

Практическое пособие

# ЭЛЕКТРОННЫЙ БАНКИНГ

сопутствующие риски и особенности  
безопасного функционирования



## **ОЗНАКОМИТЕЛЬНАЯ ВЕРСИЯ ПОСОБИЯ**

Содержит целостные фрагменты из полного издания  
и позволяет оценить практическую ценность  
информации, стилистику изложения,  
а также удобство ее пользования

# **ЭЛЕКТРОННЫЙ БАНКИНГ**

## **СОПУТСТВУЮЩИЕ РИСКИ И ОСОБЕННОСТИ БЕЗОПАСНОГО ФУНКЦИОНИРОВАНИЯ**

**Практическое пособие**

Москва  
Издательский дом «Регламент»  
2009

## Содержание

Введение .....	6
<b>Глава 1</b> <b>ВОЗНИКНОВЕНИЕ И РАЗВИТИЕ</b> <b>ЭЛЕКТРОННОГО БАНКИНГА</b> .....	7
Возникновение Интернета .....	8
Возникновение интернет-банкинга .....	11
Возникновение электронного банкинга в мире .....	14
Возникновение электронного банкинга в России .....	15
Перспективы электронного банкинга в России .....	16
<b>Глава 2</b> <b>ПРИНЦИПЫ УПРАВЛЕНИЯ РИСКАМИ</b> <b>ЭЛЕКТРОННОГО БАНКИНГА</b> .....	19
Проблемы, связанные с управлением рисками электронного банкинга .....	21
Основные принципы управления рисками электронного банкинга .....	22
Наблюдение со стороны Совета директоров и высшего руководства банка (Принципы 1–3) .....	24
Средства обеспечения безопасности (Принципы 4–10) .....	34
Управление правовым и репутационным рисками (Принципы 11–14) .....	42
<b>Глава 3</b> <b>ВОЗМОЖНЫЕ РИСКИ ПРИ ИСПОЛЬЗОВАНИИ ТЕХНОЛОГИИ</b> <b>ИНТЕРНЕТ-БАНКИНГА</b> .....	49
Услуги и обслуживание в рамках интернет-банкинга .....	50
Развитие интернет-банкинга .....	51
Типы интернет-банкинга .....	53
Риски интернет-банкинга .....	54
Кредитный риск .....	54
Процентный риск .....	55
Риск ликвидности .....	56
Ценовой риск .....	56
Валютный риск .....	56
Операционный риск .....	56
Риск несоответствия .....	58
Стратегический риск .....	58
Репутационный риск .....	59
Управление рисками .....	60
Внутренний контроль .....	61

## СОДЕРЖАНИЕ

<b>Глава 4</b>	
<b>ВНУТРЕННИЙ КОНТРОЛЬ ПРИ ИСПОЛЬЗОВАНИИ СИСТЕМ ЭЛЕКТРОННОГО БАНКИНГА</b> .....	63
Качество корпоративного управления в части развития и применения систем электронного банкинга .....	64
Ориентированность кредитной организации на развитие технологий электронного банкинга .....	64
Роль Совета директоров кредитной организации в организации внутреннего контроля .....	66
Общие процедуры организации внутреннего контроля .....	68
<i>Документарное обеспечение системы внутреннего контроля</i> .....	68
<i>Особенности подбора кадров в Службу внутреннего контроля</i> .....	69
<i>Методологическое обеспечение Службы внутреннего контроля</i> .....	70
<i>Организация работы Службы внутреннего контроля с результатами проверок применения технологий электронного банкинга</i> .....	72
Организация управления рисками, связанными с использованием систем электронного банкинга .....	74
Организация (адаптация) процедур внутреннего контроля в части систем электронного банкинга .....	79
Организация процедур внутреннего контроля на этапе обоснования нового проекта системы электронного банкинга .....	81
Организация процедур внутреннего контроля на этапе принятия решения о новом проекте системы электронного банкинга .....	84
Организация (адаптация) процедур внутреннего контроля на этапе планирования реализации системы электронного банкинга .....	87
Организация (адаптация) процедур внутреннего контроля на этапе проектирования системы электронного банкинга .....	89
Организация (адаптация) процедур внутреннего контроля на этапе разработки системы электронного банкинга .....	94
Организация (адаптации) процедур внутреннего контроля на этапе испытаний, сдачи и приемки в эксплуатацию системы электронного банкинга .....	106
Организация (адаптация) процедур внутреннего контроля на этапе эксплуатации системы электронного банкинга .....	117
<b>Глава 5</b>	
<b>ПРЕДУПРЕЖДЕНИЕ ПРОТИВОПРАВНОГО ИСПОЛЬЗОВАНИЯ СИСТЕМ ЭЛЕКТРОННОГО БАНКИНГА</b> .....	123
<b>Глава 6</b>	
<b>ИНФОРМАЦИОННАЯ БЕЗОПАСНОСТЬ ЭЛЕКТРОННОГО БАНКИНГА С УЧЕТОМ ТРЕБОВАНИЙ СТАНДАРТОВ БАНКА РОССИИ</b> .....	147

**ЭЛЕКТРОННЫЙ БАНКИНГ**  
**СОПУТСТВУЮЩИЕ РИСКИ И ОСОБЕННОСТИ БЕЗОПАСНОГО ФУНКЦИОНИРОВАНИЯ**

<b>ПРИЛОЖЕНИЯ</b> .....	169
Приложение I. Перечень вопросов для проверки обеспечения в кредитной организации контроля над противоправным использованием технологии электронного банкинга .....	170
Приложение II. Политика информационной безопасности Банка .....	182
Приложение III. Политика антивирусной защиты .....	197
Приложение IV. Политика использования электронной почты .....	200
Приложение V. Порядок организации парольной защиты .....	207
Приложение VI. Регламент реагирования на нарушения информационной безопасности .....	212
Приложение VII. Памятка пользователя по информационной безопасности ..	238
<b>Перечень нормативных документов</b> .....	241

## Введение

Очевидной тенденцией нескольких последних лет становится развитие принципиально новых технологий банковского обслуживания клиентов. Наиболее динамично развивающимися являются технологии электронного банкинга, основными из которых можно назвать:

- интернет-банкинг — управление банковскими счетами и картами через Интернет и web-браузер в режиме онлайн;
- мобильный банкинг — управление банковскими счетами и картами с КПК, коммуникаторов и смартфонов.

Использование электронного банкинга дает ряд преимуществ:

- существенно экономится время за счет исключения необходимости посещать банк лично;
- клиент имеет возможность 24 часа в сутки контролировать собственные счета и оперативно реагировать на изменения ситуации на финансовых рынках;
- клиент может отслеживать операции с пластиковыми картами, поскольку доступ к работе с системой не зависит от его местонахождения — достаточно иметь доступ в Интернет.

По мнению экспертов, к концу 2009 года около 25 процентов абонентов мобильной связи в мире будут пользоваться беспроводными банковскими услугами.

Закономерно, что с развитием электронного банкинга становятся актуальными вопросы, связанные с безопасностью использования таких технологий и с появлением новых (ранее нетипичных) источников банковских рисков. При этом перечень рисков остается прежним, повышается лишь роль технической составляющей их профиля.

Авторы надеются, что данное практическое пособие окажет помощь не только в понимании основных проблем, связанных с использованием систем электронного банкинга, но и станет отправным материалом для разработки внутренних документов (положений, инструкций и пр.), в том числе методик для проверки различными службами кредитной организации безопасного функционирования данных систем дистанционного банковского обслуживания.

## Организация (адаптация) процедур внутреннего контроля на этапе проектирования системы электронного банкинга

Данный этап предусматривает работы, связанные непосредственно с проектированием системы электронного банкинга, заключающиеся в большей части в разработке проектной документации, содержащей основные взаимосвязанные проектные решения по системе в целом, ее функциям и всем видам обеспечения системы электронного банкинга, достаточные для разработки, наладки и функционирования системы электронного банкинга, ее проверки и обеспечения работоспособности.

Учитывая, что система электронного банкинга представляет собой сложное в организационном и технологическом плане решение, значительное внимание следует уделять качеству организации ее документарного обеспечения и качеству самих документов.

Одним из аспектов является систематизация документарной базы, что необходимо в связи с потребностью внесения изменений в документы по мере развития системы во взаимосвязи между собой. В противном случае

внесение изменений в отдельные документы может привести к возникновению противоречий с положениями, отраженными в других документах.

В целях систематизации документарного обеспечения системы электронного банкинга должен быть разработан перечень необходимой проектной и рабочей документации<sup>1</sup> на систему электронного банкинга.

Перечень проектной документации на систему электронного банкинга утверждается одним из руководителей кредитной организации, курирующим вопросы применения информационных технологий (куратором по ИТ).

К числу разрабатываемой проектной документации могут относиться:

1. **Описание постановки комплекса задач** или иной подобный документ представляет собой комплекс задач или совокупность технических заданий на разработку комплекса программных и аппаратных средств, составляющих информационный контур системы электронного банкинга.

Описание постановки комплекса задач может включать в себя следующие зоны.

*Информация об основании для разработки системы электронного банкинга* — указывается документ (документы), на основании которого планируется разработка; орган или ответственное лицо кредитной организации, утвердившие данный документ.

*Информация о функциональном назначении предполагаемой системы или модуля системы электронного банкинга.*

В основной части документа должны быть отражены *требования к системе или модулю системы электронного банкинга*. Наиболее детально должны быть описаны требования к функциональным характеристикам системы и ее модулей. Подлежат описанию все бизнес-процедуры, связанные с обслуживанием клиентов банка и соответствующими внутрибанковскими процессами по обработке информации, поступившей от клиентов банка, и информацией задействованных подразделений и функциональных узлов кредитной организации.

Также должны быть кратко описаны *условия эксплуатации системы электронного банкинга*, в том числе приведено количество клиентов, предполагаемое к подключению к работе с системой электронного банкинга на момент ввода ее в эксплуатацию, а также с учетом динамики развития кредитной организации. Должно быть оговорено количество пользователей внутри кредитной организации, периоды функционирования, периоды технического обслуживания и т.д.

Дополнительно в данном документе может быть отражена *информация в части требований к техническим характеристикам аппаратных средств*, совместимости с программным обеспечением, используемым в деятельности кредитной организации, и пр.

Описание постановки комплекса задач является основным проектным документом системы электронного банкинга, отражающим требования

<sup>1</sup> ГОСТ 34.003-90 «Информационная технология. Комплекс стандартов на автоматизированные системы. Автоматизированные системы. Термины и определения».

к информационному и функциональному контуру с точки зрения различных аспектов. Данный документ является связующим в комплексе проектной документации, на основании которого при необходимости подготавливаются частные технические задания и требования к отдельным элементам информационного контура.

В подготовке описания постановки комплекса задач должны быть задействованы специалисты подразделения — заказчика системы электронного банкинга, а также ряд представителей других подразделений, к компетенции которых относятся соответствующие вопросы.

2. Другим немаловажным документом из числа проектной документации является **«Описание системы защиты»** или иной подобный документ. По содержанию данный документ является частным техническим заданием системы электронного банкинга на реализацию процедур и средств информационной безопасности в рамках информационного контура.

Документ содержит:

- перечень критически важной информации, обрабатываемой и генерируемой в среде системы электронного банкинга;
- перечень технических средств обеспечения информационной безопасности информационного контура системы электронного банкинга;
- описание организационных процедур обеспечения информационной безопасности;
- описание технологических средств и систем защиты и обеспечения целостности информации, варианты их сопряжения и функционирования в информационном контуре системы электронного банкинга;
- механизм организации парольной защиты, администрирования и систематизации данной работы;
- механизм реализации антивирусной защиты системы электронного банкинга.

Приложением к данному документу могут выступать:

- детальное распределение прав и обязанностей внутрибанковских пользователей системы электронного банкинга;
- описание их ролей с функциональной точки зрения и прав «владения» определенными массивами информации.

3. Частным документом, связанным с описанием постановки комплекса задач является **альбом выходных форм** или иной подобный документ, содержащий описание всех диалоговых окон и выходных форм системы электронного банкинга, доступных как для клиентов кредитной организации в процессе их работы с программным комплексом, так и для внутренних пользователей, задействованных функционально в информационном контуре системы электронного банкинга. Документ содержит как точное визуальное графическое отображение выходных форм, так и правила их заполнения, информационные источники заполнения форм.

Также в части каждой выходной формы приводятся перечень программных модулей, в которых она используется, и перечень функций и процедур, вызывающих данную форму.

Приводятся назначение каждого элемента выходной формы, действия по управлению ими и результаты данного управления.

**4. Описание технологии взаимодействия с банковской автоматизированной системой** или иной подобный документ.

Данный документ разрабатывается, как правило, ввиду сложной архитектуры внутрибанковских автоматизированных систем и необходимости описания правил и технологических решений по их взаимодействию между собой.

Интегрирование системы электронного банкинга в работу внутрибанковских автоматизированных систем вызывает необходимость описания решений следующих основных моментов:

- перечень информационных ресурсов и данных, подлежащих передаче в другие внутрибанковские автоматизированные системы;
- перечень информационных ресурсов других внутрибанковских автоматизированных систем, подлежащих использованию в системе электронного банкинга;
- перечень аппаратных ресурсов информационного контура системы электронного банкинга, используемых в целях взаимодействия с другими внутрибанковскими автоматизированными системами;
- выбор (разработка) формата файлов для обмена данными системы электронного банкинга с другими внутрибанковскими автоматизированными системами;
- процедуры защиты информации и обеспечения целостности данных на участках обмена с другими внутрибанковскими автоматизированными системами могут быть также приведены в описании системы защиты.

**5. Описание комплекса технических средств** или иной подобный документ.

Документ представляет собой детальное описание перечня аппаратных средств, входящих в состав информационного контура системы электронного банкинга.

Помимо состава оборудования указываются также описания: необходимых настроек аппаратных средств; условий эксплуатации каждого средства; вариантов проверки работоспособности средства.

Документ может также содержать информацию об оборудовании других марок или модификаций, которое может быть использовано для замены используемого аппаратного обеспечения.

**6. Обобщающим проектным документом является Схема функциональной структуры информационного контура системы электронного банкинга.** Подобные схемы зачастую документируются при разработке автоматизированных комплексов и систем.

Документ представляет собой графическое отображение и соответствующее описание совокупности аппаратных и программных средств и каналов связи, посредством которых программные и аппаратные средства взаимодействуют между собой.

Такой документ должен содержать следующую информацию:

1) о технологическом решении вычислительной сети, на которой основывается система электронного банкинга<sup>1</sup>;

2) об аппаратных и программных средствах на стороне самой кредитной организации, на стороне ее клиента и на стороне провайдера кредитной организации. При этом следует представить описание в разрезе всех провайдеров услуг для кредитной организации и контрагентов, выполняющих заказную обработку данных (процессинг, клиринг и пр.);

3) данные о маршрутах прохождения информации при взаимодействии клиента и кредитной организации, об этапах ее преобразования, обработки и контроля.

Кроме указанной информации, позитивным является наличие общего описания внешнего информационного контура кредитной организации, в котором выделены участки взаимодействия непосредственно с информационным контуром системы электронного банкинга.

Схема информационного контура приводится с кратким функциональным описанием ее элементов.

Качество документа должно позволить:

- выделить основные технологические и функциональные участки передачи, приема, контроля, обработки и хранения информации;
- установить их физическое размещение;
- оценить концентрацию источников рисков на различных участках информационного контура.

Сведения, отображаемые в схеме функциональной структуры информационного контура системы электронного банкинга, требуются для ее тестирования и качественной организации обслуживания.

Помимо отмеченных документов в кредитной организации могут быть разработаны и другие проектные документы в соответствии с утвержденным перечнем проектной документации на систему электронного банкинга.

Все проектные документы должны разрабатываться в соответствии с принятой в кредитной организации практикой ведения документооборота ответственными по соответствующим направлениям деятельности с учетом их координации между собой и утверждаться куратором по информационным технологиям.

Все перечисленные выше аспекты являются основой для оценки качества организации процесса внутреннего контроля на этапе проектирования системы электронного банкинга. При этом основными вопросами являются следующие:

- *разработан ли перечень необходимой проектной документации?*
- *разработаны ли следующие (или подобные) документы: описание постановки комплекса задач и систем защиты; альбом выходных форм; описание технологии взаимодействия с банковской автоматизированной системой и комплекса технических средств; схема*

<sup>1</sup> При этом в случае наличия альтернативных вариантов взаимодействия элементов информационного контура такие варианты должны быть отражены и описаны.

## ФРАГМЕНТ ПРАКТИЧЕСКОГО ПОСОБИЯ

*функциональной структуры информационного контура системы электронного банкинга?*

- *разработаны ли иные документы, предусмотренные перечнем проектной документации?*

### Организация (адаптация) процедур внутреннего контроля на этапе разработки системы электронного банкинга

На данном этапе производится непосредственно разработка системы электронного банкинга. Подразумеваются следующие этапы.

1. Разработка либо приобретение программного обеспечения в соответствии с перечнем программного обеспечения, утвержденным на этапе проектирования и в соответствии с другими проектными документами, такими как описание постановки комплекса задач, альбом выходных форм, описание системы защиты, описание технологии взаимодействия с банковской автоматизированной системой. Разрабатываются или приобретаются: клиентская часть для случая «толстого клиента», автоматизированные рабочие места операторов в кредитной организации, администраторов системы, администраторов информационной безопасности системы, программное обеспечение серверной части системы, необходимое для сопряжения с другими внутрибанковскими автоматизированными системами, и пр.

2. Разработка (монтаж) сегментов электронной вычислительной сети, являющихся частью информационного контура системы электронного банкинга, в соответствии с разработанной на этапе проектирования проектной документацией (в том числе функциональной схемы информационного контура) — прокладка необходимых участков кабеля, установка и настройка сетевого оборудования, сетевого программного обеспечения и пр.

3. Разработка необходимой эксплуатационной документации.

4. Разработка необходимой внутренней документации, регламентирующей обеспечение информационной безопасности и непрерывности функционирования системы электронного банкинга.

5. Заключение договоров (контрактов) с контрагентами-поставщиками программного обеспечения и оборудования для информационного контура системы электронного банкинга.

6. Заключение договоров (контрактов) с провайдерами на предоставление услуг связи.

7. Разработка типовых договоров с клиентами на обслуживание посредством системы электронного банкинга.

Важным на данном этапе является **обеспечение должного качества договоров** с контрагентами. Данному вопросу, помимо юридической службы, должны также уделять внимание и специалисты Службы внутреннего контроля кредитной организации.

К числу аспектов, которым следует уделять внимание, относится наличие в **договоре (контракте) с поставщиком программного, а также аппаратного обеспечения** системы электронного банкинга, положения о сопровождении поставляемого программного обеспечения или иных техни-

ческих средств на весь срок их службы либо приобретения полного комплекта технической документации, обеспечивающего возможность сопровождения программного обеспечения или иных технических средств и их компонентов без участия разработчика.

**В части договорных отношений с организациями-провайдерами** услуг связи важным является наличие в договоре положения, предусматривающего ответственность провайдера за качественное и бесперебойное предоставление услуг, ответственность в случае возникновения сбоев не по вине кредитной организации и ответственность провайдера за сохранность и целостность информации, в случае если часть ресурсов информационного контура обслуживается специалистами организации-провайдера или арендуется кредитной организацией у организации-провайдера, и т.д.

Помимо включения в договоры с провайдерами положений об обеспечении информационной безопасности и конфиденциальности клиентской и банковской информации, в кредитной организации могут быть разработаны соответствующие внутренние документы, такие как:

- порядок (порядки) соблюдения конфиденциальности клиентской информации;
- порядок (порядки) соблюдения конфиденциальности банковской информации;
- должностные инструкции сотрудников, ответственных за соблюдение информационной безопасности и конфиденциальности информации клиентов и банковской информации об операциях и сделках;
- различные документы, регламентирующие порядок взаимодействия кредитной организации и провайдеров по вопросам обеспечения информационной безопасности и обеспечения конфиденциальности информации.

**В части документов, регламентирующих порядок взаимодействия кредитной организации и провайдеров** по вопросам обеспечения информационной безопасности и обеспечения конфиденциальности информации, следует отметить, что их содержание должно быть направлено на обеспечение приемлемого уровня «прозрачности» организации-провайдера кредитной организации с учетом специфики организационной структуры организации-провайдера.

Такая «прозрачность» в отношении вопросов информационной безопасности может быть обеспечена возможностью осуществления проверок или мониторинга организации-провайдера со стороны Службы внутреннего контроля кредитной организации по обозначенным вопросам.

Другим вариантом может быть периодический мониторинг качества организации работы по обеспечению информационной безопасности и конфиденциальности информации специализированными аудиторскими компаниями. В этом случае в документах, о которых идет речь, может быть отражено положение о возможности доступа специалистов Службы внутреннего контроля или Службы информационной безопасности к актам или другим документам, подготовленным аудиторами.

## ФРАГМЕНТ ПРАКТИЧЕСКОГО ПОСОБИЯ

Позитивным является наличие у организации-провайдера собственной Службы внутреннего контроля и Службы информационной безопасности либо отдельных квалифицированных в данной области специалистов. Наличие таких специалистов, очевидно, стало бы фактором, повышающим эффективность взаимодействия кредитной организации и организации-провайдера по обозначенным вопросам.

В случае, когда организация-провайдер (в силу своего финансового состояния или объемов бизнеса) не обладает такими Службами внутреннего контроля и информационной безопасности, становится очевидной необходимость наличия документов, регламентирующих взаимодействие кредитной организации и провайдеров по данным вопросам. Отсутствие таких документов и служб у провайдера является фактором, значительно повышающим риски.

Следует отметить, что основная ответственность перед клиентами за обеспечение информационной безопасности и конфиденциальности клиентской информации приходится на кредитную организацию. Качественная организация взаимодействия с организациями-провайдерами является лишь одним из факторов (значительным) обеспечения «прозрачности» и уменьшения риска нарушения целостности, потери или утечки данных о клиенте и его операциях посредством системы электронного банкинга.

Кредитная организация определяет методы обеспечения информационной безопасности и конфиденциальности информации, к их числу могут относиться:

- 1) общий мониторинг источников рисков, связанных с деятельностью организации-провайдера;
- 2) оценка и мониторинг финансового состояния провайдера, в том числе:
  - оценка частоты сменяемости топ-менеджмента кредитной организации-провайдера;
  - текучесть кадров;
  - стабильность развития бизнеса, частота изменения основных направлений бизнеса;
  - профессиональные навыки и опыт работы ключевых сотрудников организации-провайдера в области информационных технологий, непосредственно связанных с особенностями реализации системы электронного банкинга;
- 3) разработка и использование специализированных процедур оценки технологических особенностей провайдера, возможностей его оборудования и т.д.;
- 4) совместная или согласованная между кредитной организацией и провайдером политика обеспечения информационной безопасности и конфиденциальности информации;
- 5) процедуры, обеспечивающие информирование клиентов кредитной организации о состоянии информационной безопасности и конфиденциальности их данных, о способах противодействия и предупреждения источников угроз информационной безопасности и конфиденциальности информации и т.д.

Другим немаловажным фактором, который необходимо учитывать уже на этапе разработки системы электронного банкинга, является **обеспечение непрерывности ее функционирования**, способности быстро восстанавливать свою работоспособность в случае наступления непредвиденных сбоев и других проявлений источников рисков.

Положения в части обеспечения непрерывности функционирования системы электронного банкинга рекомендуется отражать как в договорах с организациями-провайдерами и поставщиками, так и во внутренних документах кредитной организации. Положения должны быть сформатированы таким образом, чтобы между кредитной организацией, ее провайдерами и поставщиками оборудования и программного обеспечения, используемого в составе информационного контура системы, была четко разграничена ответственность за обеспечение непрерывности функционирования системы. Например, следует отразить следующие моменты:

- конкретные временные ограничения по устранению сбоев и неисправностей в поставленном ими по договору оборудовании или программном обеспечении;
- ответственность провайдера о предоставлении, помимо основного, также резервного канала связи, который может быть задействован в короткие сроки и обеспечивать должное качество связи.

В кредитной организации должны быть разработаны соответствующие внутренние документы, регламентирующие:

- функции структурных подразделений в части обеспечения непрерывности функционирования системы электронного банкинга и процедуры реализации данных функций;
- порядок информирования органов управления и других структурных подразделений, а также клиентов о возникновении нештатных ситуаций, способных привести к нарушению непрерывности функционирования системы электронного банкинга и мероприятий, направленных или необходимых для устранения причин;
- планы обеспечения непрерывности и восстановления работоспособности системы электронного банкинга;
- методики стресс-тестирования кредитной организации в части непрерывности функционирования системы электронного банкинга.

При разработке указанных документов кредитной организации следует учитывать все наиболее вероятные сценарии, способные привести к нарушению непрерывности функционирования системы электронного банкинга. К их числу могут относиться:

- сетевые (хакерские атаки) на ресурсы кредитной организации или провайдера;
- механическое нарушение основного и дублирующего канала связи с провайдером;
- выход из строя сервера баз данных системы электронного банкинга;
- выход из строя сервера приложений системы электронного банкинга;
- временное отключение электроэнергии в сети;

## ФРАГМЕНТ ПРАКТИЧЕСКОГО ПОСОБИЯ

- отключение резервного источника электропитания системы электронного банкинга;
- воздействие на систему электронного банкинга или на ее отдельные модули компьютерных вирусов.

Ключевым документом в целях обеспечения непрерывности функционирования системы электронного банкинга является разработанный в кредитной организации соответствующий план обеспечения непрерывности и восстановления работоспособности системы, который должен основываться на перечне наиболее критичных для работоспособности системы электронного банкинга воздействий.

В целях обеспечения эффективности плана данные воздействия могут быть классифицированы по степени возможного материального ущерба кредитной организации и ее клиентам, а также по вероятности их возникновения.

В отношении каждого из видов возможного воздействия на систему электронного банкинга планом должны быть предусмотрены соответствующие действия кредитной организации, ее клиентов и организаций-провайдеров. Наиболее подробно должны быть описаны внутренние восстановительные процедуры самой кредитной организации с описанием действий ее внутренних подразделений, а также с указанием временных параметров осуществления данных процедур.

Помимо процедур восстановления работоспособности системы электронного банкинга, план должен предусматривать также процедуры по организации проведения операций клиентов альтернативными способами (без использования системы электронного банкинга) в наиболее короткие сроки.

Процедуры, регламентированные планом, должны учитывать распределение ответственности, зафиксированное в договорах с организациями-поставщиками программного обеспечения и оборудования.

Качественная разработка плана должна учитывать возможные действия в целях реагирования на сбои не только кредитной организации, но и организаций-провайдеров, а также возможности оперативного привлечения к устранению неисправностей других организаций, оказывающих сервисные услуги в области информационных технологий.

Помимо плана обеспечения непрерывности функционирования системы электронного банкинга в кредитной организации должны быть регламентированы:

- способы мониторинга системы электронного банкинга, ее внешней и внутренней среды с целью выявления и предупреждения воздействий, способных нарушить непрерывность функционирования;
- методики оценки ущерба (материального и нематериального) в случае проявления негативных воздействий или кризисных ситуаций;
- процедуры и рекомендации по уведомлению ее клиентов в случае нарушения непрерывности функционирования системы электронного банкинга.

Целесообразным является функционирование в кредитной организации Службы поддержки клиентов в части функционирования системы электронного банкинга.

Также в целях координации деятельности структурных подразделений кредитной организации в условиях возникновения сбоя и приостановки работы системы электронного банкинга (в соответствии с закрепленными за ними функциями по устранению нарушений в работе системы электронного банкинга и организации альтернативных способов проведения операций) в кредитной организации распоряжением ее руководства может быть сформирована **антикризисная группа или комиссия** из числа руководителей соответствующих подразделений, в том числе из руководителей служб информационных технологий, информационной безопасности, операционной работы, хозяйственного обеспечения, по связям с общественностью, юридической службы и др. (при необходимости).

Основной задачей членов комиссии является правильная классификация нештатных ситуаций<sup>1</sup> и выбор соответствующих процедур реагирования в соответствии с планом обеспечения непрерывности функционирования системы электронного банкинга.

Так, например, право квалифицировать отрицательное воздействие внешнего фактора на деятельность банка статусом «кризисная ситуация» и предлагать соответствующие процедуры предоставляется следующим членам антикризисного комитета:

- по вопросам электроснабжения — руководителю Службы хозяйственного обеспечения;
- по вопросам качества систем связи — начальнику Управления информатики;
- по вопросам репутационного риска — руководителю Службы по связям с общественностью;
- по вопросам возникших правовых коллизий, связанных с обслуживанием клиентов посредством системы электронного банкинга, — руководителю юридической службы и пр.

Окончательное решение о работе кредитной организации по антикризисному плану (поддержка функционирования банка во внештатной ситуации в соответствии с ее характером, координация деятельности структурных подразделений, руководителей и отдельных сотрудников) возлагается на председателя антикризисной комиссии. Условием для принятия такого решения является наступление события, квалифицируемого как кризисная ситуация.

Председателем антикризисного комитета может быть либо руководитель кредитной организации, либо куратор по ИТ, если ему делегированы данные полномочия.

Для повышения эффективности разработки плана обеспечения непрерывности функционирования мероприятия, направленные на обеспечение непрерывности функционирования системы, целесообразно разрабатывать на основе результатов стресс-тестирования — процедур, позволяющих оценить качественное и количественное влияние на основные показатели функционирования кредитной организации потенциального воздействия наиболее вероятных источников рисков.

<sup>1</sup> Речь идет о нештатных ситуациях, при которых может быть нарушена непрерывность функционирования системы электронного банкинга.

Процедуры стресс-тестирования могут учитывать функционирование как отдельных участков информационного контура системы электронного банкинга (например, внешние участки — аппаратные и программные средства клиентов кредитной организации или ее провайдеров; внутренние участки — автоматизированное рабочее место операциониста, контролера, администратора системы и т.д.), так и информационного контура в целом.

При этом в процедурах стресс-тестирования могут использоваться простейшие сценарии, когда анализируется воздействие одного или небольшого количества факторов (источников) рисков. Следует отметить, что использование простейших сценариев целесообразно в отношении отдельных сегментов или элементов информационного контура системы электронного банкинга, части ее функциональных возможностей.

Предпочтительным является использование комплексных сценариев, что значительно расширяет анализ потенциального воздействия источников рисков и позволяет получить более объективные результаты.

Достоверная оценка потенциального комплексного воздействия основных источников рисков на функционирование системы электронного банкинга значительно повышает качество разрабатываемых процедур реагирования на такие воздействия в целях обеспечения непрерывности или восстановления функционирования системы.

**В части разработки типовых договоров с клиентами на обслуживание посредством системы электронного банкинга** следует отметить, что с точки зрения минимизации правового и репутационного рисков кредитной организации целесообразным является унификация договоров о подключении к системе электронного банкинга с клиентами. При этом унификация должна учитывать, что различным клиентам кредитной организации при работе с системой электронного банкинга могут быть предоставлены различные права и возможности, что делает необходимым разработку соответствующих типовых договоров.

Помимо типовых форм договора могут быть также разработаны типовые формы заявлений на предоставление услуг по системе электронного банкинга, изменение вариантов обслуживания.

В общем случае договор о подключении и обслуживании в системе электронного банкинга между кредитной организацией и ее клиентом может содержать следующие положения: предмет договора, права и обязанности сторон, ответственность сторон, стоимость услуг, срок действия договора, прочие условия.

В разделе, раскрывающем **предмет договора**, могут оговариваться:

- перечень и объем предоставляемых услуг;
- возможность и порядок изменения вариантов обслуживания;
- порядок проведения расчетных операций в электронной форме по открытому клиентом счету в банке;
- способ передачи от банка к клиенту необходимых программных или аппаратных средств, в том числе используемых для генерирования ключей электронной цифровой подписи, и состав данных средств;

— способы обмена между банком и клиентом электронными документами. В разделе, раскрывающем **права и обязанности** сторон, могут быть отмечены:

- обязанность банка по обеспечению электронного документооборота в системе электронного банкинга по указанным клиентом адресам;
- перечень случаев, в которых банк имеет право по неисполнению электронных документов клиента;
- порядок уведомления клиента об изменениях размера и условий оплаты за услуги использования системы электронного банкинга;
- обязанность клиента своевременно и надлежащим образом формировать и передавать электронные документы;
- обязанность клиента своевременно и надлежащим образом генерировать секретный ключ и хранить его в секрете, при его компрометации незамедлительно письменно извещать банк для прекращения работы;
- порядок уведомления банка клиентом о намерении изменения варианта обслуживания в системе электронного банкинга.

В разделе, раскрывающем **ответственность сторон**, в рамках действующего законодательства детально раскрывается ответственность клиента и банка, в том числе могут оговариваться положения:

1. В случае нарушения договора и других документов, определяющих правила взаимодействия банка и клиента посредством системы, ответственность за последствия несет сторона, которая допустила эти нарушения. При этом каждая сторона не несет ответственности за убытки, понесенные другой стороной не по вине первой в результате использования системы электронного банкинга, в том числе при исполнении ошибочных платежных электронных документов, если эти документы надлежащим образом клиентом оформлены и переданы, а кредитной организацией получены, проверены и признаны верными.

2. Клиент несет ответственность за правильность формирования документов, их достоверность и срочность передачи их банку.

3. Устанавливаются пределы ответственности кредитной организации за невыполнение своих обязательств по договору с клиентом, причиной которого стали ситуации, влияние кредитной организации на которые ограничено (отключение напряжения в электросети, повреждение линий связи с провайдером и им подобные), при этом должен быть приведен перечень таких ситуаций.

4. Разграничена ответственность в случае, если информация, передаваемая сторонами друг другу через электронную почту Интернет, стала доступна третьим лицам либо если ущерб возник из-за составляющей системы электронного банкинга, находящейся вне непосредственного контроля кредитной организации.

**В отношении проектной документации**, в соответствии с которой разрабатывается и монтируется система электронного банкинга, следует иметь в виду, что на этапе разработки системы электронного банкинга по различным причинам **могут вноситься изменения в изначальный проект систе-**

**мы**, связанные с усовершенствованием ее отдельных функций или технологических решений. Данные изменения должны сопровождаться корректировкой проектной документации, подготовленной на предыдущем этапе.

Все изменения, вносимые в проектную документацию, должны предварительно анализироваться комитетом по технологиям кредитной организации в рамках текущей работы по проекту системы электронного банкинга на предмет:

- выявления и парирования факторов рисков;
- совместимости, согласованности с технологическими решениями на других участках системы электронного банкинга;
- информационной безопасности;
- экономической целесообразности.

Все вносимые в проектную документацию изменения утверждаются решением комитета по технологиям или куратором по ИТ.

На этапе разработки системы электронного банкинга, как и на этапе проектирования, значительное внимание следует уделять качеству организации ее документарного обеспечения **в части эксплуатационной документации**.

На этапе планирования системы электронного банкинга должны быть определены специалисты или подразделения, ответственные за подготовку данной документации.

В целях систематизации эксплуатационной документации на этапе планирования составляется и утверждается перечень документации решением комитета по технологиям либо куратором по ИТ.

**К числу разрабатываемой эксплуатационной документации системы электронного банкинга могут относиться:**

- спецификация аппаратных средств и программных средств и модулей;
- инструкция по эксплуатации комплекса технических средств;
- руководства по установке и настройке компонентов системы и по сопровождению программного обеспечения системы;
- руководство пользователей компонентов системы.

Первые два документа являются аналогом «Описанию комплекса технических средств» или иному подобному документу, разрабатываемому на этапе проектирования. Данные документы также представляют собой детальное описание перечня программных и аппаратных средств, фактически используемых в составе информационного контура системы электронного банкинга, с учетом всех доработок в проектной документации и информационном контуре, внесенных на этапе разработки.

**Инструкция по эксплуатации комплекса технических средств** представляет собой документ, отражающий в соответствии со спецификацией программных средств и модулей и спецификацией аппаратных средств системы электронного банкинга описание основных особенностей, допустимого режима работы программных и аппаратных средств в составе информационного контура системы электронного банкинга, требования к необходимым для данного программного обеспечения техническим средствам, общие характеристики входной и выходной информации, а также требования и условия организационного, технического и технологического характера и т.п.

**Руководство(а) по установке и настройке** представляет собой один или несколько документов, содержащих описание:

- процесса установки серверного программного обеспечения (формирования баз данных, программного обеспечения, обслуживающего работу баз данных информации о клиентах и их операциях, и т.д.);
- процесса установки и настройки программного обеспечения в части автоматизированного рабочего места (АРМ) специалистов кредитной организации, в том числе операционных работников; АРМ контролера операций; АРМ администратора системы электронного банкинга; АРМ администратора информационной безопасности системы электронного банкинга; программных модулей и комплексов, обеспечивающих взаимодействие информационного контура системы электронного банкинга с другими банковскими автоматизированными системами; другого специализированного программного обеспечения;
- настройки аппаратного обеспечения информационного контура.

Все особенности настройки программного и аппаратного обеспечения системы электронного банкинга, описываемые в данном документе, должны соответствовать положениям, отраженным в инструкции по эксплуатации комплекса технических средств.

**Руководство по сопровождению программного обеспечения системы электронного банкинга** — документ, представляющий собой перечень и описание инструкций в части сопровождения программного и аппаратного обеспечения системы электронного банкинга. Данный документ, как правило, содержит:

- общие сведения о программном обеспечении или модуле — могут быть указаны назначение и функции программного обеспечения и сведения о рекомендуемых технических и программных средствах, обеспечивающих выполнение данного программного обеспечения, минимальный состав технических средств, обеспечивающий работу программного обеспечения;
- структуру программного обеспечения — могут быть приведены сведения о структуре программного обеспечения, его составных частях, о связях между составными частями и связях с другим программным обеспечением;
- правила действий ответственных специалистов кредитной организации при установке модулей обновления программного обеспечения;
- описание дополнительных разделов функциональных возможностей программного обеспечения и способов их выбора;
- тексты сообщений, выдаваемых в ходе выполнения настройки, проверки программного обеспечения, а также в ходе его выполнения, описание их содержания и действий, которые необходимо предпринять по этим сообщениям;
- описание способов детальной проверки, позволяющих дать общее заключение о работоспособности программного обеспечения (контрольные примеры, методы прогона, результаты);

## ФРАГМЕНТ ПРАКТИЧЕСКОГО ПОСОБИЯ

- правила действий ответственных специалистов кредитной организации по устранению наиболее типичных случаев сбоев программного и аппаратного обеспечения системы электронного банкинга;
- правила действий ответственных специалистов кредитной организации по другим операциям, связанным с обслуживанием программного и аппаратного обеспечения информационного контура системы электронного банкинга.

**Руководство пользователей программных компонентов системы электронного банкинга** представляет собой документ, предназначенный непосредственно для пользователей системы электронного банкинга как вне кредитной организации (клиенты кредитной организации — физические и юридические лица), так и внутри нее (сотрудники, в функциональные обязанности которых входит совершение определенных операций и бизнес-процедур с использованием компонентов системы электронного банкинга).

Такой документ на соответствующее программное обеспечение в составе информационного контура системы электронного банкинга может содержать следующую информацию, сгруппированную по разделам<sup>1</sup>.

*В разделе «Введение»:*

- область применения программного обеспечения;
- краткое описание возможностей программного обеспечения;
- требуемый уровень подготовки пользователя программного обеспечения;
- перечень эксплуатационной документации, с которой необходимо ознакомиться пользователю программного обеспечения.

*В разделе «Назначение и условия применения»:*

- виды операций, функции, для автоматизации которых предназначено данное программное обеспечение;
- условия, при соблюдении (выполнении, наступлении) которых обеспечивается применение средств автоматизации в соответствии с назначением (например, вид ЭВМ и конфигурация технических средств, операционная система и общесистемные программные средства, входная информация, носители данных, база данных).

*В разделе «Подготовка к работе»:*

- состав и содержание дистрибутивного носителя данных;
- порядок загрузки данных в программное обеспечение;
- порядок проверки работоспособности программного обеспечения пользователем.

*В разделе «Описание операций»:*

- детальное описание всех выполняемых функций, задач, комплексов задач и процедур;
- описание операций технологического процесса обработки данных, необходимых для выполнения функций и процедур.

<sup>1</sup> Представлены условные названия разделов документа и их содержание.

При этом для каждой операции обработки данных может указываться:

- наименование;
- условия, при соблюдении которых возможно выполнение операции;
- подготовительные действия;
- основные действия в требуемой последовательности;
- заключительные действия;
- ссылки на файлы подсказок, размещенные на магнитных носителях.

*В разделе «Аварийные ситуации»* могут указываться действия:

- в случае несоблюдения условий выполнения технологического процесса, в том числе при длительных отказах технических средств;
- по восстановлению программного обеспечения или данных при отказе магнитных носителей или обнаружении ошибок в данных;
- в случаях обнаружения несанкционированного вмешательства в данные и пр.

*В разделе «Рекомендации по освоению»* могут указываться рекомендации по освоению и эксплуатации, включая описание контрольного примера, правила его запуска и выполнения.

Все отмеченные выше аспекты являются основой для оценки качества организации процедур внутреннего контроля на этапе разработки системы электронного банкинга. При этом основными вопросами являются следующие:

- *производится ли разработка системы электронного банкинга в сроки, определенные планом на проект?*
- *имеются ли в наличии отчеты о выполнении работ, определенных планом по проекту?*
- *предусмотрен ли комплексный анализ специалистами Службы внутреннего контроля положений договора (контракта) о поставке программного обеспечения системы электронного банкинга или его части, а также иных технических средств?*
- *Предусмотрен ли комплексный анализ специалистами Службы внутреннего контроля положений договора (контракта) с организацией-провайдером о предоставлении услуг связи?*
- *разработаны ли проекты типовых договоров с клиентами на обслуживание посредством системы электронного банкинга?*
- *разработана ли необходимая внутренняя документация, регламентирующая обеспечение информационной безопасности и непрерывности функционирования системы электронного банкинга?*
- *внесены ли изменения в разработочную документацию, которые (при необходимости) принимались на этапе разработки?*
- *санкционированы ли изменения в технико-разработочную документацию на этапе разработки куратором информационных технологий или комитетом по технологиям?*
- *разработан ли ответственными за документацию перечень необходимой эксплуатационной документации?*
- *разработаны ли следующие или подобные документы:*
  - инструкция по эксплуатации комплекса технических средств;

**ФРАГМЕНТ ПРАКТИЧЕСКОГО ПОСОБИЯ**

- спецификация программных средств и модулей системы электронного банкинга;
- руководства по сопровождению программного обеспечения системы электронного банкинга по установке и настройке;
- руководства пользователей?
- разработаны ли ответственными за документацию иные документы, предусмотренные перечнем эксплуатационной документации?



## Подписаться можно:

- **по телефону:** +7 (495) 921-2334. С помощью менеджера отдела подписки Издательского дома «Регламент» вы можете получить консультацию и приобрести любые издания
- **через Интернет:** воспользуйтесь Центром online-подписки на нашем сайте [www.reglament.net](http://www.reglament.net). Данный способ сэкономит ваше время и предоставит максимум информации о наших изданиях
- **по эл. почте и факсу:** отправьте заявку в свободном формате на адрес [podpiska@bdc.ru](mailto:podpiska@bdc.ru) или факс на номер +7 (495) 921-2334