопросам управления рисками интернет-банкинга.

3.7. Распределение подчиненности и подотчетности в рамках управления рисками интернет-банкинга рекомендуется организовывать таким образом, чтобы обеспечить непрерывность, своевременность, полноту и адекватность информирования органов управления кредитной организации:

о состоянии и характеристиках аппаратно-программного обеспечения систем интернет-банкинга;

о выявленных недостатках в функционировании информационного контура интернет-банкинга;

о связанных с интернет-банкингом источниках (факторах) рисков;

о результатах выполнения принятых решений по управлению банковскими рисками;

о процедурах реагирования на возможные события, которые могут негативно повлиять на безопасность, финансовую устойчивость или деловую репутацию кредитной организации (например, неправомерный доступ к информационным ресурсам, нарушение правил безопасности со стороны служащих, выход из строя аппаратно-программного обеспечения систем интернет-банкинга, любые серьезные нарушения в использовании компьютерных систем), и результатах их выполнения.

3.8. Управление рисками интернет-банкинга рекомендуется организовывать таким образом, чтобы обеспечить:

предоставление клиентам услуг интернет-банкинга на согласованной и своевременной основе;

установку правил авторизации и способов аутентификации осуществляемых банковских операций;

контроль логического и физического доступа к аппаратно-программному обеспечению систем интернет-банкинга;

адекватную структуру обеспечения безопасности для соблюдения установленных прав и полномочий пользователей интернет-банкинга;

целостность выполнения операций, записей баз данных и передаваемой в системах интернет-банкинга информации;

ведение внутрисистемных компьютерных журналов для всех осуществляемых в рамках интернет-банкинга банковских операций;

принятие мер по соблюдению конфиденциальности клиентской и другой внутрибанковской информации, а также банковской тайны;

полноту и достоверность информации, представляемой на WEB-сайтах, используемых кредитной организацией;

эффективные механизмы реагирования на сбои в обслуживании клиентов и осуществления банковских операций в рамках интернет-банкинга;

идентификацию клиентов, выгодоприобретателей и лица (лиц), уполномоченного (уполномоченных) распоряжаться денежными средствами, находящимися на счетах, к которым имеется доступ посредством интернет-банкинга, с использованием аналогов собственноручной подписи, кодов, паролей и других средств подтверждения наличия таких полномочий;

организацию антивирусной защиты;

предотвращение неправомерного доступа к информационным ресурсам кредитной организации и возможных хищений денежных средств.

3.9. Кредитной организации рекомендуется оказывать методологическую и консультационную помощь клиентам интернет-банкинга, доводить до них информацию о принимаемых ими рисках, а также необходимом комплексе мер по защите информации.

3.10. Кредитным организациям, предполагающим оказание клиентам (в том числе находящимся за рубежом) трансграничных банковских услуг посредством интернет-банкинга, рекомендуется предварительно изучить возможные дополнительные источники (факторы) банковских рисков, связанных с нарушением законодательства зарубежных государств и (или) территорий, а также возможности учета факторов риска, относящихся к той или иной стране или юрисдикции, в том числе в соответствии с рекомендациями Группы разработки финансовых мер борьбы с отмыванием денег (ФАТФ) <*>.

<*> Рекомендации 8 - 10 Сорока Рекомендаций ФАТФ.

3.11. Принятие решений при выборе провайдеров кредитной организации, взаимодействие с которыми необходимо для осуществления обслуживания клиентов в рамках интернет-банкинга, целесообразно основывать на анализе возможных банковских рисков. Рекомендуется предусмотреть резервные варианты обслуживания клиентов в рамках интернет-банкинга в случае невозможности выполнения провайдером обязательств перед кредитной организацией.

3.12. Кредитной организации рекомендуется в рамках управления рисками интернет-банкинга разработать и внедрить непрерывные процессы наблюдения и контроля за выполнением обязательств провайдеров, участвующих в обеспечении интернет-банкинга.

3.13. Для снижения влияния факторов рисков, связанных с деятельностью провайдеров по обработке банковских данных, кредитной организации рекомендуется организовать контроль за:

определением обязательств по договорам с провайдерами (например, в случае неисполнения или ненадлежащего исполнения обязательств);

учетом всех операций и систем интернет-банкинга, зависящих от провайдеров, в процессах обеспечения выполнения обязательств перед клиентами, целостности банковских данных, защиты информации и соблюдения ее конфиденциальности, выявления и мониторинга банковских рисков;

проведением периодического независимого внутреннего и (или) внешнего аудита содержания и оценки качества выполнения провайдерами предусмотренных договорами функций по меньшей мере в том же объеме, который осуществлялся бы при выполнении таких операций самой кредитной организацией.

3.14. Кредитной организации рекомендуется в рамках заключаемых договоров предъявлять к провайдерам требования по осуществлению внутреннего контроля и организации обеспечения информационной безопасности.

Раздел 4. Внутренние документы кредитной организации, устанавливающие порядок управления рисками интернет-банкинга

4.1. Внутренними документами кредитной организации рекомендуется регламентировать работу на всех технологических участках информационного контура интернет-банкинга, организационное и информационное взаимодействие с клиентами и провайдерами, а также функционирование аппаратно-программного обеспечения интернет-банкинга.

4.2. Во внутренних документах кредитной организации, связанных с управлением интернет-банкингом и контролем за функционированием реализующих его систем, рекомендуется определить:

4.2.1. Роль органов управления и структурных подразделений кредитной организации, в том числе:

распределение полномочий между органами управления кредитной организации (совет директоров (наблюдательный совет), единоличный и коллегиальный исполнительные органы);

распределение прав и обязанностей, ответственности, подчиненности и подотчетности структурных подразделений кредитной организации, служащих кредитной организации, в обязанности которых входит выполнение функций в рамках интернет-банкинга и управление связанными с ним рисками интернет-банкинга;

реализация учетной политики кредитной организации во внутрибанковских автоматизированных системах с учетом особенностей применения систем интернет-банкинга;

определение допустимых уровней банковских рисков, принимаемых кредитной организацией при использовании систем интернет-банкинга;

определение порядка информирования органов управления кредитной организации о выявленных источниках (факторах) банковских рисков и принятие мер, обеспечивающих снижение уровня рисков.

4.2.2. Порядок обеспечения непрерывности управления, в том числе:

испытание систем интернет-банкинга на соответствие требованиям, предъявляемым к осуществлению банковских операций;

меры по обеспечению надежности функционирования систем, с помощью которых осуществляется обслуживание в рамках интернет-банкинга (в том числе внутрибанковских автоматизированных систем кредитной организации, систем и комплексов провайдеров);

взаимосвязанные внутрибанковские процессы и процедуры, необходимые для осуществления обслуживания в рамках интернет-банкинга;

план действий на случай чрезвычайных обстоятельств с учетом специфики интернет-банкинга, включающий меры по предотвращению влияния источников (факторов) рисков, а также меры по защите интересов кредитной организации и ее клиентов, пользующихся интернет-банкингом, включая восстановление обслуживания;

документирование и анализ информации о сетевых атаках, других противоправных действиях, о нарушениях функционирования систем интернет-банкинга и доведение этой информации до органов

управления кредитной организации;

действия при возникновении нештатных ситуаций во внутрибанковских автоматизированных системах кредитной организации, связанных с осуществлением операций интернет-банкинга (включая умышленные повреждения, сетевые и вирусные атаки), и в системах и комплексах провайдеров (с описаниями мероприятий по выявлению нарушений и защите от них функционирования информационного контура интернет-банкинга, попыток неправомерного доступа к программно-информационным ресурсам и мер по их предупреждению, а также порядок информирования органов управления кредитной организации о таких ситуациях).

4.2.3. Порядок управления рисками интернет-банкинга, в том числе:

описание наиболее вероятных внутренних и внешних источников (факторов) рисков интернет-банкинга;

разработка различных способов оценки и минимизации рисков интернет-банкинга;

организация процесса управления рисками интернет-банкинга и мониторинга источников (факторов) рисков интернет-банкинга;

назначение ответственного лица (лиц) за реализацию процессов управления рисками интернет-банкинга и их мониторинга.

4.2.4. Требования к организационно-техническому обеспечению в части:

организации, ведения, сопровождения (поддержания функционирования), модернизации и закрытия (отказ от использования) WEB-сайта, применяемого для интернет-банкинга, а также распределения обязанностей, ответственности, подотчетности и контроля в отношении содержания WEB-сайта <*>;

<*> Рекомендации по содержанию WEB-сайтов приведены в Указании оперативного характера Банка России от 3 февраля 2004 г. N 16-Т "О Рекомендациях по информационному содержанию и организации WEB-сайтов кредитных организаций в сети Интернет" и в Письме Банка России от 19 января 2005 г. N 8-Т "О сведениях, рекомендуемых для размещения на WEB-сайтах кредитных организаций в сети Интернет" ("Вестник Банка России" от 26 января 2005 года N 4).

порядка пользования сетью Интернет служащими кредитной организации;

разграничения прав и полномочий доступа служащих кредитной организации к системам интернет-банкинга;

планирования, внедрения, применения (эксплуатации), модификации в случае модернизации обслуживания в рамках интернет-банкинга;

содержания технического описания внутрибанковских автоматизированных систем, на которых основаны и реализованы системы интернет-банкинга, в том числе схемы вычислительной сети кредитной организации с указанием потоков данных (передаваемых, обрабатываемых и хранимых);

содержания инструкций, правил, руководств и иных документов для операторов внутрибанковских автоматизированных систем, администраторов этих систем и администраторов информационной безопасности, а также служащих кредитной организации, обслуживающих эти системы;

актуализации документации на технические средства, используемые кредитной организацией для интернет-банкинга, а также контроль их модификации (в том числе меры по предотвращению внесения несанкционированных изменений в соответствующее аппаратно-программное обеспечение систем интернет-банкинга и в информационные массивы);

установления договорных отношений с клиентами, пользующимися услугами интернет-банкинга, и контроля выполнения обязательств сторон;

установления договорных отношений с провайдерами и контроля выполнения обязательств сторон.

4.2.5. Порядок обеспечения информационной безопасности в части:

политики обеспечения информационной безопасности с учетом особенностей интернет-банкинга, внешних и внутренних угроз информационной безопасности и защите банковских операций и данных, возможных сценариев реализации угроз, а также способов противодействия таким угрозам, как неправомерное уничтожение, изменение, копирование данных, доступ к ним со стороны неуполномоченных лиц;

методической и консультационной помощи клиентам, доведения до них информации о принимаемых рисках, информирования клиентов об осуществляемых по их счетам операциях, а также о типичных признаках противоправных действий и о необходимом комплексе мер по защите информации.

4.2.6. Порядок обеспечения внутреннего контроля в части:

состава системы внутреннего контроля с учетом особенностей интернет-банкинга, в том числе описания встроенных средств автоматизированного (программного) контроля, используемых для целей противодействия легализации (отмыванию) доходов, полученных преступным путем, и финансированию терроризма, а также для выявления и документирования подозрительных операций;

действий по выявлению нарушений и недостатков при осуществлении кредитными организациями

банковских операций с применением систем интернет-банкинга;

действий по устранению нарушений и недостатков, выявленных службой внутреннего контроля.

4.2.7. Порядок противодействия легализации (отмыванию) доходов, полученных преступным путем, и финансированию терроризма в части:

взаимодействия подразделений информатизации, информационной безопасности, службы внутреннего контроля и служащего (структурного подразделения), ответственного за соблюдение правил внутреннего контроля в целях противодействия легализации (отмыванию) доходов, полученных преступным путем, и финансированию терроризма;

установления и идентификации выгодоприобретателей и установления личности лица (лиц), уполномоченного (уполномоченных) распоряжаться денежными средствами, находящимися на счете, используя аналог собственноручной подписи, коды, пароли и иные средства, подтверждающие наличие указанных полномочий;

идентификации и изучения клиентов интернет-банкинга (в первую очередь клиентов, с которыми кредитная организация осуществляет банковские операции с повышенной степенью риска) и соблюдения принципа "Знай своего клиента".

Раздел 5. Информационное обеспечение управления рисками интернет-банкинга

5.1. Кредитной организации рекомендуется организовать и контролировать процесс информационного обеспечения в целях эффективного управления рисками интернет-банкинга, выработки мотивированных решений в отношении применения систем интернет-банкинга и принятия мер по снижению и исключению влияния возможных источников (факторов) указанных рисков.

5.2. В состав информационного обеспечения управления рисками интернет-банкинга рекомендуется включать сведения по следующим направлениям:

5.2.1. Обслуживание в рамках интернет-банкинга, в том числе:

предлагаемые услуги и виды банковского обслуживания в сети Интернет (в том числе мобильные системы);

состав клиентской базы интернет-банкинга и ее динамика;

объемы денежных средств на счетах клиентов, управление которыми осуществляется клиентами в сети Интернет (в рублях и в иностранной валюте), их динамика и обороты, в том числе в составе операций с клиентами, находящимися за рубежом (в отношении резидентов и нерезидентов);

состав и численность обособленных подразделений и внутренних структурных подразделений кредитной организации, участвующих в обслуживании клиентов интернет-банкинга;

состав и численность структурных подразделений, осуществляющих информатизацию и автоматизацию банковской деятельности;

результаты использования интернет-банкинга (в сопоставлении с бизнес-планом кредитной организации).

5.2.2. Техническое оснащение интернет-банкинга, в том числе:

состав и характеристики аппаратно-программного обеспечения систем интернет-банкинга и внутрибанковских автоматизированных систем кредитной организации (с особым вниманием к возможным конструктивным и эксплуатационным недостаткам);

структурная схема внутрибанковской вычислительной сети и каналов связи с сетью Интернет, состав и характеристики специальных аппаратно-программных средств, обеспечивающих их функционирование;

содержание внесенных в используемые внутрибанковские автоматизированные системы изменений в связи с внедрением интернет-банкинга;

состав средств обеспечения бесперебойной работы систем интернет-банкинга и связанных с ними внутрибанковских автоматизированных систем, а также средства резервного копирования информации об ордерах клиентов и о проведенных банковских операциях;

состав средств защиты банковской и клиентской информации.

5.2.3. Отношения с провайдерами, в том числе:

перечень провайдеров и разработчиков программного обеспечения для кредитной организации;

условия договоров, заключенных с провайдерами, разработчиками программного обеспечения для кредитной организации;

состав и описание услуг, функций, операций, процедур, переданных на исполнение провайдерам;

данные о провайдерах, позволяющие оценивать их возможности по выполнению обязательств перед кредитной организацией;

компьютерные системы и системы связи, используемые провайдерами, а также их характеристики.

5.2.4. Условия применения интернет-банкинга:

описание процедур и фактическое распределение обязанностей, ответственности, прав операторов

внутрибанковских автоматизированных систем в части интернет-банкинга;

описание процедур системного администрирования, результатов их осуществления, а также данные внутрисистемных компьютерных журналов;

состав и характеристики средств криптографической защиты информации интернет-банкинга, а также связанных с их применением лицензий и сертификатов;

описание процедуры подготовки (распорядительный документ) и содержание планов на случай чрезвычайных обстоятельств, и результаты их тестирования;

методические материалы по внутреннему контролю (в том числе методики выявления, оценки, мониторинга, контроля и (или) минимизации банковских рисков, связанных с интернет-банкингом);

результаты проверок, проведенных службой внутреннего контроля (внутреннего аудита);

описание процедур и фактическое распределение полномочий доступа служащих кредитной организации к сетевым информационным ресурсам интернет-банкинга;

описание процедур администрирования информационной безопасности и результаты его осуществления;

описание процедур противодействия возможному противоправному использованию интернет-банкинга и результаты его осуществления.

5.2.5. Документирование информации об авариях, отказах, сбоях функционирования аппаратно-программного обеспечения систем интернет-банкинга, в том числе компьютерных систем и средств связи провайдеров кредитной организации, и их причинах, о попытках неправомерного доступа (внешнего и внутреннего) к внутрибанковским автоматизированным системам, информационным и процессинговым ресурсам, о сетевых и вирусных атаках, их последствиях и принятых мерах, а также в целом об источниках (факторах), влияющих на повышение банковских рисков.