БИБЛИОТЕКА ЦЕНТРА ИССЛЕДОВАНИЙ ПЛАТЕЖНЫХ СИСТЕМ И РАСЧЕТОВ

А. М. Сычев, П. В. Ревенков, А. Б. Дудка

БЕЗОПАСНОСТЬ ЭЛЕКТРОННОГО БАНКИНГА

2-е электронное издание (стереотипное)

Москва, ЦИПСиР
Саратов, Ай Пи Эр Медиа
2019

УДК 004.56
ББК 32.971.353
С95

Сычев, А. М.

С95 Безопасность электронного банкинга / А. М. Сычев, П. В. Ревенков, А. Б. Дудка. — 2-е эл. изд. (стер.) — М. : ЦИПСиР; Саратов : Ай Пи Эр Медиа, 2019. — 320 с.

ISBN 978-5-4486-0776-9

Книга «Безопасность электронного банкинга» посвящена вопросам, связанным с обеспечением безопасного функционирования систем электронного банкинга.

А.М. Сычев, П.В. Ревенков, и А.Б. Дудка описывают в ней основные принципы управления рисками электронного банкинга и риски, возникающие в кредитных организациях при внедрении ими систем интернет-банкинга, а также организация внутреннего контроля при использовании систем электронного банкинга, обеспечение информационной безопасности электронного банкинга с учетом требований стандартов Банка России по обеспечению информационной безопасности, а также приводятся уникальные для российской аудитории примеры влияния «теневого Интернета» на безопасность электронного банкинга.

Издание предназначено для банковских специалистов, практикующих консультантов и аудиторов, преподавателей, аспирантов и студентов, обучающихся финансовым специальностям в вузах.

Для создания электронного издания использовано:
Приложение pdf2swf из ПО Swftools, ПО IPRbooks Reader,
разработанное на основе Adobe Air

УДК 004.56
ББК 32.971.353

ISBN 978-5-4486-0776-9

СОДЕРЖАНИЕ

ВСТУПИТЕЛЬНОЕ СЛОВО

Вопросы безопасности финансовых инструментов и сервисов находятся в центре внимания как пользователей финансовых услуг, так и организаций, предоставляющих такие услуги, и, конечно, государственных регуляторов. Например, уязвимости систем безопасности финансовых транзакций могут не просто привести к существенным потерям для их участников, но и подорвать доверие к данным инструментам со стороны пользователей, что в крайнем своем выражении повлечет их отказ от применения безналичных форм расчетов и переход к «проверенным» наличным. Такая ситуация невыгодна для всех экономических субъектов, поэтому столь значительные усилия и направляются на решение проблем безопасности финансовых операций.

Законодательно предусматриваются механизмы защиты прав клиентов при совершении несанкционированных финансовых операций, усиливается ответственность за соответствующие правонарушения. Государственными регуляторами уточняются нормативные требования и продвигаются лучшие практики в формате стандартов. Участниками финансового рынка совместно с вендорами разрабатываются и внедряются качественно новые системы защиты от несанкционированных операций. Эта деятельность в ряде сегментов финансового рынка уже дает определенные положительные результаты. Так, по уровню несанкционированных операций с платежными картами Российская Федерация отстает от большинства развитых стран, при этом за 2015 г. ситуация только улучшилась.

Однако, несмотря на достигнутые успехи по противодействию мошенническим действиям в отдельных сегментах финансовой сферы, противостояние продолжает оставаться весьма активным. Мошенники изобретают все новые способы совершения несанкционированных финансовых операций. Например, от атак на счета клиентов кредитных организаций мошенники перешли к атакам на корреспондентские счета самих кредитных организаций,

и в 2016 г. ряд таких атак увенчались успехом. На этом фоне одно из важнейших направлений противодействия несанкционированным операциям — повышение уровня информированности участников финансового рынка, их клиентов, рост профессиональной квалификации лиц, ответственных за разработку и проведение мероприятий по повышению безопасности финансовых операций.

Книга «Безопасность электронного банкинга» призвана внести существенный вклад в указанное направление противостояния мошенническим действиям в финансовой сфере. В книге рассмотрены вопросы риск-менеджмента современных транзакционных систем — систем электронного банкинга, представлено подробное описание порядка организации внутреннего контроля и обеспечения информационной безопасности в условиях применения систем электронного банкинга, приведен большой объем практических рекомендаций по обеспечению защиты информации. Книга сочетает подробную теоретическую информацию с широким раскрытием практических аспектов ее применения, что достигается благодаря уникальному авторскому коллективу, включающему как представителей мегарегулятора — Банка России, так и выдающихся практикующих экспертов по безопасности финансовых операций. Поэтому книга будет полезна самому широкому кругу читателей — от начинающих до профессионалов финансовой безопасности.

Роман Анатольевич Прохоров,
председатель правления
Ассоциации «Финансовые инновации» (АФИ)

ПРЕДИСЛОВИЕ

Современный банковский бизнес не может находиться в стороне от магистрального движения в сторону цифровизации самых разнообразных сфер экономической деятельности. К этому его настойчиво подталкивают и конкурентная среда, в том числе не только деятельность коллег по банковскому сектору, но и молодые, но зубастые стартапы, и необходимость оптимизации операционных затрат, и требования клиентов, которые хотят пользоваться банковскими сервисами с минимальными для себя затратами времени и усилий.

Цифровизация охватывает как внутренние процессы банка, так и прежде всего формат его взаимодействия с клиентами. И в этом отношении системы электронного банкинга играют первостепенную роль. К таким системам предъявляются высокие требования по быстродействию, отказоустойчивости, юзабилити и, конечно, защищенности. Движение банковских клиентских сервисов в цифровую сферу, в сторону удаленного обслуживания клиентов, обусловливает возникновение принципиально новых по отношению к стандартному обслуживанию клиентов в офисах банка рисков и угроз в сфере безопасности.

Выявление и предотвращение указанных угроз и снижение рисков является одной из ключевых задач при создании систем банковского дистанционного обслуживания, поскольку напрямую влияет на уровень доверия клиентов к данным сервисам. При этом средства решения данной задачи включают как собственно набор соответствующих технических и организационных мероприятий, так и просветительский аспект, который зачастую остается вне сферы внимания кредитных организаций. Так, анализ публикуемых на официальном сайте Банка России (www.cbr.ru) Обзоров о несанкционированных переводах денежных средств показывает, что первое место среди способов совершения таких несанкционированных операций в отношении физических лиц прочно удерживают методы социальной инженерии. В этой связи повышение уровня финансовой грамотности клиентов, пользующихся дистанционными сервисами, является

весьма важной задачей, в особенности с учетом существующей законодательной защиты финансовых интересов клиентов при выявлении несанкционированных операций с их денежными средствами. Соответственно, такая просветительская деятельность в отношении клиентов экономически выгодна и самим кредитным организациям.

Повышение уровня квалификации банковских специалистов по ИБ — направление, актуальность которого вроде бы не надо объяснять. Тем не менее, к сожалению, в особенности в непростых экономических условиях, зачастую этим вопросам не уделяется должного внимания. А на «темной стороне» активность не снижается. Кто бы еще несколько лет назад мог предположить, что атакам, в том числе успешным, подвергнутся системы доступа к счетам самих кредитных организаций в Банке России?

В свете изложенного невозможно переоценить информационные источники, которые комплексно и на высоком профессиональном уровне освещают различные аспекты обеспечения безопасности цифровых банковских сервисов. Особое место среди таких источников занимает настоящая книга — «Безопасность электронного банкинга», написанная представителями регулятора. Фактически это — настольная книга для самого широкого круга банковских специалистов, преподавателей, студентов и клиентов кредитных организаций.

Олег Николаевич Кисляк,
председатель наблюдательного совета
АО «Банк Воронеж»

СПИСОК АВТОРОВ

А.М. Сычев,	заместитель начальника Главного управления безопасности и защиты информации Банка России, кандидат технических наук (глава 6)
Д.Б. Фролов,	начальник Центра мониторинга и реагирования на компьютерные атаки в кредитно-финансовой сфере Главного управления безопасности и защиты информации Банка России, доктор политических наук, кандидат юридических наук (глава 2)
П.В. Ревенков,	заместитель начальника Центра мониторинга и реагирования на компьютерные атаки в кредитно-финансовой сфере Главного управления безопасности и защиты информации Банка России, доктор экономических наук (главы 1, 2, 3, 4)
С.В. Конявская,	генеральный директор компании САПР, кандидат филологических наук (глава 7)
А.Б. Дудка,	главный экономист Отдела банковского надзора Отделения по Омской области Сибирского главного управления Центрального банка Российской Федерации, кандидат экономических наук (глава 5).
А.А. Бердюгин,	независимый эксперт в области информационной безопасности (глава 2)
А.В. Неваленный,	независимый эксперт в области информационной безопасности (глава 8)
Д.Ю. Персанов,	корпоративный риск-менеджер группы QIWI (глава 8)

СПИСОК СОКРАЩЕНИЙ

АПО	Аппаратно-программное обеспечение
АРМ	Автоматизированное рабочее место
АС	Автоматизированная система
БКБН	Базельский комитет по банковскому надзору
ВРБ	Высшее руководство банка
ДБО	Дистанционное банковское облуживание
ИКТ	Информационно-коммуникационные технологии
ИТ	Информационные технологии
КА	Код аутентификации
ПАК	Программно-аппаратный комплекс
ПИБ	Политика информационной безопасности
ПИН	Персональный идентификационный номер
РКБ	Резидентный компонент безопасности
СБР	Системный банковский риск
СВА	Служба внутреннего аудита
СВК	Служба внутреннего контроля
СВТ	Средство вычислительной техники
СД	Совет директоров
СИБ	Служба информационной безопасности
СН	Служебный носитель
СУИБ	Система управления информационной безопасности
СФК	Среда функционирования криптографии
СЭДО	Система электронного документооборота
СЭБ	Система электронного банкинга
ТБР	Типичный банковский риск
ЦОД	Центр обработки данных
ЭБ	Электронный банкинг
ЭБР	Элементарный банковский риск

ВВЕДЕНИЕ

Электронный банкинг (ЭБ) — один из самых динамично развивающихся видов дистанционного банковского обслуживания (ДБО)[1]. Получив широкое распространение в Америке и Европе, ЭБ завоевывает и российский рынок.

Вот только самые известные преимущества, которые получает клиент кредитной организации, использующий для совершения своих банковских операций системы ЭБ (СЭБ):

- отсутствие необходимости для клиентов кредитных организаций посещать банк лично и возможность контролировать свои счета или управлять ими в так называемом режиме «24×7» (то есть круглосуточно 7 дней в неделю);
- ряд кредитных организаций устанавливает продленный режим операционного дня, и все платежи (зачисления и списания), поступившие в банк до 18:00 по московскому времени, исполняются банком в этот же операционный день;
- вся информация по счетам и операциям хранится на сервере кредитной организации и всегда доступна для пользователей ЭБ;
- для защиты информации используются современные средства криптографической защиты;
- разработчики большинства программных продуктов СЭБ производят обновление своих программ автоматически (не требуется обращения в кредитную организацию).

Внедрение данной услуги обходится для кредитной организации относительно недорого и в дальнейшем быстро окупается только за счет абонентской платы.

Однако, наряду с очевидной привлекательностью такого способа совершения банковских операций, как у кредитной организации, так

1 Как правило, под ДБО понимают совокупность методов представления банковских услуг с помощью средств телекоммуникации, при которых присутствие самого клиента в банке не требуется.

и у ее клиентов появляется немало дополнительных источников банковских рисков. Основными причинами их возникновения являются:

- виртуальный характер дистанционных банковских операций;
- общедоступность открытых телекоммуникационных систем;
- предельно высокая скорость выполнения транзакций;
- глобальные масштабы межсетевого операционного взаимодействия;
- активное участие фирм — провайдеров услуг в проведении операций.

Книга состоит из восьми глав, в которых последовательно рассматриваются вопросы, связанные с возрастанием рисков информационной безопасности в условиях ЭБ, принципами управления рисками ЭБ, организацией внутреннего контроля в банках и обеспечением информационной безопасности ЭБ с учетом требований стандартов Банка России по обеспечению информационной безопасности.

Данная книга не претендует на полное рассмотрение всевозможных угроз и сопутствующих рисков, связанных с внедрением в кредитных организациях СЭБ, однако может оказать помощь менеджерам банков, специалистам риск-подразделений, служб внутреннего контроля, подразделений безопасности и финансового мониторинга в разработке внутренних методических документов, направленных на минимизацию последствий проявления источников рисков, связанных с внедрением в кредитных организациях СЭБ.

1. ЭЛЕКТРОННЫЙ БАНКИНГ И РИСКИ НЕДОСТАТОЧНОГО ОБЕСПЕЧЕНИЯ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ

«Настанет время, когда наши потомки будут удивляться, что мы не знали таких очевидных вещей».

Луций Анней Сенека,
древнеримский философ

1.1. Интернет и банковский бизнес

«Во всех странах железные дороги для передвижения служат, а у нас сверх того и для воровства».

Михаил Салтыков-Щедрин,
русский писатель

Современный банковский бизнес невозможно представить без использования новейших достижений в области информационных и телекоммуникационных технологий. Технологии ДБО стали не только способом снижения себестоимости самих процессов выполнения банковских операций, но и основным конкурентным преимуществом любой кредитной организации на рынке банковских услуг.

Одним из условий повышения доверия к технологиям ДБО является обеспечение должного уровня информационной безопасности.

Перед тем как начать разговор о проблемах, связанных с безопасным применением различных систем ДБО (включая СЭБ), необходимо разобраться, что такое безопасность.

Безопасность (как самостоятельный объект исследования) имеет некоторые фундаментальные свойства:

1) безопасность никогда не бывает абсолютной — всегда есть некий риск ее нарушения, таким образом, усилия по обеспечению безопасности реально сводятся к задаче понижения уровня риска до приемлемого;

2) измерить уровень безопасности невозможно, можно лишь косвенно его оценить, измерив соответствующие показатели, характеризующие состояние безопасности банка[2];
3) наступление рискового события в общем случае предотвратить невозможно, можно лишь понизить вероятность его наступления, то есть добиться того, что такие события будут наступать реже;
4) можно также понизить степень ущерба от наступления такого события, но при этом чем реже наступает рисковое событие, тем сильнее ущерб от него;
5) при любом несанкционированном вмешательстве в процесс обработки информации и принятия управленческих решений в первую очередь страдает ее безопасность.

Учитывая, что современный банк представляет собой комплекс, состоящий не только из квалифицированного персонала, но и из сложных автоматизированных систем, одним из наиболее уязвимых его элементов является банковская автоматизированная система кредитной организации.

Современные достижения в развитии информационных и коммуникационных технологий, в основе которых лежат возможности глобальной сети Интернет, значительно повлияли на эволюционные процессы, связанные с формами проявления функции денег как средства платежа, и привели к формированию глобальной электронной среды для экономической деятельности за счет существенного снижения себестоимости выполнения банковских операций. Технологии ДБО можно рассматривать и как качественный аспект поступательного развития кредита[3].

Еще в конце прошлого века эксперты в области экономики стали говорить о новой среде — «сетевой экономике» (networked economy)[4]. Так, например, в докладе, подготовленном Европейской

2 В связи с этим можно говорить только о вероятности наступления того или иного события и степени его последствий, то есть использовать для оценок уровня безопасности рисковый подход.

3 См.: Валенцева Н.И. Законы и закономерности развития кредита // Банковские услуги. 2010. № 12. С. 2–9.

4 Данное понятие часто упоминается в сочетании со словом «глобальная».

комиссией[5], глобальная сетевая экономика определяется как «среда, в которой любая компания или индивид, находящиеся в любой точке экономической системы, могут контактировать легко и с минимальными затратами с любой другой компанией или индивидом по поводу совместной работы, для торговли, для обмена идеями и ноу-хау или просто для удовольствия». Возникновение сетевой экономики приводит к эволюции современных экономических систем, развитию нерыночных механизмов регулирования и сетевых организационных структур.

Новые возможности глобальных коммуникаций между людьми дают им и новые инструменты для реорганизации форм их совместной деятельности.

Одним из самых эффективных способов модернизации инфраструктуры в экономике и создания сетевых институциональных структур является использование возможностей интернет-технологий.

Интернет-технологии не только быстро внедряются в политику, бизнес, государственное управление, но и трансформируют характер межличностных отношений в обществе (формируются виртуальные онлайновые сообщества, устанавливаются отношения информационного партнерства, осуществляется группировка пользователей по определенным информационным интересам). Все это приводит к тому, что общество привыкает к активному использованию современных информационных и коммуникационных технологий. Тенденция распространяется и на банковские услуги. Это свидетельствует о том, что мы имеем дело с самым быстрорастущим в истории человечества рыночным сообществом. Буквально за несколько лет все основные экономические виды деятельности были освоены Интернетом и появились: интернет-коммерция, интернет-реклама, интернет-банкинг и т. д.

Анализ научных трудов отечественных и зарубежных ученых позволил выявить ряд отличительных признаков Всемирной паутины, способных существенным образом влиять на экономику:

5 Status Report on European Telework // Telework 1997, European Commission Report, 1997. URL: http://www.eto.org.uk/twork/tw97eto

- Интернет втягивает в глобальную конкуренцию все компании и организации (в том числе коммерческие банки) независимо от места их расположения. Большинство кредитных организаций предоставляет одинаковый набор банковских услуг, поэтому выбор клиентов, как правило, связан с качеством их оказания и уровнем доверия к данному коммерческому банку;
- Глобальная сеть значительно обострила конкурентную борьбу и потребовала от всех участников банковского рынка соответствия международным стандартам (оформление web-сайтов, поддержка нескольких языков, доступность и функциональность своих представительств в Интернете и т. д.);
- многие процессы, в том числе обслуживание и эксплуатацию аппаратно-программного обеспечения систем ДБО (включая СЭБ), можно передать в аутсорсинг. Многие web-сайты кредитных организаций разрабатывали профессиональные компании, хорошо владеющие вопросами продвижения брендов и привлечения максимального числа клиентов;
- клиенты, использующие системы интернет-банкинга, более требовательны к качеству выполнения банковских операций, так как могут легко сравнивать с аналогичными услугами других кредитных организаций-конкурентов (значительно удаленные географически банки в Глобальной сети находятся «на расстоянии одного клика»);
- Интернет позволяет выбирать коммерческие банки почти в любой стране мира и устанавливать с ними взаимовыгодное сотрудничество для повышения эффективности и снижения издержек;
- стремительное развитие интернет-технологий не позволяет однозначно спрогнозировать все стратегические риски, связанные с ДБО;
- Интернет ускоряет распространение новых технологий и идей. Коммерческие банки в любой стране мира, в том числе в развивающейся, могут с помощью Глобальной сети отслеживать технологические инновации, получать

информацию о новых банковских продуктах, используемых в Европе, Японии, Северной Америке, и о новых проектах и действиях лидеров в каждом секторе банковского бизнеса — с точки зрения бизнеса национальные границы утратили свое былое значение;

- электронные банковские технологии требуют от коммерческих банков действовать «в режиме Интернета» или «со скоростью Интернета» — скорость становится одним из основных достоинств успешного бизнеса;
- технологии ДБО (включая СЭБ) позволяют оформлять первичные бухгалтерские документы намного быстрее;
- Интернет служит самым дешевым на сегодняшний день каналом обслуживания клиентов. Предоставление банковских услуг через Интернет позволяет сократить служащих, которые ведут телефонные переговоры, оформляют банковские документы, консультируют клиентов по особенностям выполнения отдельных банковских операций, принимают различные претензии, предложения и др.[6];
- под интернет-проекты относительно легко получить инвестиции. Во многих странах инвестиции в интернет-проекты поддерживаются государством, так как, развивая интернет-технологии во всех отраслях экономики (включая банковский бизнес), страна выходит на новый качественный уровень;
- интернет-технологиям постоянно требуется ценный ресурс — человеческий талант, как в форме технических знаний и опыта, так и в форме управленческих ноу-хау. Самые ценные в конкурентном отношении активы организации — это лидерство в разработке ключевых технологий и кадры с уникальным опытом и знаниями.

6 Еще в середине 1999 г. на web-сайте Международного валютного фонда были приведены расчеты затрат на выполнение банковских операций, где стоимость ручной обработки транзакции в филиале коммерческого банка обычно составляла в среднем более 1 долл., телефонное обслуживание оценивалось в 60 центов за услугу, транзакции через банкоматы и клиринговые центры стоили около 25 центов, а транзакция через Интернет обходилась всего в 1 цент. Учитывая постоянное снижение тарифов на предоставление Интернета, можно предположить, что сейчас банковские операции, выполняемые в рамках интернет-банкинга, обходятся еще дешевле.

Благодаря возможностям Интернета сообщество людей стало преобразовываться в новую социально-экономическую формацию — глобальное информационное общество.

На данном этапе развития общества можно говорить об информационной революции, которая постепенно охватывает все страны, невзирая на их экономическое развитие и уровень финансовой грамотности населения.

Интернет изменил мир и продолжает менять его в геометрической прогрессии. Изменились отношения людей, их общение, поиск данных, мировоззрение, а вместе с тем методы работы институтов и организаций. Каких-то 15 лет назад еще не было таких профессий, как разработчик архитектуры социальных сетей и руководитель цифровой рекламы. В последние годы в нашу жизнь ворвались и с тех пор доминируют в ней Facebook, LiveJournal, YouTube, Twitter, Skype и многие другие интернет-продукты и социальные сети. Эти технологии стабильно наращивают темпы своего развития.

Многие банки сегодня рассматривают Facebook[7] как важный источник информации, поскольку данная социальная сеть содержит огромное количество информации о пользователях. Эти данные могут быть использованы для оценки кредитных рисков и кредитоспособности клиентов.

Сегодня мы производим и потребляем контент с огромной скоростью. Темпы обращения клиентов интернет-пространства с информацией отражает статистика:

- каждую минуту на YouTube загружают 300 часов видео;
- каждую минуту в Twitter посылают 278 000 сообщений;
- каждый час около 10,5 млн песен загружают незаконно, по большей части из мест, где законная загрузка невозможна;
- каждый день создают 7000 новых статей в Wikipedia;
- каждый день на Facebook заходит более 720 млн пользователей.

Отметим особенность в поведении людей, которая стала проявляться в связи с появлением Интернета. Все большее количество

7 Имея более 1,7 млрд зарегистрированных пользователей, эта социальная сеть фактически является крупнейшей базой данных в мире.

людей предпочитают потреблять значительное количество маленьких фрагментов информации, нежели целостный блок текста[8].

Зная об этом, западные информационные агентства на своих интернет-страницах иногда пишут абзацы, состоящие из одного предложения. Маленьким фрагментом сложно (а чаще невозможно) передать много смысла, но для совершения транзакции с помощью систем ДБО клиент и не должен читать длинные инструкции (они могут быть оформлены в аудио- или видеоролик).

Заметим, что информационные процессы человека, такие как обнаружение и интерпретация сенсорных сигналов, память, образы, мышление и их изменения во времени, представляют объект исследования когнитивной психологии. Поэтому серьезные компании, занимающиеся созданием программ для систем ДБО и пользовательских интерфейсов, основывают свои разработки на моделях, являющихся плодами когнитивной психологии.

По мере проникновения Интернета в нашу жизнь растет популярность всевозможных мобильных устройств. Классические ноутбуки слишком громоздки, а планшеты еще не всегда обладают нужной функциональностью, поэтому и появляются все новые и новые миниатюрные лэптопы с сенсорными экранами.

Подобные устройства теперь не роскошь, а неотъемлемые компаньоны современного человека (в этом убеждаешься, когда забываешь мобильный телефон или планшетный компьютер дома).

По оценке Бретта Кинга, основателя первого в мире мобильного банка Movenbank, в 2016 г. среднестатистический клиент розничного банка в развитых странах взаимодействовал с ним следующим образом:

- отделение (1-2 раза в год);
- колл-центр, система интерактивного речевого ответа IVR (5–10 раз в месяц);
- банкомат (3–5 раз в месяц);
- Интернет (с использованием компьютера или планшета, 7–10 раз в месяц);
- мобильный телефон (20–30 раз в месяц).

8 По этой же причине у многих возникает желание пропустить большой абзац.

По данным исследования, проведенного специалистами компании Juniper Research, к концу 2019 г. более 1,75 млрд владельцев мобильных устройств (каждый третий взрослый житель Земли) будут использовать их для банковских целей. Для сравнения, на сегодняшний день сервисами мобильного банкинга пользуются около 800 млн человек во всем мире[9].

В России ежегодно растет количество интернет-пользователей. По результатам опроса Фонда «Общественное мнение», в 2016 г. Интернетом пользовались 83 млн россиян[10].

Смелые прогнозы, конечно, можно подвергать сомнению, но очевидно, что наша потребность в наличных деньгах будет постоянно уменьшаться — их заменят электронные деньги и ЭБ.

Еще одно изобретение человечества в сфере высоких технологий — это «облака». Облачные платформы все чаще и успешнее используются для решения корпоративных и операторских задач. В отчете аналитической компании IDC говорится, что в 2012 г. на программное обеспечение для частных «облаков», включая «облака» с хостингом, тратилось 62% ИТ-бюджетов[11].

В целом применение облачных технологий позволяет:

- создать простую абстрактную среду, в которой пользователь может получить ресурсы по требованию, а компания — легче и быстрее внедрить новые приложения и услуги;
- отвлечь организацию от рутинных задач и сконцентрировать внимание на главных направлениях, выделяющих ее из конкурентной среды и значительно повышающих эффективность работы.

Нигерийская кредитная организация Renaissance Credit, образованная в октябре 2012 г., за первые полгода расширила клиентскую базу до 3000 человек. Все информационные процессы компании (составление документов, работа с электронными таблицами

9 См. подробнее: «Через 5 лет каждый третий взрослый житель планеты будет пользоваться мобильным банкингом» // MoneyNews.ru. 9 июля 2014 г.

10 См. подробнее: «Количество пользователей Интернета в России» // www.bizhit.ru/index/users_count/0–151. 7 ноября 2016 г.

11 См. подробнее: Джоанн Старк. Как воспарить в облака. URL: www.cisco.com/web/services/it-case-studies/swisscom-telecommunications-case-study.html

и почтой, а также все банковские операции) происходят «на облаке», что позволило сократить штат ИТ-специалистов до одного человека[12].

По словам представителя Microsoft, в богатых странах банки с помощью облачных технологий уже начали обрабатывать данные, не содержащие значимой информации о клиентах, но требующие больших вычислительных мощностей. Испанский банк Bankinter использует облачную платформу Amazon для моделирования кредитных рисков: вычисления, выполнявшиеся на оборудовании самого банка за 20 часов, теперь занимают 20 минут. Также крупные банки задействуют «облака» для тестирования своих компьютерных систем, не подвергая сам банк опасности сбоев. Многие банки переконфигурируют свои системы в частные облачные платформы, что также позволяет подключаться к облачным технологиям, находящимся в общественном доступе.

Разумеется, у широкого применения «облаков» есть и свои недостатки. Прежде всего, это безопасность и защита данных. Небольшим банкам крупные информационные центры, созданные такими компаниями, как Amazon и Microsoft, обеспечивают более высокий уровень безопасности, чем они сами могут себе позволить. Крупные банки, имеющие собственные вычислительные центры, опасаются передавать клиентскую информацию в посторонние руки. Кроме того, кража информации или сбой в работе банка, пользующегося «облаком», вызовет жесткую реакцию регулирующих органов. Некоторые страны настаивают на том, чтобы данные клиентов хранились в пределах национальных границ. Компании, предоставляющие облачные услуги, будут вынуждены строить небольшие информационные центры, снижая тем самым экономию издержек. Кроме того, эти компании из соображений безопасности стремятся не раскрывать местонахождение своих «облаков».

Впрочем, возможность повышения рентабельности делает переход банков на облачные технологии неизбежным, а указанные выше проблемы могут повлиять лишь на скорость указанного процесса.

12 См. подробнее: The IT cloud // The Economist. 2013. № 8845. P. 61.

1.2. Основные виды мошенничества в сети Интернет

Сегодня из всех видов ДБО наиболее востребованным является интернет-банкинг, который представляет собой способ ДБО 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[13].

Использование Интернета изначально сопряжено с рисками, так как многие способы мошенничества совершаются именно с применением возможностей Глобальной сети.

Приведем несколько известных способов мошенничества в Интернете.

Фишинг (phishing) — способ мошеннических действий, при котором злоумышленник рассылает множество сообщений по электронной почте с целью получения личной и финансовой информации о потенциальных жертвах (для дальнейшего доступа к их банковским счетам и другим важным ресурсам)[14].

Подобные сообщения приходят якобы от лица банков, платежных систем, онлайн-аукционов, крупных и широко известных интернет-магазинов. Письмо создается, форматируется и оформляется таким образом, чтобы выглядеть как отправленное легальным источником. Причем подделываются заголовки письма, его внешний вид (включая графические и текстовые элементы), а также ссылки на реальный web-сайт. В случае с интернет-банкингом, как правило, письмо содержит информацию о внезапно возникших технических проблемах на web-сайте банка, в связи с чем необходима проверка учетных записей и регистрационных данных пользователей. Далее жертве предлагается открыть «регистрационную форму» и ввести интересующие мошенника данные. И так как эта регистрационная

13 Данное определение приведено в Письме Банка России от 31 марта 2008 г. № 36-Т «О Рекомендациях по организации управления рисками, возникающими при осуществлении кредитными организациями операций с применением систем интернет-банкинга» и, по мнению авторов, является наиболее полным.

14 По данным Антифишинговой рабочей группы (APWG — Anti-Phishing Working Group), количество фишинговых атак ежемесячно увеличивается на 50%, причем их главной целью является банковское мошенничество.

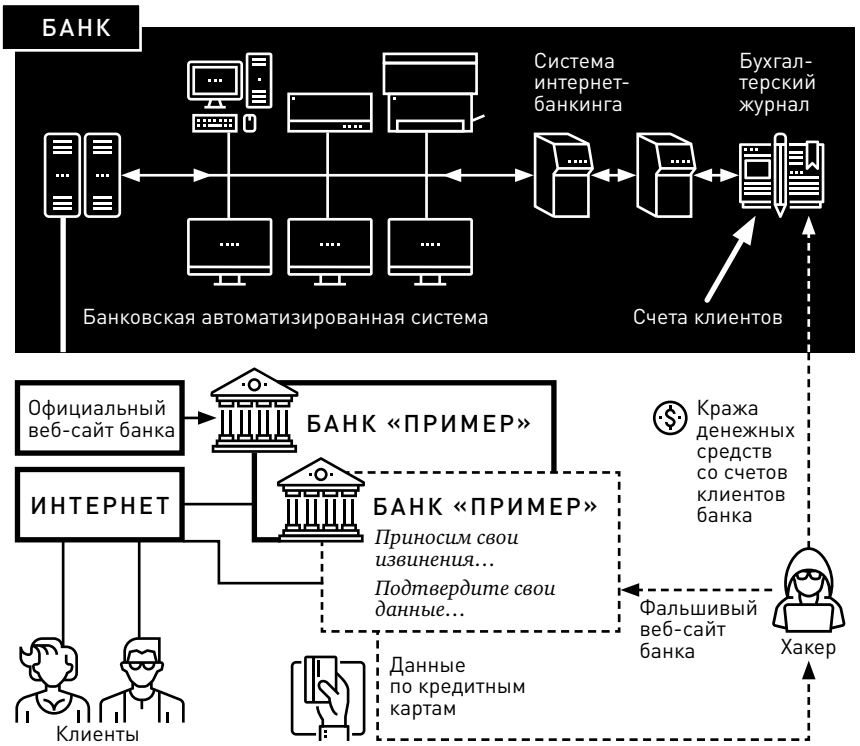

Рис. 1. Использование фальшивого web-сайта для выманивания данных по кредитным картам

форма загружается не с web-сайта банка, то вся личная информация жертвы отправляется мошеннику. Получив эти данные, мошенник распоряжается банковским счетом жертвы и кредитной картой по своему усмотрению (рис. 1).

Приведем основные рекомендации для клиентов системы интернет-банкинга, которые могут помочь определить действия интернет-мошенников[15]:

15 Эти же рекомендации должны знать и специалисты кредитной организации, отвечающие за бесперебойное и безопасное функционирование web-сайта, чтобы без промедления пресекать подобные мошеннические действия.

- никогда не следует отвечать на запросы, касающиеся личной информации, данных банковских счетов, кредитных карт и паролей доступа, которые приходят по электронной почте;
- стараться не использовать ссылки на интернет-ресурсы, которые содержатся в сообщениях, присланных по электронной почте, а вводить URL сайта в адресную строку web-браузера самостоятельно;
- убеждаться, что при работе с web-сайтом кредитной организации информация передается в кодированном (шифрованном) виде;
- регулярно проверять состояние баланса банковского счета (кредитной карты);
- немедленно сообщать уполномоченным сотрудникам кредитной организации о всех подозрениях в случаях несанкционированного доступа к личной информации и злоупотребления ею.

Вот несколько признаков, по которым можно определить, что соединение произошло с фальшивым web-сайтом:

- невозможно просмотреть исходный текст сайта[16];
- при использовании другого web-браузера адресная строка заметно не «попадает» на привычное место;
- при сворачивании окна web-браузера на панель задач окошко с ложным адресом не сворачивается, а «зависает» в нижней части экрана;
- окно с ложной адресной строкой ведет себя как самостоятельное окно Windows-задачи с возможностью перемещения по экрану монитора, но с тенденцией занять определенное место;
- фальшивую адресную строку невозможно редактировать.

Схемы «быстрого» обогащения («Золотой поток» (Golden Stream), «Алмазный дождь» (Diamond Rain) и др.). Речь идет о всевозможных пирамидах. Как правило, все начинается с того, что

16 Самостоятельно получить сведения о web-сайте можно на следующих сетевых ресурсах: www.dnsdtuff.com, www.geobytes.com, www.nextwebsecurity.com, www.domaintools.com и др.

на электронный адрес потенциальной жертвы приходит письмо с предложением заработать большие деньги, участвуя в игре. Например, перечислив 100 руб. (такое предложение было в игре «Золотой поток») можно заработать 1 млн руб. всего за 90 дней[17]. В ответ на пересылку 100 руб. жертва получает какую-нибудь дополнительную информацию или программу. Далее, как обещают организаторы, все зависит только от активности игрока: чтобы заработать свой миллион рублей, он должен искать новых «участников», и чем быстрее, тем лучше. Писем, которые начинались с просьбы дочитать обязательно до конца и не сравнивать эту игру с другими, было много. При этом принцип во всех этих схемах один — в самом начале игры жертва теряет некоторую сумму денег и все дальнейшие усилия тратит на компенсацию своих потерь, подыскивая новых «участников».

Лотерея или розыгрыш. Мошенники начинают с массовой рассылки писем с предложением принять участие в каком-нибудь несложном конкурсе (например, придумать название для какого-нибудь магазина или компании).

После отправления какого-либо варианта ответа отправителю высылают «поздравительное письмо» о том, что его вариант признан лучшим и для получения главного приза необходимы некоторые формальности. Мошенники даже могут запросить какие-нибудь сведения, то есть «продолжить разговор», для того чтобы потенциальная жертва поверила в честность данной затеи. Затем наступает самое главное — мошенники просят перечислить небольшую сумму (по сравнению с выигрышем) для оплаты услуг нотариуса или другого специалиста. Как только «победитель» перечисляет деньги — связь с ним прекращается навсегда.

«Нигерийские письма». Афера с «нигерийскими письмами»[18] — это современный вариант известного сотни лет

17 Все эти махинации носят название MLN-схемы (Multi Level Marketing — многоуровневый маркетинг).

18 Другое распространенное название «Афера 419» (по номеру соответствующей статьи в Уголовном кодексе Нигерии).

назад мошенничества «Испанский узник», когда самозваные графы Монте-Кристо XVIII в., используя обычную почту, выманивали деньги у доверчивых людей, обещая им несметные сокровища, зарытые где-то в дальних странах.

Мошенники рассылают письма (в нашем случае по электронной почте, хотя может использоваться и обычная почта или факс), в которых содержится очень выгодное деловое предложение по переводу значительной суммы денег с африканского континента за рубеж под очень солидные комиссионные (до 40%)[19]. От жертвы требуется совсем немного — предоставить свои личные данные в качестве гарантии сохранности денег и расчетный счет в банке для размещения средств. Сценарии дальнейшего развития сюжета похожи на описанные выше. Под каким-либо предлогом мошенники просят перечислить незначительную сумму за выполнение услуг. Это могут быть просьбы внести деньги на оплату услуг юриста, компенсировать стоимость пересылки каких-либо документов и т. д. Дальше мошенники (если имеют необходимую информацию для снятия денег со счета жертвы) опустошают его счет, а могут и пригласить в какую-нибудь страну, где также, но уже с применением силы отнимают все деньги.

Существует много разновидностей «нигерийской» аферы, но идея везде одна: требуется оказать помощь хозяину по переводу значительной суммы денег под очень высокий процент[20].

Опасные инвестиции. Сущность данных афер заключается в предложениях инвестировать денежные средства в какое-нибудь дело (выпуск дорогостоящего продукта, ценные бумаги и т. д.). Проценты (очень высокие), как правило, начисляются каждый день (об этом инвестор может узнать на web-сайте инвестиционного фонда). Но как только инвестор захочет взять свои деньги — у него, как и во всех перечисленных выше случаях, возникают

19 Надо отметить, что география подобных преступлений постоянно растет, были даже примеры, когда делили сбережения российских олигархов.

20 Сразу хочется задать вопрос, почему обладатель такого состояния решает обратиться через сеть Интернет к незнакомцу, а не иметь дело со знакомым и проверенным человеком.

проблемы: web-сайт инвестиционного фонда исчезает или становится недоступен, а адрес электронной почты (зарегистрированный на одном из бесплатных почтовых серверов) становится безответным.

Виртуальная медицина. «Хватит переплачивать за лекарства — посетите наш магазин» — примерно такие сообщения приходят на многие адреса электронной почты с указанием адреса web-сайта (торговой точки). Практически все лекарственные препараты (более 97%), реализация которых производилась через интернет-сайты, рекламированные в спаме, являются контрафактными. Фальсифицированные таблетки производятся без надлежащего контроля качества и с нарушениями технологического процесса (при этом внешний вид и упаковка практически неотличимы от настоящих). Очевидно, что, кроме вреда, такие препараты ничего принести не могут.

Другой исход при обращении в такие виртуальные аптеки — потеря денежных средств (отправленных в виде предоплаты за лекарства и доставку).

По статистике, на подобные web-сайты заходят от 500 000 до 2 млн посетителей в месяц. Помимо опасности отдать преступникам свои деньги и приобрести контрафактные и недоброкачественные лекарственные препараты, здесь существует и еще одна опасность. Открывая такие спам-письма, можно загрузить на свой компьютер вредоносную программу (червя[21], трояна[22] и др.) и в дальнейшем придется заниматься не только своим лечением, но и лечением своего компьютера.

Виртуальное трудоустройство. В основном предложения касаются работы в сети Интернет (на дому), например, «виртуальным бухгалтером». Будущему работнику предлагают заниматься

21 Червь (worm) — разновидность самовоспроизводящихся компьютерных программ, распространяющихся в локальных и глобальных компьютерных сетях. В отличие от компьютерных вирусов червь является самостоятельной программой.

22 Троянская программа, или троян (trojan) — разновидность компьютерных программ, которые «претендуют» на то, что выполняют некоторую определенную функцию, в действительности же работают совершенно иначе (свое название получила в честь «троянского коня»).

определенными посредническими услугами не больше 2–3 часов в день и получать заработную плату около 400 долл. Чаще всего работать предлагают с системой WebMoney. Работодатель открывает для работника новый счет (кошелек) и получает для него аттестат. Владельцем счета является работодатель. Работа заключается в том, чтобы осуществлять денежные переводы (WMZ[23]). Все переводы (их бывает от 30 до 50 в день) нужно осуществлять в течение суток. В среднем затрачиваются 2–3 минуты на один перевод. Предложение достаточно заманчивое (как, впрочем, и все те, которые были описаны выше), только в данном случае работодатель просит перевести 7 долл. (7 WMZ) на получение аттестата (своего рода гарантия для работодателя компенсировать свои затраты в случае вашего отказа).

Конечно, 7 долл. не такая уж большая сумма, но на это и рассчитана данная афера. После того как жертва перечислит эти деньги на получение аттестата, связь с ней прекратится.

Кстати, можете попробовать представиться работодателю опытным пользователем сети Интернет, знакомым со всеми платежными системами. Потом скажите, что у вас есть счет в платежной системе, в которой вам предлагают работать, а также персональный аттестат и что работа с денежными переводами вам хорошо знакома. Скорее всего, мошенники сразу оставят вас в покое, так как такие «кадры» им не нужны.

Ниже приведены несколько признаков, по которым можно определить, что работу, скорее всего, предлагают мошенники:

- расплывчатые описания вакансий;
- неясные требования к работникам;
- бесплатное обучение;
- слишком высокая заработная плата;
- обширный социальный пакет;
- в качестве реквизитов указан анонимный абонентский ящик или адрес электронной почты;
- обещание гарантированного трудоустройства.

23 В системе WebMoney используются различные валюты, WMZ — средства, эквивалентные долларам США.

Горячие торговые точки. Интернет-магазины сегодня привлекают покупателей своими ценами (за счет экономии на аренде помещений для магазина), а также возможностью удобной доставки. Но и здесь бывают такие цены, о каких никто даже и не мечтал. Причем продавец обосновывает эти цены, иногда совсем не скрывая таких фактов, как «товар краденый», «конфискованный» и т. п.

Поэтому если жертва и решит покупать такой товар, то вряд ли потом пойдет жаловаться, так как по сути является соучастником преступления (скупка краденого).

Схема мошенничества в данном случае прежняя: как только покупатель переводит свои деньги на счет продавца, связь с ним прекращается (web-сайт магазина перестает работать, электронная почта не отвечает).

«Сетевое попрошайничество». Если раньше большинство попрошаек можно было встретить на городских площадях и вокзалах, то теперь появился целый класс сетевых попрошаек, которые обращаются за помощью посредством сети Интернет. Выпрашивают деньги под разными предлогами: на срочную и дорогую операцию, избавиться от угроз вымогателей, погасить кредит и т. п.

Можно встретить сообщения о внезапно возникших проблемах в платежной системе WebMoney[24], в связи с чем администратор просит перечислить какую-то сумму на свой кошелек для решения проблем. Причем если клиент, к которому обращается администратор, не перечислит деньги — в дальнейшем он не сможет воспользоваться своим кошельком (то есть своими деньгами).

К сожалению, есть случаи, когда люди, особо не вдумываясь в суть происходящего, перечисляют свои деньги и потом узнают, что обращение поступило от мошенника, а не от администратора системы WebMoney.

В качестве совета можно порекомендовать — ни в коем случае не перечислять свои деньги до тех пор, пока не пришло подтверждение достоверности полученного сообщения.

24 В последнее время в качестве причин проблем все чаще называют финансовый кризис.

Ботнеты[25]. Термин «бот» появился намного раньше, чем его стали использовать для обозначения компьютерного вируса и инструмента для атаки на компьютеры и сети. В IRC-сетях он до сих пор обозначает специальную программу, которая замещает собой живого человека и может поддерживать активность на IRC-канале даже в то время, когда к нему не подключен ни один из пользователей. Бот может контролировать и модерировать содержание бесед на канале, удалять посетителей, которые нарушают принятые правила поведения, и т. д. Это своего рода вариант искусственного разума.

Однако на вооружении хакера бот может доставить серьезные проблемы. В сети Интернет хакеры также могут находить незащищенные компьютеры и загружать на них специальные программы, которые будут по их команде выполнять различные действия (например, рассылка спама или участие в DDoS-атаке).

В качестве защиты от подобного заражения можно порекомендовать иметь в арсенале защитных средств хороший и мощный анализатор сетевого трафика, который позволит выполнять диагностику, идентификацию и перенаправление всего подозрительного интернет-трафика. Можно также использовать программное обеспечение для фильтрации пакетов, комбинируя со специальными техническими и аппаратными средствами, которые устанавливаются между маршрутизаторами и межсетевыми экранами.

Достаточно эффективный способ решения этих проблем разработало правительство Австралии. Во взаимодействии с пятью крупнейшими интернет-провайдерами страны оно создало технологию и программу для своевременного обнаружения компьютеров-зомби и принятия оперативных мер по их блокировке. В большинстве случаев владельцы своих компьютеров даже не представляли, что они участвовали в DDoS-атаке или что с их IP-адреса рассылался спам.

Сетевые банды. Одной из тенденций сегодняшнего дня является заметное возрастание новых компьютерных вирусов, червей и троянских программ. Троянские программы не могут рассылать себя по сети Интернет самостоятельно, подобно компьютерным вирусам,

25 Ботнет (botnet) — компьютерная сеть, состоящая из некоторого количества зараженных компьютеров (ботов).

так что масштабы их распространения должны быть меньше, чем у вирусов. Но на самом деле количество троянских программ и пораженных ими компьютеров становится с каждым годом все больше и больше. Поэтому специалисты компании Sophos[26] сделали вывод, что такая ситуация стала следствием активности профессиональных преступников.

Криминальные группы, которые ранее занимались исключительно мошенничеством с банковскими картами, начали объединяться и все более тесно сотрудничать с создателями компьютерных вирусов, спамерами и группами безжалостных хакеров.

Приведенные примеры мошенничества в сети Интернет ни в коем случае нельзя считать исчерпывающим перечнем всевозможных ухищрений компьютерных злоумышленников. К сожалению, во Всемирной паутине, которая является, по своей сути, неуправляемой средой, постоянно возникают все новые и новые угрозы со стороны хакеров. И от того, насколько своевременно будет построена защита от новых угроз, будет зависеть доверие клиентов кредитных организаций к технологиям ДБО (включая СЭБ).

В условиях ДБО клиентов кредитные организации вынуждены существенно повышать уровень обеспечения информационной безопасности, так как основные атаки киберпреступников направлены именно на тех клиентов банков, которые осуществляют свои операции удаленно (то есть вне офиса).

Очевидно, что абсолютной защиты от угроз для ДБО не существует. Компьютерные злоумышленники в состоянии взломать практически любую систему[27]. Однако непрерывная работа по поддержанию достаточного уровня информационной безопасности может сильно осложнить и (или) свести к минимуму возможности кибермошенников.

Масштабы кибермошенничества заставляют серьезно относиться к данному виду преступлений. Так, например, в июне 2012 г. новостные агентства распространили информацию о задержании преступной

26 Компания Sophos является одним из мировых лидеров в области решений для информационной безопасности.

27 Плюс сами банки иногда используют недостаточно надежные системы ДБО.

группы, включая ее организатора[28], который вместе со своими сообщниками похитил из систем ДБО более 150 млн руб.

По словам генерального директора компании Group-IB[29] Ильи Сачкова, принимавшего участие в расследовании деятельности данной преступной группы, это самая большая по численности участников киберпреступная группировка в России из тех, о которых известно специалистам по информационной безопасности[30]. В течение 2011 г. работала целая группа технических специалистов: заливщиков (распространителей вредоносного программного обеспечения), специалистов по шифрованию, администраторов, обслуживавших бот-сети, и др.

На протяжении последних трех лет, по данным Group-IB, мошенники использовали зарекомендовавшую себя в хакерских кругах троянскую программу Carberp[31]. Обобщая наиболее распространенные схемы совершения киберпреступлений в системах ДБО, можно выделить два способа.

Если сумма украденного составляет не более 1–1,5 млн руб., то деньги выводят сразу на пластиковые карты так называемых дропов (специально нанятых владельцев банковских карт, которые занимаются обналичиванием похищенных денег). Обычно в течение 15 минут после того, как деньги поступили на карточные счета, дропы обналичивают их через банкоматы и затем отдают своим нанимателям (рис. 2).

28 Более известен во Всемирной сети под псевдонимами Гермес и Араши.

29 Компания Group-IB является международной компанией, лидером российского рынка по оказанию полного комплекса услуг в области расследований инцидентов информационной безопасности и компьютерных преступлений, начиная от оперативного реагирования на инцидент и заканчивая постинцидентным консалтингом (официальный сайт компании http://www.group-ib.ru).

30 См. подробнее интервью Ильи Сачкова для РИА Новости «Хакер, укравший 150 млн руб., работал с 25 сообщниками» // Прайм. Бизнес-лента 22 июня 2012 г., а также «Гендиректор Group-IB: у хакеров есть несколько собственных платежных систем» // ПЛАС-daily. 19 июля 2012 г.

31 Carberp — распространенная среди киберпреступников вредоносная программа. Она собирает информацию о пользователе и системе и отправляет на сервер злоумышленников. Также бот может делать снимки экрана, перехватывать нажатия клавиш, содержимое буфера обмена и отправлять на сервер. Троянец имеет возможность самоудаления и установки дополнительных вредоносных модулей, крадет цифровые сертификаты для популярных систем ДБО.

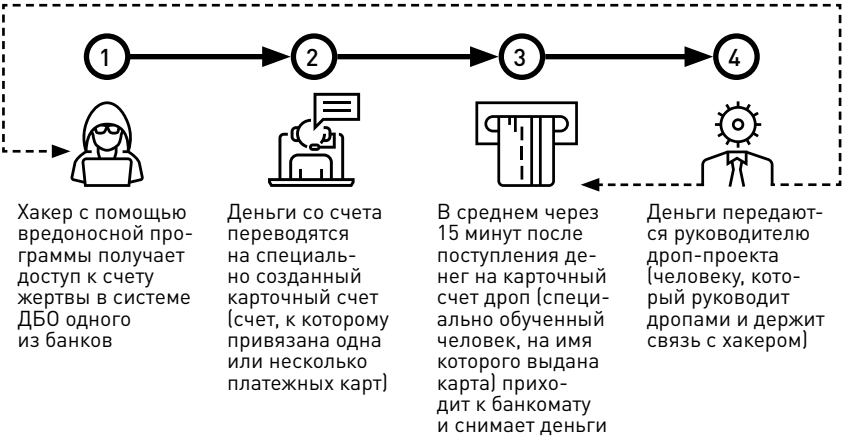

Рис. 2. «Простая» схема — примерно до 1,5 млн руб.

Если суммы крупнее, используются более сложные схемы обналичивания. Они применяются обычно при хищении средств в объеме от 1 млн до 5 млн руб. В этом случае деньги предварительно переводят на счет юридического лица. Дальше сумму могут раздробить и распределить по другим счетам, чтобы сильнее запутать следы (рис. 3).

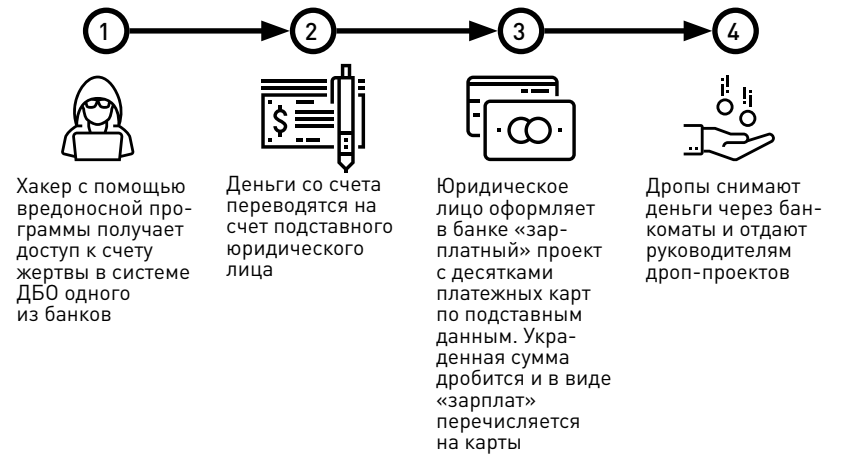

Рис. 3. «Сложная» схема — примерно до 5 млн руб.

Группы мошенников, специализирующиеся на обналичивании, минимум 50% суммы оставляют себе. Такой большой процент объясняется тем, что хищению предшествует длительный период подготовки. «Обнальщики» и похитители договариваются заранее. К моменту, когда производится хищение, у «обнальщиков» уже все готово: создано подставное юридическое лицо, открыт счет в банке и выпущены карты, которые раздали дропам.

Современные условия позволяют любому юридическому лицу удаленно создать «зарплатный проект». Условно говоря, представитель компании сообщает в банк: у нас работают 15 человек, нам нужны зарплатные карты. Далее банку предоставляются паспортные данные «сотрудников», и тот выпускает карты. Паспортные данные берутся у тех же дропов или покупаются на хакерских форумах.

Кибермошенники чаще прибегают к помощи «обнальщиков», чем самостоятельно разворачивают дроп-проекты[32].

В последнее время участились кражи из электронных платежных систем. Схемы примерно те же, только деньги выводятся либо на другие кошельки, либо опять же на банковские карты.

Распределение ответственности в сфере применения технологий ДБО в связи с вступлением в действие статьи 9[33] Федерального закона Российской Федерации от 27 июня 2011 г. № 161-ФЗ «О Национальной платежной системе» — наиболее острый вопрос, требующий доработки и четкого понимания обеими сторонами (банками и их клиентами). В действующей редакции большая часть ответственности переходит на кредитные организации, поэтому становятся понятны их многочисленные обращения к регулятору с просьбой выстроить сбалансированную справедливую систему, в которой все участники защищены и имеют возможность получить необходимую информацию.

Суть обращений сводится к тому, что каждая из сторон должна нести ответственность за свои действия (или бездействия)

32 Главари организованных преступных группировок с большим интересом участвуют в их махинациях, так как хакеры готовы отдавать до 50% украденных денег.

33 Вступила в действие с 1 января 2014 г.

в пределах, не превышающих ее физические возможности, а также не должна допускать неотвратимого и безнаказанного причинения ущерба другой стороне.

В связи с этим было бы целесообразно:

- регулятору установить минимальный набор средств защиты, который банк должен обеспечивать клиенту. Этот набор определяется исходя из соображения, что при условии строгого соблюдения клиентом всех правил, установленных банком, риск потерь при проведении операции в обычных условиях не превышает допустимой величины;

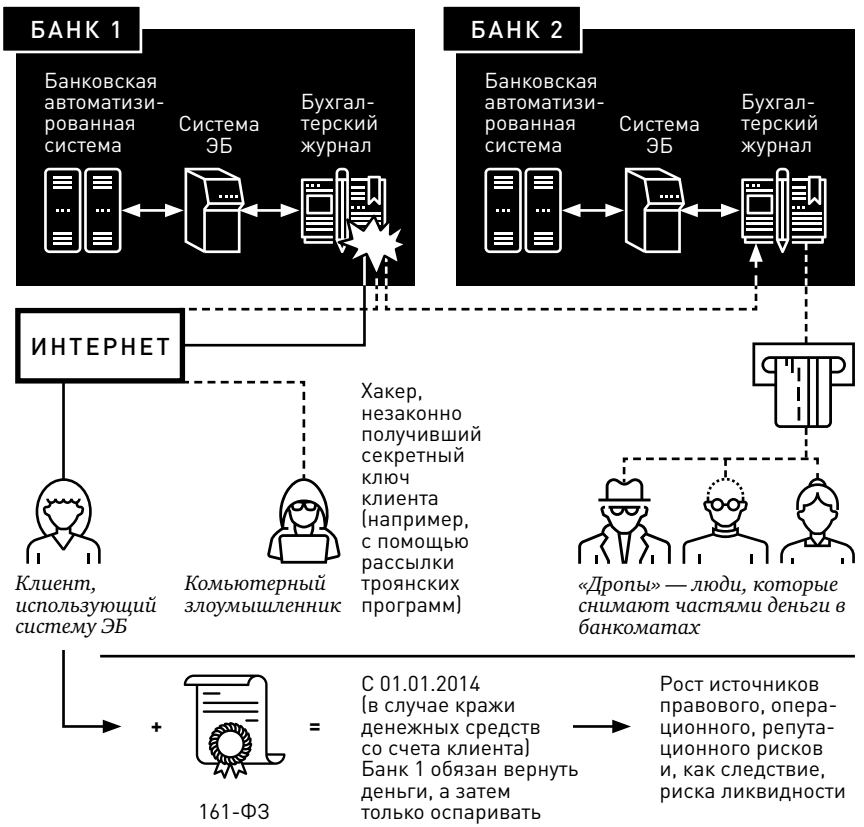

Рис. 4. Дополнительные источники банковских рисков в условиях применения СЭБ

- регулятору контролировать предоставление банками минимального набора средств защиты для клиентов;
- обязать банки, по желанию клиента, предоставлять ему дополнительные средства защиты (например, ограничения на суммы, виды операций, режимы и каналы проведения, использование дополнительного подтверждения транзакции и т. п.);
- обязать банки предоставлять клиенту полную и изложенную в доступном для понимания обычным пользователем виде информацию о рисках, основных и дополнительных средствах защиты, правилах использования средств защиты и оборудования, применяемого при проведении операции, — клиент должен четко понимать риски, знать, что он может делать (или не может), и письменно подтвердить, что ознакомлен с правилами проведения транзакций и осознает принимаемые на себя риски.

Перенос рисков на кредитные организации означает, что цены на оказание услуг вырастут (риски неизбежно закладываются в стоимость банковского продукта). Добросовестные держатели банковских карт, которые соблюдают элементарные правила безопасности, будут вынуждены переплачивать за тех клиентов, которые пишут свой PIN-код на карте.

Напомним, что коммерческие банки, работая в условиях жесткой конкуренции, не заинтересованы расходовать на обеспечение информационной безопасности средств больше, чем конкуренты. Информационная безопасность всегда связана с затратами для кредитных организаций, неудобствами для банковского персонала и клиентов. Что касается клиентов, то они обращают больше внимания на удобство банковских услуг, чем на их безопасность.

Поэтому кредитным организациям нужен разумный компромисс, который строится на нескольких базовых принципах организации информационной безопасности:

- стоимость защиты не должна превышать стоимости защищаемых информационных ресурсов;
- банк и клиент должны выйти на такой уровень защиты транзакций, когда защита еще удобна и приемлема по стоимости клиенту, а злоумышленнику уже не выгодно совершать преступление из-за высоких расходов на преодоление защиты.

1.3. Актуальные направления регулирования в условиях электронного банкинга

Наряду с очевидными преимуществами СЭБ принесли в банковский бизнес дополнительные риски. А если быть точнее, то количество типичных банковских рисков[34] осталось прежним, а вот их техническая составляющая значительно возросла.

Непрерывность выполнения банковских операций стала во многом зависеть:

- от различных сбоев в аппаратно-программном обеспечении (АПО) СЭБ;
- качества и надежности каналов связи;
- наличия резервных источников электропитания;
- качества архивации данных об операциях с использованием СЭБ;
- недостатков в обеспечении информационной безопасности конфиденциальных сведений.

Однако необходимо хорошо понимать, что, применяя современные технологии и средства, мы можем осуществить те или иные процедуры удобнее, быстрее и в гораздо больших объемах, но при этом не надо рассчитывать на чудеса — за все надо платить. И если регулирование в области ДБО (включая услуги ЭБ) будет отставать от появления и распространения новых источников типичных банковских рисков, то «удобнее, быстрее и в больших объемах» в целом будет дороже. В первую очередь возрастают затраты на обеспечение безопасности данного способа оказания банковских услуг, так как кредитные организации будут вынуждены учитывать не только внутрибанковские риски, но и риски, возникающие на стороне клиента и различных провайдеров (например, интернет-провайдеры в случае интернет-банкинга, сотовые операторы в случае мобильного банкинга)[35].

34 Перечень типичных банковских рисков приведен в Письме Банка России от 23 июня 2004 г. № 70-Т «О типичных банковских рисках».

35 Следует отметить, что риски, возникающие на стороне различных провайдеров услуг и сотовых операторов, контролировать сотрудникам кредитных организаций весьма затруднительно (а в ряде случаев — невозможно).

По мнению авторов, на сегодняшний день есть четыре причины, по которым применение СЭБ нуждается в дополнительном регулировании:

1) расширение профиля операционного риска в условиях ЭБ;
2) значительный рост числа киберпреступлений в финансовой сфере (включая хищения денежных средств в СЭБ);
3) использование СЭБ в схемах, направленных на легализацию преступных доходов (или, другими словами, отмывание денег);
4) недостаточная подготовка сотрудников коммерческих банков по вопросам обеспечения информационной безопасности и управления сопутствующими рисками в условиях ЭБ.

Причиной повышенного внимания к операционному риску стал выход соглашения Базельского комитета по банковскому надзору «Международная конвергенция изменения капитала и стандартов капитала: новые подходы» — Basel II.

Соглашение Basel II является одним из наиболее актуальных нормативных актов, регулирующих банковский сектор. Оно предъявляет требования к минимальному размеру банковского капитала, на основании которых кредитные организации обязаны оценивать операционные, рыночные и кредитные риски, а также резервировать капитал на их покрытие.

Basel II трактует операционный риск как риск убытков, возникающий в результате неадекватных или ошибочных внутренних процессов, действий сотрудников и систем или в результате внешних событий.

В качестве возможных проявлений операционного риска можно выделить следующие типы событий:

- внешние воздействия (наводнения, пожары, аварии и т. п.);
- внутренние и внешние мошенничества;
- ошибки персонала;
- сбои в реализации бизнес-процессов и обслуживании клиентов;
- физический ущерб активам;
- сбои информационных систем;
- нарушение процессов обработки и хранения данных.

Требования, предъявляемые документами Basel II, были дополнены в документах Basel III, в том числе и в отношении операционного риска.

Отметим, что Базельский комитет по банковскому надзору рекомендует привлекать к процессу управления рисками, возникающими при внедрении в кредитных организациях СЭБ, не только риск-подразделения, но и совет директоров, высшее руководство банка, а также топ-менеджеров банка.

Операционный риск является одним из основных типичных банковских рисков, на который в большей степени оказывают влияние СЭБ.

Он определяется как вероятность образования убытков и (или) неполучение прибыли вследствие сбоев в выполнении каждодневных, рутинных банковских операций. Применительно к ЭБ выделяются три главные зоны операционного риска:

1) функционирование системы безопасности;
2) привлечение сторонних организаций к предоставлению некоторых видов электронных банковских услуг (аутсорсинг);
3) освоение новых технологий сотрудниками банка.

В первом случае речь идет о том, что возможны нарушения в процессах электронного хранения, передачи и обработки информации (искажение, уничтожение, перехват данных или злоупотребление ими в результате технических неполадок, действий хакеров, ошибок или мошенничества персонала и клиентов) и отказы в функционировании банковских информационных систем (возникновение перегрузок из-за недостаточной мощности аппаратно-программного обеспечения и целенаправленных DoS-атак[36] на web-серверы банка).

Вторая потенциально подверженная операционному риску сфера становится в последнее время весьма значимой. Предоставление банковских услуг в области информационных технологий

36 DoS-атака (от англ. Denial of Service — отказ в обслуживании) и DDoS-атака (от англ. Distributed Denial of Service — распределенный отказ в обслуживании) — это разновидности атак на вычислительную систему. Цель этих атак — довести систему до отказа, то есть создание таких условий, при которых легитимные (правомерные) пользователи системы не могут получить доступ к предоставляемым системой ресурсам либо этот доступ затруднен.

посредством специализированных фирм (в первую очередь банки сотрудничают с компаниями по разработке прикладных программ) позволяет сократить инвестиционный бюджет и избежать найма дорогостоящих специалистов, что особенно важно для небольших финансовых учреждений. В то же время банки оказываются в определенной степени зависимыми от подобных партнеров, а общий уровень банковского обслуживания начинает определяться результатами работы нескольких, нередко никак не связанных между собой компаний, сотрудники которых могут и не обладать достаточными знаниями о специфике банковского дела.

Наконец, ускорение процесса модернизации информационных систем повышает требования к адаптационным способностям персонала банков и увеличивает опасность возникновения трудностей при переходе ко все более сложным интегрированным электронным решениям. Довольно часто внедрение более «умной» и производительной технологии оборачивается для работников и клиентов банков значительными проблемами[37].

Смысл управления операционным риском заключается в прогнозе периодичности различных сбоев и нарушений непрерывности функционирования аппаратно-программного обеспечения СЭБ и оценке величины вероятных убытков. Отметим, что у потерь есть и положительная сторона — они вскрывают слабые места и открывают новые возможности. Поэтому самая большая ошибка — сокрытие нежелательного инцидента. Даже после устранения рисковой ситуации или последствий неблагоприятного события нельзя оставлять происшедшее в тайне, гораздо лучше использовать инцидент в качестве наглядного урока для других сотрудников.

Формы проявления операционного риска в условиях ЭБ могут быть самыми разнообразными. Однако все они вызваны, как правило, несоответствием определенных процедур требованиям законодательства, несоразмерностью технических возможностей СЭБ и объема бизнеса, техническими сбоями и отказами оборудования, непреднамеренными или умышленными действиями персонала

37 В основном это связано с обучением персонала и совершенствованием методик проведения проверок специалистами риск-подразделений и служб внутреннего контроля.

и внешних субъектов, что отвечает классическому определению операционного риска.

Минимизировать операционный риск в условиях ЭБ можно с помощью общепринятых стратегий:

- принятие риска (отказ от превентивных мероприятий, воздействие на источники риска, самострахование (в том числе через кэптивные страховые компании), диверсификация активов и т. д.);
- полная или частичная передача риска (страхование, хеджирование, синдицирование и т. п.);
- избежание риска (отказ от применения данной системы, профилактика как устранение источников риска и проч.).

Следующая проблема связана с возрастанием активности киберпреступников, чьи усилия направлены на хищение денежных средств клиентов банков, использующих для выполнения своих операций СЭБ.

Киберпреступления ежегодно наносят ущерб мировой экономике в размере 445 млрд долл., говорится в отчете Центра стратегических и международных исследований (CSIS).

В 2013 г. из-за киберпреступлений пострадали как минимум 40 млн американцев, а также одна неназванная нефтяная компания, чьи данные по разведке месторождений попали к хакерам. США, Китай, Япония и Германия ежегодно теряют около 200 млрд долл. Потери, связанные с личными данными граждан, оцениваются в рекордные 150 млрд долл.[38]

По статистике компании Group-IB, специализирующейся на расследовании компьютерных преступлений, объем российского рынка киберпреступности в 2013 г. составил около 2,44 млрд долл.[39]

Компьютерные злоумышленники сегодня совсем не похожи на тинейджеров, получивших первоначальные знания с хакерских web-сайтов, а представляют собой специалистов с достаточно

38 См. подробнее: «Мировая экономика недополучает $445 млрд ежегодно из-за киберпреступлений» // vedomosti.ru. 9 июня 2014 г.

39 См. подробнее: «Доходы хакеров снижаются» // vedomosti.ru. 15 октября 2014 г.

высокой подготовкой в области информационных технологий и в финансовых вопросах. Причем большинство из них действуют в составе организованных преступных групп. Сегодня доходы от компьютерных преступлений значительно превышают доходы, получаемые от продажи оружия и наркотиков[40].

Очевидно, что в будущем угрозы не станут проще. Уже сегодня многие атаки — это комбинации различных методик. Использование только традиционных систем, таких как сигнатурные антивирусы, не дает возможности адекватно защищаться от современных типов атак. Кредитные организации, которые защищаются только от известных угроз, всегда рискуют, поскольку атакующие продолжают выдумывать и создавать новые техники атак.

Следующая проблема, связанная с применением СЭБ, заключается в активном привлечении данных систем к процессу легализации преступных доходов. В последнее время отмывание денег стало одной из основных международных проблем, к решению которой привлечены ведущие страны мира.

Процедура отмывания денег имеет решающее значение для функционирования практически всех форм транснациональной и организованной преступности. Различные меры экономического характера, призванные исключить или ограничить возможность использования преступниками полученных незаконными путями доходов, представляют собой важнейший и действенный компонент программ по борьбе с преступностью.

Приведем лишь некоторые факторы, способствующие отмыванию денег:

- высокая доля неофициальных доходов населения и бизнеса (существование параллельной экономики и (или)«черного рынка»);
- несовершенство механизмов контроля и мониторинга за деятельностью кредитных организаций;

40 Такое мнение высказывали многие докладчики в своих выступлениях на VI Уральском форуме «Информационная безопасность банков», который проходил в феврале 2014 г. в Республике Башкортостан. Как отмечают ведущие эксперты в области информационной безопасности, данный форум является одним из самых авторитетных мероприятий по вопросам обеспечения информационной безопасности в банках в России.

- несоблюдение международных стандартов регулирования финансовой деятельности, разработанных специализированными международными организациями;
- распространение коррупции в различных органах власти;
- законодательное закрепление тайны финансовых операций;
- широкое использование предприятиями и банками операций с вовлечением офшорных компаний и др.

Как правило, в процесс отмывания денег включается целый ряд операций, направленных на сокрытие источника финансовых активов, но все они входят в одну из трех составляющих (стадий) обобщенной модели отмывания денег: размещение (placement), расслоение (layering) или интеграцию (integration). Указанные стадии могут осуществляться одновременно или частично накладываться друг на друга в зависимости от выбранного механизма легализации и от требований, предъявляемых преступной организацией.

На стадии размещения необходимо изменить форму денежных средств с целью сокрытия их нелегального происхождения. Например, поступления от незаконной торговли наркотиками чаще всего представляют собой мелкие купюры. Конвертирование их в более крупные купюры, чеки или иные финансовые документы часто производится с помощью предприятий, имеющих дело с большими суммами наличных денег (рестораны, гостиницы, казино, мойки машин) и используемых в качестве прикрытия.

На стадии расслоения лица, отмывающие деньги, стараются еще больше скрыть следы, по которым их могут обнаружить. Для этого одни сложные финансовые сделки наслаиваются на другие. Например, для отмывания больших денежных сумм создаются фиктивные компании в странах, отличающихся строгими законами о банковской тайне или слабыми механизмами обеспечения соблюдения законодательных положений, касающихся отмывания денег. Затем «грязные» деньги переводятся из одной фиктивной компании в другую до тех пор, пока не приобретут видимость законно полученных средств.

На этой стадии активно используются СЭБ (рис. 5).

На стадии интеграции преступник пытается трансформировать денежные доходы, полученные от противозаконной деятельности, в средства, имеющие внешне легальное происхождение (деньги

обычно вкладываются в бизнес, недвижимость, покупку драгоценностей и др.).

Поскольку процесс отмывания денег в определенной степени полагается на существующие финансовые системы и операции, имеющиеся у преступника, выбор конкретных механизмов ограничивается лишь его изобретательностью. Деньги отмываются через валютные и фондовые биржи, торговцев золотом, казино, компании по продаже автомобилей, страховые и торговые компании. Частные и офшорные банки, подставные корпорации, зоны свободной торговли, электронные системы и торгово-финансовые учреждения — все эти структуры могут скрывать незаконную деятельность.

Далее приведем наиболее распространенные негативные последствия отмывания денег:

Рис. 5. Обобщенная схема отмывания денег с использованием СЭБ

1. Бесконтрольное отмывание денег способно нанести серьезный *удар по репутации банков* страны, негативно влиять на курсы валют и процентные ставки вследствие высокой интеграции фондовых рынков. Эти деньги могут поступать в глобальные финансовые системы и подрывать экономику и валюту отдельных стран. Проведение банковских операций через Интернет позволило значительно сократить время на осуществление различных платежей.
2. *Подрыв целостности финансовых рынков*. Кредитные организации, полагающиеся на доходы от преступных деяний, сталкиваются с дополнительными трудностями.
   Например, крупные суммы отмытых денег могут поступить в банк и затем внезапно бесследно исчезнуть через электронные переводы в ответ на такие нерыночные факторы, как операции правоохранительных органов.
3. *Утрата контроля над экономической политикой*. В некоторых странах с формирующейся рыночной экономикой незаконные доходы могут намного превосходить государственные бюджеты, что приводит к утрате правительственного контроля над экономической политикой. В ряде случаев огромная база активов, накопленная за счет отмытых денег, может использоваться для спекулятивной скупки рынков или даже целой экономики небольшой страны.
4. *Экономические деформации и нестабильность*. Лица, отмывающие деньги, заинтересованы не столько в извлечении прибыли, сколько в защите доходов. Они направляют свои средства в области, не обязательно приносящие экономическую выгоду той стране, в которой они размещены.
5. *Потеря доходов*. Отмывание денег снижает налоговые доходы правительства и тем самым наносит косвенный ущерб честным налогоплательщикам (затрудняется государственный сбор налогов). Данная потеря доходов означает более высокие ставки налогообложения по сравнению с нормальной ситуацией, при которой преступные доходы были бы законными и облагались налогами.
6. *Риск для программ приватизации.* Отмывание денег угрожает стремлению многих стран реформировать свою

экономику путем приватизации. Преступные организации располагают финансовыми средствами, позволяющими приобретать по более высоким ценам предприятия, прежде находившиеся в государственной собственности.

7. *Социальные издержки*. Отмывание денег ведет к росту государственных расходов на правоохранительные органы (создание специализированных подразделений) и здравоохранение (например, лечение наркотической зависимости) для преодоления возникающих серьезных последствий.

В целом, отмывание денег ставит перед мировым сообществом сложную задачу, постоянно приобретающую новые формы. Характер процессов требует разработки глобальных стандартов и международного сотрудничества для уменьшения возможности преступников осуществлять свою деятельность.

Регулирующие органы рекомендуют банкам эффективнее использовать все ресурсы для выявления сомнительных операций, направленных на отмывание денег.

Меры по предотвращению отмывания денег предпринимаются банками не только в соответствии с требованиями законодательства, но и в собственных интересах.

В рамках проведения процедур по идентификации клиентов кредитным организациям следует:

- разработать и внедрить комплексные процедуры, связанные с открытием счетов, установлением кредитных и других деловых взаимоотношений, а также совершением операций с лицами, не имеющими счетов;
- иметь данные о действительной личности пользующегося его услугами клиента, в том числе о подлинном владельце счета, открытого на другое имя;
- подвергать проверке данные, удостоверяющие личность, во избежание открытия счетов для фиктивных пользователей;
- располагать данными о роде занятий или профессиональной деятельности клиента, об источниках его доходов, состояния или активов, а также о конкретном источнике денежных средств, вовлеченных в совершаемые через данный банк операции;

- знать цель, с которой открывается счет, и представлять типы операций, в которые обычно вовлечен данный клиент. При открытии счета сотрудники банка должны понимать, нужно ли отнести клиента к категории высокого риска, требующей повышенного внимания.

В рамках выполнения процедуры мониторинга кредитным организациям следует:

- иметь внутренние системы для идентификации и мониторинга вызывающих подозрения операций;
- оценивать риск исходя из конкретных видов счетов, регионов и операций;
- обращать внимание на любую операцию, превышающую установленный денежный порог депозитов при открытии счета, ежемесячные телеграфные переводы, операции с наличностью, дорожными чеками, получение кредитов и заключение сделок (включая покупку и продажу валют, опционов и драгоценных металлов) и т. п.;
- обращать внимание на усиление активности по банковским счетам, особенно тем, которые могут стать объектами сомнительных операций (офшорные и корреспондентские счета, счета небанковских финансовых институтов, политических деятелей и др.);
- установить пороговые размеры сделок и время от времени проверять их адекватность.

Отдельно следует отметить роль топ-менеджеров кредитных организаций. Они должны стремиться к постановке и практической реализации задач в области предотвращения незаконных операций и демонстрировать, что банк как субъект корпоративной культуры заботится о своей репутации не меньше, чем о прибылях, маркетинге и качестве обслуживания клиентов.

Топ-менеджерам кредитных организаций необходимо хорошо представлять, что клиенты коммерческих банков, использующие для выполнения своих операций СЭБ и занимающиеся противоправной деятельностью, могут не только нанести удар по репутации банка, но и создать для него серьезные осложнения во взаимоотношениях с регулирующими органами, вплоть до отзыва лицензии на осуществление банковских операций.

Четвертая область связана с совершенствованием профессиональной подготовки персонала банка (включая сотрудников служб внутреннего контроля кредитных организаций) по вопросам обеспечения информационной безопасности. Учитывая заметное увеличение источников банковских рисков, основу которых составляют особенности функционирования СЭБ, специалистам коммерческих банков, в чьи функции входит управление рисками, необходимо иметь не только экономическое или юридическое, но и техническое образование, позволяющее достаточно уверенно ориентироваться в особенностях функционирования различных технологий ДБО.

Ненадлежащее обеспечение информационной безопасности СЭБ (в частности, продажа населению слабозащищенных финансовых услуг) ведет к созданию предпосылок для хищения денежных средств и финансирования криминала. Существующая динамика развития современных процессов, связанная с ростом технических возможностей, способна многократно увеличить объемы финансирования криминала. Если допустить рост уровня хищений в больших объемах (соизмеримый с госсектором), это может быть серьезной угрозой экономической безопасности страны.

2. КИБЕРБЕЗОПАСНОСТЬ В УСЛОВИЯХ ПРИМЕНЕНИЯ СИСТЕМ ЭЛЕКТРОННОГО БАНКИНГА

2.1. Парадигмы построения системы кибербезопасности

В современном обществе Интернет и сотовая связь стали привычными каналами предоставления информационных услуг. В банковской сфере эти два способа связи легли в основу ЭБ, который является лидером среди технологий ДБО. СЭБ фактически переместили весь процесс взаимодействия кредитных организаций со своими клиентами в виртуальное пространство, или, другими словами, в киберпространство.

Внедрение СЭБ не только значительно сокращает операционные издержки, но и является одним из основных конкурентных преимуществ среди кредитных организаций. В то же время, перенося свой бизнес в киберпространство, кредитные организации не освобождаются от ответственности за качество предоставления своих финансовых услуг и должны в полной мере осознавать, что сегодня компьютерные атаки кибермошенников направлены в первую очередь на СЭБ с целью кражи денег как со счетов банков, так и их клиентов.

Если рассматривать информационный контур банковской деятельности, формируемый в условиях применения СЭБ, то наиболее слабым звеном является клиент. АПО СЭБ достаточно хорошо защищено на стороне банка, а на стороне клиента все в точности наоборот. Поэтому взломать современные системы защиты, которые используют кредитные организации, намного сложнее, чем получить доступ в личный кабинет клиента.

К основным сдерживающим факторам развития ДБО можно отнести: отсутствие доверия клиентов к технологиям ДБО из-за роста компьютерных атак на СЭБ (в том числе с использованием социальной инженерии) и низкий уровень финансовой грамотности клиентов (включая недостаточную информированность о возможностях современных технологий ДБО и способах обеспечения кибербезопасности в них).

Повышение уровня финансовой грамотности населения — это задача, которая должна решаться комплексно. Во многих странах с основами кибербезопасности начинают знакомить еще в начальной школе, а в институтах этот предмет является обязательным — другого подхода в информационный век и не может быть.

Следует принимать во внимание, что уровень финансовой грамотности населения всегда будет уступать уровню и скорости развития мошеннических технологий. Поэтому разработчики АПО СЭБ изначально должны ориентироваться на «среднего» пользователя и обеспечивать максимальную защиту от внешних воздействий.

Минимизировать риски «успешного» воздействия компьютерных атак можно с помощью построения комплексной системы кибербезопасности в кредитно-финансовой сфере.

В основе такой системы безопасности может лежать одна из двух парадигм: парадигма защищенности и парадигма развития.

Парадигма защищенности предполагает, что основу обеспечения безопасности составляет борьба с опасностями (угрозами). Менталитет защищенности приводит к отождествлению безопасности с жизнедеятельностью, вследствие чего идея безопасности ставится во главу угла всей деятельности. Необходимой предпосылкой обеспечения безопасности в рамках данной парадигмы является определение угроз безопасности, на устранение которых и направляется деятельность прежде всего специальных служб[41].

Парадигма развития базируется не столько на осуществлении борьбы с опасностями, сколько на развитии собственных внутренних сил. И потому опасность представляет собой не только то, что отрицает существование объекта, а прежде всего то, что угрожает его самоутверждению.

В настоящее время наблюдается устойчивая тенденция смещения акцентов в деятельности по обеспечению безопасности с парадигмы защищенности на парадигму развития. Появилось понятие

41 Эта парадигма уходит корнями в историю России. Так, система государственной безопасности СССР и деятельность КГБ были построены на этой модели. Четко просматривается эта парадигма и в начале 90-х гг. XX в. Например, в Федеральном законе «О безопасности» (1992) безопасность определяется как состояние защищенности жизненно важных интересов личности, общества и государства от внутренних и внешних угроз.

«безопасность через развитие». Его суть заключается в том, что обеспечение безопасности все в большей степени осуществляется через развитие и все в меньшей — через защиту[42].

Система не может быть жизнеспособной, только сохраняя достигнутое, без изменений и развития, поэтому следование исключительно парадигме защищенности в действительности не укрепляет безопасность, а постепенно разрушает объект, так как он не развивает свои внутренние силы, а лишь противостоит опасностям. И наоборот — только самоутверждение, постоянное изменение без сохранения основы системы ставят под удар существование последней. Таким образом, парадигмы защищенности и развития должны не исключать, а дополнять друг друга. Именно такого подхода необходимо придерживаться при построении комплексной системы кибербезопасности в кредитно-финансовой сфере.

Очевидно, что большая работа должна быть проведена регулятором. Как минимум, он должен обеспечить определение необходимых условий ведения банковского бизнеса в киберпространстве и разработать рекомендации по снижению рисков для кредитных организаций.

В условиях применения СЭБ в ряде случаев на стороне киберпреступников оказываются:

- стремительная скорость устаревания техники. Именно поэтому многие успешные компьютерные атаки реализовываются при запуске новых банковских сервисов (речь идет об атаках «нулевого дня» — когда атака уже реализуется, а противоядия еще не найдено; такие атаки наносят самый большой вред);
- безграничность Интернета и неадекватность нормативно-правовой базы, регулирующей информационные потоки. В связи с этим чрезвычайно сложно идентифицировать киберпреступников (особенно если они находятся на территории

42 Подтверждением этому может служить принятие ряда важнейших концептуальных документов, направленных на обеспечение разных видов безопасности Российской Федерации (в которых акценты сделаны именно на проблемах развития): «Стратегия национальной безопасности Российской Федерации» (2009), «Доктрина информационной безопасности Российской Федерации» (2000), «Стратегия развития информационного общества в Российской Федерации» (2008) и др.

офшорных государств, где действует запрет на выдачу определенной информации).

Очевидно, что в будущем угрозы не станут проще. Уже сегодня многие атаки — это комбинации различных методик. Использование только традиционных систем обеспечения информационной безопасности (ИБ), таких как сигнатурные антивирусы, не дает надежной защиты от современных типов атак. Кредитные организации, которые защищаются только от известных угроз, всегда рискуют, поскольку атакующие выдумывают и создают все новые технологии и схемы.

2.2. Методология анализа рисков недостаточного обеспечения кибербезопасности

Основными причинами повышенного внимания регулирующих органов к технологиям ДБО (включая СЭБ) являются «виртуальная» форма совершаемых банковских операций (когда каждая проводка выражается в мгновенном изменении содержания центральной базы банковских данных), снижение надежности и устойчивости кредитных организаций, а также банковской системы в целом, так как любые новые высокотехнологичные нововведения повышают и усложняют банковские риски.

В условиях применения СЭБ возникают ранее не учитываемые источники угроз, способные создать дополнительные проблемы, связанные со снижением уровня надежности банковских автоматизированных систем и с угрозами безопасности информационных ресурсов (в том числе АПО, находящегося на стороне провайдеров). Для перехода на новый качественный уровень управления рисками, возникающими в условиях применения СЭБ, не следует ограничиваться только выявлением причин и определением размеров возможных финансовых потерь. Необходимо шире рассматривать проблемы, связанные с использованием СЭБ, выходить за рамки привычных методов учета рисков. В качестве итоговых оценок следует рассматривать риски, связанные с системными характеристиками и показателями (риски системного уровня): возможность продолжения функционирования

банка и выполнение им функций финансового посредника в неизменном или измененном масштабе, временный запрет на выполнение определенного вида банковских операций, введение временной администрации, отзыв лицензии на банковскую деятельность.

Иерархию рисков можно представлять в виде трех уровней: системный банковский риск (СБР), типичный банковский риск (ТБР) и элементарный банковский риск (ЭБР). Количество источников ЭБР для каждого из ТБР различно, так как они имеют разную природу. Каждый ЭБР отражает некий выявляемый факт, каждый ТБР — какое-либо событие в банке, образуемое совокупностью фактов и связанное с финансовыми потерями, а СБР описывает некоторую итоговую рисковую ситуацию (рис. 6).

Поиск источников ЭБР и дальнейшее выстраивание причинно-следственных связей представляет наиболее сложную задачу для адекватной оценки. Поэтому специалисты, входящие в риск-подразделения и службы внутреннего контроля, должны хорошо представлять особенности функционирования СЭБ и возможные последствия

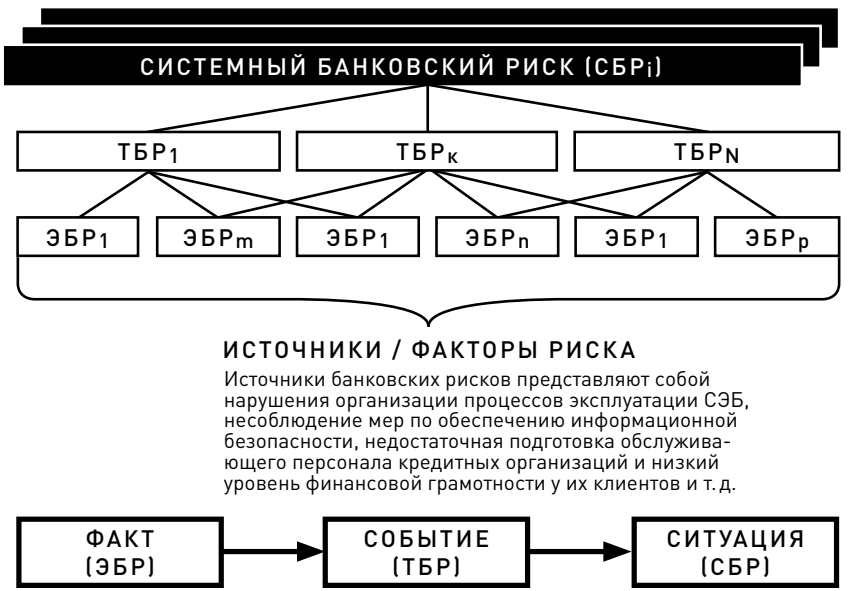

Рис. 6. Иерархическая схема для выявления, анализа и мониторинга банковских рисков

проявления сопутствующих рисков (включая воздействие компьютерных атак на информационные ресурсы банка). Очевидно, что реализованные компьютерные атаки значительно расширяют профили типичных банковских рисков[43].

Примерная схема анализа возможных последствий нарушения кибербезопасности в условиях ДБО на деятельность кредитных организаций представлена на рис. 7. Например, в случае реализованной компьютерной атаки на системы ДБО банка вполне вероятно, что многие клиенты откажутся от услуг данной кредитной организации. Следовательно, сумма остатков на их счетах и будет возможной суммой единовременного снятия средств клиентами (риск ликвидности). Далее такие клиенты могут быстро распространить отрицательные отзывы о банке, и вполне вероятно, что их знакомые, которые также являются клиентами банка, могут последовать их примеру и закрыть свои счета (репутационный риск и возрастание риска ликвидности).

Добавим, что некоторые клиенты могут обратиться в суды за возмещением не только похищенной суммы, но и суммы упущенной выгоды (например, в случае временной неплатежеспособности при взаимодействии с выгодным клиентом, деловым партнером и т. п.). Судебные издержки, негативная информация об этих судебных решениях в СМИ могут серьезно повлиять на репутацию организации (правовой и репутационный риски).

Для многих кредитных организаций существует управленческая проблема: несоразмерность мер по информационной безопасности (включая обеспечение кибербезопасности) основным целям и общему уровню принимаемых рисков. Это говорит о нехватке качественного управления рисками и о том, что кибербезопасность обеспечивается постфактум, по уже совершившемуся событию, а должна носить превентивный характер и работать на опережение.

К основным причинам появления рисков недостаточного обеспечения кибербезопасности в условиях применения СЭБ можно отнести:

- наличие множественных уязвимостей АПО СЭБ, отсутствие должной реализации процедур контроля за соответствием СЭБ требованиям информационной безопасности;

43 Перечень типичных банковских рисков приведен в Письме Банка России от 23.06.2004 № 70-Т «О типичных банковских рисках».

Рис. 7. Возможные последствия реализации компьютерных атак

- низкую эффективность мероприятий, проводимых кредитными организациями по внедрению и использованию документов Банка России в области стандартизации обеспечения информационной безопасности;
- отсутствие правовой основы по распространению нормативных требований к обеспечению защиты информации, устанавливаемых Банком России, на все процессы деятельности кредитных организаций;
- отсутствие должной достоверности контроля выполнения технических требований, как правило, реализуемого в форме самооценки.

Для минимизации последствий проявления рисков недостаточного обеспечения кибербезопасности Банк России выделяет следующие ключевые направления деятельности:

- проработка вопроса о законодательном закреплении права Банка России, совместно с ФСТЭК России и ФСБ России, на нормативное регулирование и контроль всех вопросов, связанных с обеспечением информационной безопасности в кредитных организациях, в том числе вопросов защиты информации, отнесенной к категории банковской тайны;
- законодательное закрепление основ деятельности по реализации системы противодействия хищениям денежных средств (системы антифрод) и создание такой системы на базе FinCERT Банка России[44];
- обеспечение скорейшей разработки и ввода в действие национальных стандартов, регулирующих технические вопросы обеспечения информационной безопасности в организациях кредитно-финансовой сферы;
- создание совместно с ФСБ России и ФСТЭК России системы для подтверждения соответствия обеспечения информационной безопасности кредитно-финансовых организаций требованиям национальных стандартов;

44 Другое название — Центр мониторинга и реагирования на компьютерные атаки в кредитно-финансовой сфере. Создан в июне 2015 г. в составе Главного управления безопасности и защиты информации Банка России.

- пересмотр технологических требований, связанных с осуществлением переводов денежных средств, внедрение безопасных технологий, в том числе для участников платежной системы Банка России;
- пересмотр технологии контроля со стороны Банка России за соблюдением участниками платежной системы Банка России требований к обеспечению информационной безопасности;
- реализация системы надзорных мер, учитывающей результаты контроля информационной безопасности в рамках системы подтверждения соответствия национальным стандартам.

В ближайшем будущем количество физических банковских офисов в России будет постепенно уменьшаться из-за развития технологий ДБО. Наличие собственного кабинета в киберпространстве станет таким же распространенным явлением, как сегодня наличие мобильного телефона.

Активное использование в банковском бизнесе СЭБ создает не только новые общие возможности, но и общие уязвимости, формируя при этом общую ответственность. Создание системы кибербезопасности и соблюдение культуры кибербезопасности всеми участниками информационного обмена в условиях применения СЭБ является залогом доверия клиентов не только к конкретной кредитной организации, но и ко всей банковской системе в целом.

2.3. Информационное общество и кибербезопасность

Средства информационного обмена постоянно развиваются и совершенствуются, благодаря чему наш мир пронизывают все более тесные взаимосвязи. Информатизация общества берет начало во второй половине XX в., и уже к началу XXI в. были охвачены практически все отрасли человеческого бытия. За первые 10 лет нового тысячелетия численность «населения» киберпространства возросла с 350 млн до 2 млрд. При этом Интернет продолжает и дальше быстро развиваться. Судя по имеющимся данным, в 2014 г. число пользователей

Интернета по сравнению с 2013 г. увеличилось на 6,6% и составило свыше 3 млрд человек, без подключения оставались 4,3 млрд человек, из которых 90% проживают в развивающихся странах, а за пять лет (с 2009 по 2014 г.) число интернет-пользователей возросло вдвое. Таким образом, в связи с глобализацией человечество получило доступ к растущему по экспоненте количеству передаваемой информации. На сегодня с помощью электронной почты по всему миру рассылаются более 200 млрд сообщений в день, а в 2015 г. количество сайтов в мировом Интернете превысило 1 млрд. Однако последствия такого бурного развития информационно-коммуникационных технологий (ИКТ) политологами и международной общественностью еще не осознаны.

Психологи говорят об угрозах интеллектуальной деградации личности из-за чрезмерно длительного пребывания в Сети, игромании, мании преследования, боязни (фобии) потерять свой коммуникатор, нарушений памяти (способности запоминать числа и факты). В самом деле, активному пользователю киберпространства ничего знать (запоминать) не надо, ему достаточно иметь доступ к информационно-поисковым системам и уметь ими пользоваться. Подобно тому, как постоянное использование калькуляторов буквально подавляет навыки «счета в уме», систематическое получение искомых сведений без присущих человеческому мозгу мысленных усилий (например, логических ассоциаций) истощает его, подрывает интуицию, что в целом может привести к ослаблению интеллектуального потенциала человека. Вдобавок, постоянное использование внешних приспособлений снижает уровень счастья (Международный индекс счастья — Happy Planet Index) населения. Эти проблемы, пожалуй, являются фундаментальными, возникающими вследствие развития ИКТ и Интернета вещей[45].

Решением является повышение общего уровня грамотности населения и каждого конкретного человека, в том числе и с помощью

45 Интернет вещей (англ. Internet of Things, IoT) — это концепция вычислительной сети физических объектов («вещей»), оснащенных встроенными технологиями для взаимодействия друг с другом или с внешней средой, рассматривающая организацию таких сетей, как явление, способное перестроить экономические и общественные процессы, исключающее из части действий и операций необходимость участия человека.

Интернета вещей. Ведь он уже оказывает влияние на здравоохранение, образование, экологию и общую жизнедеятельность, причем возможности дальнейших IoT-взаимодействий практически безграничны.

Согласно данным IDC, в 2015 г. производственный сектор занимал 64%-ную долю российского рынка IoT по использованию этой технологии и связанных с ней платформ. 20% рынка пришлись на межотраслевой сектор («умные города» и т. п.). Государственный и потребительский сектора занимал каждый по 8% российского рынка IoT по использованию этой технологии и связанных с ней платформ.

Что касается степени использования технологий IoT в компаниях, по итогам опроса IDC130 руководителей различных компаний:

- 59% фирм не используют технологии IoT;
- 30% компаний экспериментируют с этими технологиями;
- 9% внедрили один или два сценария;
- 4% компаний уже интегрируют несколько работающих систем с технологиями, связанными с IoT.

Отсюда следует, что в целом интерес со стороны организаций к технологиям и платформам Интернета вещей есть, но пока окончательно не сформировался[46]. Тем не менее повсеместное применение ИКТ непрерывно расширяется, и человеческая жизнь уже немыслима в отрыве от этого процесса.

Развитие виртуальных взаимоотношений между людьми и различными организациями создало и новый класс преступников, специализирующихся на преступлениях в области высоких технологий, — киберпреступников, а для борьбы с ними — киберполицейских и кибербезопасность.

Под кибербезопасностью в широком смысле понимают состояние защищенности в новой виртуальной сфере, которое достигается за счет набора средств, стратегий, принципов обеспечения безопасности, подходов к управлению рисками, действий, профессиональной подготовки, страхования и технологий, которые используются для защиты виртуальной среды, ресурсов организаций и пользователей сервисов от целенаправленного деструктивного воздействия.

46 Подробнее: http://www.comnews.ru/node/99810#ixzz42a2YxSMK

Кибербезопасность направлена на защиту компьютеров, сетей, программ и данных от случайного или преднамеренного несанкционированного доступа, изменения или уничтожения.

Инструменты хакерских атак доступны не только правительствам[47], но и агрессивным политическим группировкам и террористическим организациям. Западные страны, в том числе члены НАТО, вынуждены пересматривать свои военные доктрины.

Российские и западные организации умеют защищать деньги и информацию. Но кибертеррористам сегодня стало важнее создать хаос, а еще лучше — массовую гибель людей. Их цели — АЭС, ЖКХ, транспорт, все объекты, где сбои в информационных системах могут привести к катастрофам. Недооценка угрозы кибертерроризма напоминает недооценку фашизма между мировыми войнами.

Что касается Интернета вещей, его возможности позволят злоумышленникам удаленно управлять автомобилями, персональными медицинскими системами или заставить «умный холодильник» совершать покупки, которые не входили в планы хозяина. Вспомним атаку на Иран в 2010 г., которая остановила обогащение урана и отбросила национальную ядерную программу Ирана на два года назад. Вирус Stuxnet, запущенный на IoT-устройствах ядерного комплекса, был использован для дистанционной агрессии одного государства против другого. Поэтому IoT-инциденты не ограничиваются хищением информации и денег, а могут использоваться, чтобы нанести физический вред и значительный ущерб.

Современные теоретики, говоря о будущих кибервойнах, обычно имеют в виду не столько противоборство между компьютерами, управляющими оружием, сколько войну, цель которой состоит в захвате контроля над информационным пространством противника. Разработано множество методов и приемов для защиты IoT-пространства, и все же задачу обеспечения кибербезопасности усложняет ряд неблагоприятных факторов развития информационной инфраструктуры:

47 Атаки хакеров-одиночек — день вчерашний. Настоящие кибернетические войны теперь проводят государства. Согласно информации о взломах, наиболее развитым кибероружием обладают США, Великобритания, Россия, Китай, Индия, Иран и Северная Корея. URL: http://tadviser.ru/a/53662

- чрезмерная скорость устаревания техники;
- безграничность Интернета и неадекватность нормативно-правовой базы, регулирующей информационные потоки;
- чрезвычайная сложность (в ряде случаев невозможность) идентификации киберпреступников;
- ограниченные ресурсы обеспечения кибербезопасности.

2.4. Электронные финансы — в Интернет вещей

Аналитики прогнозируют стремительный рост рынка электронных платежей, исходя из тенденции. В 2015 г. по сравнению с 2014 г. количество банковских карт, мобильных телефонов и IoT-устройств с бесконтактной технологией возросло на 121%, было выпущено на 50% больше бесконтактных карт и устройств. В России количество таких карт и устройств с IV квартала 2014 по 2015 г. увеличилось на 44%. В Европе уже свыше 10 стран могут «похвастаться» тем, что в каждой из них функционируют более 5 млн бесконтактных карт или устройств[48].

Рост объема информации предопределил развитие инфраструктуры хранения данных в последние десять лет, в том числе и в финансовой сфере. На протяжении пяти веков в основе работы розничных банков лежал оборот наличных денег. За полвека эта модель переместилась в сторону электронного оборота, который к концу первой декады нового тысячелетия достиг зрелости, работает и уже прошел проверку. Для банков сейчас самое время сконцентрироваться на электронных платформах.

«Носимый» банкинг (для так называемых Wearable Technology — очков, часов, браслетов и прочих гаджетов) сейчас вызывает немало надежд и восторга. Например, MasterCard развивает программу, которая позволит превратить любой аксессуар, гаджет или предмет бытовой техники в устройство с функцией оплаты. Специалисты компании на техновыставке Consumer Electronics Show (CES)

48 См. подробнее: http://www.content-review.com/articles/34392/

представили сразу два таких решения. Одно из них — это приложение Groceries для покупок прямо на дисплее холодильника, которое связывает покупателей с ведущими продуктовыми магазинами. Кроме того, MasterCard объявила о партнерстве с компанией Coin, которое предполагает встраивание платежных технологий MasterCard в фитнес-браслеты, смарт-часы и другие носимые устройства[49].

По данным J'son & Partners Consulting, на конец 2015 г. общее число IoT-устройств в России составило более 16 млн штук, включая устройства, соединенные посредством сотовых, фиксированных, Wi-Fi сетей и других технологий ближнего действия. Это составляет 0,35% от общего числа подключенных устройств в мире — 4,6 млрд штук (оценки компании Ericsson). К 2018 г. российский рынок IoT достигнет уровня в 32 млн подключенных устройств[50]. Ожидается, что мировой IoT-рынок вырастет с $42,2 млрд в 2013 г. до $98,8 млрд в 2018 г. Таким образом, среднегодовой темп роста (CAGR) за 5 лет составит 18,6%. К 2020 г., по прогнозу аналитиков, доля подключенных устройств в жилых и коммерческих зданиях вырастет до 81%[51].

Отождествляя финансовые отношения с IoT-технологиями, не стоит забывать и о распространении хищений денежных средств, сбоях в работе СЭБ и, как следствие, снижении доверия к использованию IoT-услуг кредитно-финансовых организаций (возрастании операционных и репутационных рисков). В России уже сегодня существует следующая схема кражи: чтобы снять деньги со счета, достаточно приложить устройство беспроводного терминала к карману или сумке, считыватели бесконтактных карт работают на расстоянии до 20 см, достать их проблем не составляет. А ведь, как известно, мошенники находятся в местах массового скопления людей. К тому же мобильные терминалы не являются редкостью, более того, считыватель этих карт можно собрать кустарным способом

49 См. подробнее: сайт banki.ru, статья «MasterCard представила решения для платежей через холодильник и фитнес-браслеты» от 22.01.2016. URL: http://www.banki.ru/news/lenta/?id=8603837

50 Источник: интернет-портал и аналитическое агентство TAdviser. URL: http://tadviser.ru/a/302411

51 Источник: интернет-портал и аналитическое агентство TAdviser. URL: http://tadviser.ru/a/302413

с помощью нехитрых радиокомпонентов, которые можно легко заказать онлайн, набрав в поисковике искомые слова[52].

Цифровой банк станет банком расширенного финансового обслуживания, поскольку будет учитывать транзакции человек — человек, человек — машина и даже машина — машина. Взаимодействовать можно будет со всем — от одежды до эскалаторов — с помощью чипов радиочастотной идентификации — RFID[53], встроенных повсюду. Это означает, что все будет взаимодействовать со всем, разумно и без проводов, с помощью Интернета вещей, который являет нам новый дополненный мир виртуальной реальности и вместе с тем представляет множество новых угроз как для самих устройств, так и для платформ, на которых они работают. Финансовым организациям понадобятся технологии защиты от хакерских атак и непосредственного физического взлома «девайсов». Проблема усугубляется тем, что большинство IoT-устройств создаются с применением простейших операционных систем и процессоров, которые не поддерживают сложные средства защиты, что немаловажно в том случае, когда IoT-решения направлены на снижение затрат потребителей.

Поэтому банки сегодня должны попытаться продумать, какого рода операции они будут предлагать и осуществлять в реальности, когда все устройства соединены между собой и они все могут взаимодействовать и участвовать в торговле. Вот часть вопросов, на которые необходимо ответить:

1. Каким образом будут предоставляться IoT-услуги?
2. Кто будет выступать провайдерами?
3. Как будет обеспечиваться безопасность и аутентификация?
4. Когда банки начнут вводить продукты и услуги, использующие новые возможности?

52 Источник: телепередача «Вести. Дежурная часть» от 12 февраля 2016 г., сюжет «Новый вид карманных краж: в зоне риска пассажиры общественного транспорта», URL: http://www.vesti.ru/videos/show/vid/670703/cid/1741/

53 Radio Frequency Identification (RFID) — «радиочастотная идентификация», способ автоматической идентификации объектов, когда посредством радиосигналов считываются или записываются данные. Некоторые энтузиасты тестируют применение RFID-чипов в реальной обстановке: для оплаты покупок и переводов между счетами клиента. Вдобавок вживляемый в руку биочип позволяет открывать дверные замки и запускать офисное оборудование.

Самые очевидные угрозы, вызванные тем, что устройства общаются посредством сети Интернет, — это воровство данных, получение доступа к «умным» устройствам и блокирование устройств (например, с помощью DDoS-атаки). Оптимизация финансовых отношений на основе внедрения IoT-технологий будет осуществляться посредством СЭБ. И самый большой потенциал повышения безопасности СЭБ с помощью технологий — в использовании биометрических данных клиентов. Наиболее очевидный вариант — отпечатки пальцев или система распознавания лиц для удостоверения личности пользователя. Применение биометрических данных имеет два преимущества. Прежде всего оно не позволит преступникам подобрать пароль или PIN-код, воспользоваться украденной картой или скопировать ее. Следующее преимущество — это ускорение и улучшение обслуживания клиентов. Нам нужно помнить и вводить так много личных номеров и паролей, что распознавание биометрических данных кажется весьма привлекательной перспективой. Затраты на встраивание функции распознавания биометрических данных в СЭБ обязательно окупятся результативностью. Принимая во внимание широкое использование технологии распознавания отпечатков пальцев в IoT-устройствах и мобильных телефонах, признание клиентами новшества не будет проблемой. В зависимости от качества АПО, используемого в технологиях распознавания биометрических данных, угроза кражи денег и конфиденциальной информации у клиентов организаций кредитно-финансовой сферы может быть сведена к минимуму.

Хотя само биометрическое оборудование не дешево, модификация программного обеспечения и соответствующего процесса идентификации потребует от банков значительных инвестиций. По этой причине сегодня только две страны — Колумбия и Япония — внедрили в банкоматы систему распознавания биометрических данных.

Распознавание биометрических данных очень привлекательно для растущих рынков, особенно в бедных, менее развитых странах, где банкоматы появились сравнительно недавно. Расширение их применения тормозится распространением PIN-кодов и необходимостью хранения карт и PIN-кодов отдельно. Это относится в первую очередь к бедным регионам, где людям непросто запомнить PIN-коды, а их использование небезопасно.

Более интересна «биометрическая интеграция» с IoT-технологиями (распознавание лиц при приближении), которая позволит узнавать клиента и показывать подготовленные специально для него послания, основанные на портфеле продуктов этого клиента или его недавних финансовых операциях. Цифровые видеостены[54] уже используют технологию распознавания лиц и могут «сказать», какого пола клиент, стар он или молод, расстроен или доволен.

Для создания позитивного опыта самообслуживания банкам будет очень важно найти правильное сочетание персонификации, отклика на нужды отдельно взятого клиента, правил конфиденциальности и безопасности для того, чтобы сделать использование цифровых технологий более личным и человечным.

2.5. Кибербезопасность в условиях развития Интернета вещей и электронного банкинга

Проблема Интернета вещей в том, что IoT-системы создают новые точки доступа для хакеров. Входом в систему может стать сетевой принтер, предоставляющий хакерам маршрут доступа к компьютерам в сети финансовой организации, или мобильное устройство, которое имеет доступ к системе радиосвязи высокотехнологичного автомобиля. Хакеры не сидят без дела, они постоянно находят слабые места, а специалисты по безопасности ищут способы борьбы. Стоит признать, что киберпреступники всегда на шаг впереди, они нападают внезапно и могут использовать нешаблонные способы атак. В связи с этим производители средств защиты вынуждены постоянно обороняться, то есть искать защиту в условиях жесткого лимита времени, поскольку самый большой вред исходит именно от атак «нулевого дня» (когда «противоядие» еще не найдено). В некоторых случаях

54 Видеостена — компьютеризированная система наглядной информации, представляющей собой конструкцию из нескольких панелей (экранов) для демонстрации рекламы, установленную в общественных местах — метро, аэропортах, магазинах и т. д.

защищаться приходится от того, о чем есть крайне поверхностное представление: отсутствуют данные о количестве подобных атак, которые уже направлялись на банки, о том, каким способом непосредственно производилось заражение программного обеспечения, как действовали злоумышленники в определенных ситуациях и т. п.

При отсутствии взаимодействия противостояние осуществляется практически вслепую. Это все равно, что вести войну, не имея сведений о численности и дислокации врага, используемом им вооружении и источниках подкреплений.

Кибербезопасность организаций кредитно-финансовой сферы должна базироваться на готовности подразделений безопасности противостоять новым кибератакам, понимании всего спектра угроз в отношении организации в целом и распределения приоритетов между активами организации и их защитой[55].

К факторам, повышающим уровень воздействия кибератак, относятся:

- отсутствие отлаженного правового и организационно-технического обеспечения законных интересов граждан, государства и общества в области кибербезопасности (в том числе в условиях применения СЭБ);
- высокая латентность[56] киберпреступлений и недостаточное осознание органами государственной власти на федеральном и особенно региональном уровнях возможных политических, экономических, моральных и юридических последствий компьютерных преступлений;
- слабая координация действий правоохранительных органов, суда и прокуратуры в борьбе с киберпреступлениями, неподготовленность их кадрового состава к эффективному

55 Результаты мониторинга кибербезопасности кредитной организации рекомендовано оценивать не реже, чем раз в квартал. Причина такого решения — увеличение числа кибератак на системы финансовых организаций и рост финансовых потерь клиентов из-за хакерских программ (Письмо Банка России от 24.03.2014 № 49-Т «О рекомендациях по организации применения средств защиты от вредоносного кода при осуществлении банковской деятельности»).

56 Латентная киберпреступность представляет собой реальную, но скрытую или незарегистрированную часть фактически совершенных преступлений. Латентная киберпреступность является серьезным криминогенным фактором, детерминирующим дальнейшее ее распространение.

предупреждению, выявлению и расследованию таких действий;

- несовершенство системы единого учета правонарушений, совершаемых с использованием средств информатизации;
- отсутствие у Банка России подразделений по надзору за применением IoT-технологий в ОКФС и обеспечением кибербезопасности;
- существенное отставание отечественной индустрии средств и технологий информатизации и кибербезопасности от мирового уровня;
- ограниченные возможности бюджетного финансирования научно-исследовательских, опытно-конструкторских работ по созданию правовой, организационной и технической баз кибербезопасности.

Безопасность всего пространства Интернета вещей должна задаваться на уровне создания архитектуры (тем более для организаций кредитно-финансовой сферы). Иными словами, необходимо обеспечить защиту от любых вредоносных действий еще при разработке протоколов и устройств Интернета вещей. Поэтому эффективные решения по безопасности должны быть найдены на этапе развертывания всей инфраструктуры банковских сервисов.

Учитывая тот факт, что кредитно-финансовая сфера становится одной из самых привлекательных зон интересов киберпреступников (о чем свидетельствует значительный рост числа киберпреступлений и целевых атак на банки), а также оптимизацию финансовых решений в условиях Интернета вещей, необходимо оперативно принять меры по обеспечению повышенного уровня кибербезопасности (особое внимание должно быть обращено на СЭБ). Ведь мир, где все соединено со всем и буквально все может взаимодействовать и участвовать в торговле, предоставляет огромные возможности не только для банков, но и для киберпреступников. Только за четвертый квартал 2015 г. со счетов клиентов кредитно-финансовых организаций были похищены денежные средства на сумму, превышающую 1,5 млрд руб.[57]

57 Данные Банка России. URL: http://www.banki.ru/news/lenta/?id=8686505

Пожалуй, единственный способ защитить все устройства, объединенные интернет-сетью, — это надежная защита единого центра управления Интернетом вещей.

Учитывая, что финансовый и банковский сектора наиболее восприимчивы к внедрению новейших достижений в области ИКТ, приведем три основных направления совершенствования кибербезопасности в условиях применения СЭБ и Интернета вещей (см. схему).

Перечисленные направления, по мнению авторов, представляют далеко не полный перечень мероприятий, которые необходимо выполнить в рамках обеспечения кибербезопасности в условиях применения Интернета вещей. Ведь в реальной практике каждое направление будет содержать гораздо больше задач, направленных на достижение цели. В перспективе нужно стремиться создать не только систему надзора в виртуальном пространстве, но и поднять культуру поведения в нем всех участников информационного обмена. Компании должны хорошо понимать, что за рекламой различных IoT-систем стоит их ответственность за качество предоставляемых услуг. Финансовые институты должны использовать защищенные программные продукты для IoT-систем, иметь квалифицированный обслуживающий персонал, способный оперативно и грамотно реагировать на кибератаки, а также всегда готовый прийти на помощь своим клиентам, оказавшимся в трудной ситуации.

НАПРАВЛЕНИЯ СОВЕРШЕНСТВОВАНИЯ КИБЕРБЕЗОПАСНОСТИ В УСЛОВИЯХ ПРИМЕНЕНИЯ СЭБ И ИНТЕРНЕТА ВЕЩЕЙ

	ЦЕЛЬ	ЧТО НАДО СДЕЛАТЬ РЕГУЛЯТОРУ	ЧТО ДОЛЖНЫ СДЕЛАТЬ БАНКИ
Нормативно-правовое регулирование в области кибербезопасности в условиях IoT	Повысить роль регулятора в вопросах кибербезопасности СЭБ и Интернета вещей	Создать специальный орган (отдельное подразделение в структуре Банка России), в функции которого будет входить постоянный мониторинг кибератак на банки и оперативное реагирование на них (в том числе совместно с правоохранительными органами). Для этого необходимо разработать и внедрить регламенты взаимодействия при передаче сведений о кибератаках. Подготовить и выпустить рекомендации для банков по обеспечению кибербезопасности в применении СЭБ и Интернета вещей	Организовать выполнение регламентов взаимодействия при оперативной передаче сведений о кибератаках регулятору. Выполнять рекомендации регулятора по обеспечению кибербезопасности в применении СЭБ и Интернета вещей
Надежность АПО СЭБ	Повысить надежность АПО систем ЭБ, в том числе их защищенность от кибератак	Установить требования по надежности и защищенности АПО СЭБ и организовать взаимодействие по данному вопросу с разработчиками СЭБ и провайдерами услуг	Внедрять АПО СЭБ, соответствующее требованиям по надежности и защищенности. Повысить качество заключаемых договоров с разработчиками АПО СЭБ и провайдерами услуг
Финансовая грамотность населения и уровень профессиональной подготовки персонала банков в условиях применения СЭБ и Интернета вещей	Повысить уровень финансовой грамотности населения и персонала банков по вопросам обеспечения кибербезопасности в условиях применения СЭБ	Разработать и довести до банков рекомендации по повышению уровня финансовой грамотности клиентов и персонала по вопросам обеспечения кибербезопасности в условиях применения СЭБ и Интернета вещей. Разработать программу и методику проведения киберучений как для подразделений Банка России, так и для банков	Организовать доведение информации до клиентов банков (через web-сайт, смс-сообщения) о различных мошеннических схемах с использованием СЭБ. Постоянно проводить переподготовку персонала по вопросам кибербезопасности в условиях применения СЭБ и Интернета вещей

3. ПРИНЦИПЫ УПРАВЛЕНИЯ РИСКАМИ ЭЛЕКТРОННОГО БАНКИНГА[58]

«Всякого рода беспринципная деятельность приводит к банкротству».

И.В. Гете,
немецкий поэт, мыслитель и естествоиспытатель

Введение

Банковские организации предоставляют клиентам обслуживание в электронной форме и дистанционное осуществление операций уже в течение ряда лет. Перевод средств в электронной форме, включая малые платежи и управление корпоративными системами управления наличностью, равно как и общедоступные банкоматы и мониторы для управления клиентами своими счетами, стали глобальными явлениями. В то же время возросшее всемирное восприятие Интернета в качестве канала предоставления банковских услуг и обслуживания открывает банкам новые деловые возможности, а также преимущества в обслуживании их клиентам. В данном разделе Интернет определяется как все web-технологии и открытые телекоммуникационные сети, начиная с прямых модемных соединений, общедоступной World Wide Web (Всемирной паутины) и кончая частными виртуальными сетями связи.

Продолжающийся технологический прогресс и конкуренция между существующими банковскими организациями, а также появление новых участников рынка обеспечили возможности для расширения набора электронных банковских услуг, а также видов обслуживания для частных и оптовых банковских клиентов. Состав услуг включает как традиционные действия типа доступа к финансовой информации,

58 Данный раздел подготовлен на основе документа Базельского комитета по банковскому надзору «Принципы управления рисками для предоставления банковских услуг в электронной форме» (май 2001 г.).

получения ссуд и открытия депозитных счетов, так и относительно новые варианты и виды обслуживания: осуществление электронных платежей, персональные «финансовые порталы», агрегация счетов[59], а также работа на финансовых рынках и с валютой.

Несмотря на значительные достоинства технологических инноваций, быстрое развитие ЭБ привносит не только преимущества, но и риски. Банковским учреждениям важно распознавать такие риски и управлять ими пруденциальным образом. Из-за быстрых изменений в информационных технологиях никакое описание таких рисков не может считаться исчерпывающим. Тем не менее риски, с которыми сталкиваются банки, вовлеченные в ЭБ, в общем случае не являются новыми и входят в состав тех категорий, которые были определены в Основных принципах эффективного банковского надзора Базельского комитета по банковскому надзору (БКБН), выпущенных в сентябре 1997 г. В этом руководстве указаны девять категорий риска, включающие кредитный риск, страновой и трансферный риски, рыночный риск, процентный риск, риск ликвидности, операционный риск, правовой риск и репутационный риск[60]. Разработки такого рода обусловили проведение БКБН предварительного изучения в 1998 г. значимости управления рисками ЭБ и использования электронных денег[61]. В этом первоначальном исследовании продемонстрирована очевидная необходимость в проведении дополнительной работы в области управления рисками, связанными с ЭБ. Данная задача была поручена рабочей группе, сформированной в ноябре 1999 г.

59 Службы агрегации счетов позволяют клиентам получать в одном месте консолидированную информацию об их финансовых и нефинансовых счетах. Агрегатор изначально действует как агент для клиентов по предоставлению консолидированной информации о счетах клиентов по нескольким финансовым учреждениям. Клиенты предоставляют агрегатору необходимые защитные пароли или персональные идентификационные номера для получения доступа и консолидации информации о состоянии счетов, в основном это реализуется через так называемое считывание экранной информации — процесс, включающий отбор данных с web-сайтов других учреждений, зачастую без их оповещения или через контрактные отношения по прямому обмену данными финансовыми учреждениями.

60 Указанные основные принципы размещены на web-сайте Банка международных расчетов (Bank for International Settlements) www.bis.org

61 Материал «Risk Management for Electronic Banking and Electronic Money Activities» (март 1998 г.) размещен на web-сайте Банка для международных расчетов (Bank for International settlements) по адресу http://www.bis.org

и составленной из работников банковского надзора и сотрудников центральных банков, — Electronic Banking Group (EBG).

БКБН выпустил в октябре 2000 г. Отчет EBG по управлению рисками, возникающими вследствие разработок в области ЭБ, и тематике надзора за ними[62]. В этом отчете приведены и рассмотрены основные риски, ассоциируемые с ЭБ, а именно: стратегический риск, репутационный риск, операционный риск (включая риск безопасности и правовой риск)[63], а также кредитный, рыночный риски и риск ликвидности. EBG пришла к заключению, что деятельность в области ЭБ не приводит к возникновению рисков, которые не были бы уже идентифицированы в предыдущих работах БКБН. Однако ЭБ увеличивает и модифицирует некоторые из традиционных рисков, тем самым влияя на общий профиль риска банковского дела. В частности, стратегический риск, операционный риск и репутационный риск неизбежно повышаются из-за быстрого внедрения операций ЭБ и сопутствующего этому процессу усложнения технологий.

3.1. Проблемы, связанные с управлением рисками электронного банкинга

EBG отмечала, что фундаментальные характеристики ЭБ (и, в более общем варианте, электронной коммерции) обусловливают наличие ряда проблем, относящихся к управлению рисками:

- *беспрецедентная скорость изменений*, проявляющихся как инновации в технологиях и обслуживании клиентов посредством ЭБ. Исторически новые банковские технологии внедрялись в течение относительно продолжительных интервалов времени и только после тщательной проверки. Сегодня же банки испытывают конкурентное давление,

62 Electronic Banking Group Initiatives and White Papers (октябрь 2000 г.), размещен на web-сайте BIS по адресу http://www.bis.org

63 В этом разделе используется определение операционного риска, сформулированное Группой управления рисками БКБН, которое включает риск безопасности и правовой риск.

вынуждающее предлагать новые деловые механизмы в очень сжатые сроки — часто проходит всего несколько месяцев от разработки концепции до начала эксплуатации. Эта конкуренция усиливает управленческие проблемы в части обеспечения наличия адекватного стратегического оценивания, анализа рисков и проверки безопасности до внедрения новых практических решений в области ЭБ;

- *транзакционные web-сайты* и связанные с ними разнообразные и комплексные бизнес-решения *обычно интегрируются*, насколько это возможно, *с уже существующими компьютерными системами* в интересах достижения более «прямой» обработки электронных транзакций. Такая непосредственная автоматизированная обработка снижает вероятность человеческих ошибок и мошенничества, типичных для процессов, осуществляемых вручную, но она также увеличивает зависимость от того, насколько правильна конструкция систем и их архитектура, равно как и от взаимного функционирования систем и операционной масштабируемости;
- *ЭБ увеличивает зависимость банков от информационных технологий*, тем самым повышая техническую сложность многих функциональных задач и обеспечения безопасности, а также усиливая тенденцию к появлению соглашений с третьими сторонами о совместной работе, сотрудничестве и предоставлении услуг, многие из которых не подпадают под какое бы то ни было регулирование. Такое развитие ведет к возникновению новых бизнес-моделей, в которых участвуют банки и небанковские организации, такие как интернет-провайдеры, телекоммуникационные компании и другие технологические фирмы;
- *Интернет* по своей сути *имеет повсеместный и глобальный характер*. Это открытая сеть связи, к которой можно получить доступ из любого места в мире, оставаясь неизвестным, с передачей сообщений через неидентифицируемые узлы и с использованием быстро совершенствуемых беспроводных устройств. Вследствие этого существенно повышается значимость средств контроля безопасности, механизмов аутентификации пользователей.

3.2. Основные принципы управления рисками электронного банкинга

На основании проведенной ранее работы EBG БКБН пришел к выводу, что традиционные принципы управления банковскими рисками применимы к деятельности в области ЭБ. Комплексные характеристики каналов доведения услуг через Интернет вынуждают приспосабливать эти принципы ко многим банковским онлайновым операциям и соответствующим сопутствующим проблемам управления рисками.

БКБН полагает, что банкам потребуется разработка процессов управления рисками, соответствующих их индивидуальному профилю риска, функциональной структуре и культуре корпоративного управления, наряду с учетом соответствия специфическим требованиям и политике по управлению рисками, установленным органами банковского надзора в рамках конкретной юрисдикции (или нескольких).

Принципы управления рисками при осуществлении ЭБ делятся на три широкие и часто перекрывающиеся тематические категории (рис. 8). Однако эти принципы не ранжируются по степени их предпочтения или значимости. Все зависит от приоритетов, которые устанавливаются в каждой конкретной кредитной организации.

A. Наблюдение со стороны совета директоров и высшего руководства банка[64] *(Принципы 1–3):*

1. Эффективное наблюдение со стороны руководства за деятельностью в рамках ЭБ.
2. Организация полноценного процесса контроля безопасности.

64 В данном документе БКБН считается, что структура управления состоит из совета директоров и высшего руководства. БКБН осознает, что в разных странах существуют значительные различия в законодательных и регулятивных схемах, касающихся функций совета директоров и высшего руководства банков. В некоторых странах такой совет обладает главной, если не исключительной функцией надзора за исполнительным органом (высшим руководством, основным руководством) с точки зрения обеспечения выполнения последним своих обязанностей. По этой причине он иногда называется надзирающим советом. Напротив, в других странах компетенция такого совета шире и включает определение структуры основного руководства банков. Из-за различий такого рода сами термины «совет директоров» и «высшее руководство» используются для обозначения двух функций, связанных с принятием решений в банках, но не для определения узаконенных структур.

Рис. 8. Основные принципы управления рисками ЭБ

3. Полноценный процесс наблюдения за выполнением обязательств и управлением в отношении поставщиков услуг и других третьих сторон, от которых имеется зависимость.

B. Средства обеспечения безопасности (Принципы 4–10):

4. Аутентификация клиентов в операциях ЭБ.
5. Отсутствие отказов от проведения операций и возможность учета для транзакций, осуществляемых в рамках ЭБ.
6. Должные меры по обеспечению разделения обязанностей.
7. Необходимые средства авторизации в СЭБ, базах данных и прикладных программах.
8. Целостность данных в транзакциях ЭБ, записях и информации.
9. Организация формирования точных аудиторских записей для транзакций, осуществляемых в рамках ЭБ.
10. Конфиденциальность важнейшей банковской информации.

C. Управление правовыми и репутационными рисками (Принципы 11–14):

11. Правильное раскрытие информации для обслуживания в рамках ЭБ.
12. Конфиденциальность клиентской информации.
13. Планирование производительности, непрерывности операций и на случай непредвиденных обстоятельств для обеспечения доступности систем и обслуживания в рамках ЭБ.
14. Планирование реагирования на случайные события.

Каждый из перечисленных принципов обсуждается более подробно в последующих разделах в той мере, в какой они относятся к ЭБ и базовым принципам управления рисками. Там, где уместно, предлагаются дополнительные примеры правильной организации, которые могут рассматриваться как эффективные способы работы с этими рисками.

3.2.1. Наблюдение со стороны совета директоров и высшего руководства банка (Принципы 1–3)

Совет директоров (СД) и высшее руководство банка (ВРБ) отвечают за разработку деловой стратегии кредитной организации. Должны приниматься четкие стратегические решения относительно того, хочет ли СД, чтобы банк предоставлял обслуживание транзакций в рамках ЭБ до начала предложения таких услуг. В частности, СД следует убедиться в том, что планы внедрения ЭБ точно соответствуют корпоративным стратегическим целям кредитной организации. Одновременно должны быть организованы процессы смягчения и мониторинга рисков. А также необходимо убедиться, что осуществляется текущий контроль для оценивания результатов деятельности в рамках ЭБ в сопоставлении с деловыми планами и целями кредитной организации.

Кроме этого, СД и ВРБ следует удостовериться, что факторы риска, относящиеся к функционированию и безопасности в части деловых стратегий учреждения в рамках ЭБ, рассматриваются и учитываются должным образом. Обеспечение финансовых услуг через Интернет может существенно изменить и (или) даже увеличить традиционные банковские риски (например, стратегический, репутационный, операционный, кредитный и ликвидности). Поэтому следует принимать меры, чтобы существующие в банке процессы управления рисками, процессы контроля безопасности, процессы наблюдения и обеспечения выполнения обязательств для сторонних отношений должным образом оценивались и модифицировались в интересах приспособления к видам обслуживания в рамках ЭБ.

Принцип 1: СД и ВРБ следует установить эффективное управленческое наблюдение над рисками, связанными с деятельностью в рамках ЭБ, включая организацию специального учета, политики и средств контроля для управления этими рисками.

Бдительное управленческое наблюдение принципиально важно для обеспечения эффективного внутреннего контроля над деятельностью в рамках ЭБ. В дополнение к специфическим характеристикам канала предоставления услуг через Интернет[65] следующие аспекты ЭБ могут привести к значительным проблемам с традиционными процессами управления рисками:

- основные компоненты канала предоставления услуг (собственно Интернет и связанные с ним технологии) не поддаются непосредственному контролю со стороны банка;
- возможности Интернета по предоставлению услуг через множественные национальные юрисдикции, включая те страны, в которых нет физического присутствия данного учреждения;
- вопросы, ассоциируемые с ЭБ и предполагающие использование концепций и описаний на языках высоких технологий, во многих случаях оказываются незнакомыми для СД и ВРБ, имеющих традиционный опыт.

Ввиду уникальных характеристик ЭБ новые проекты в этой области, которые могут оказывать значительное влияние на профиль риска конкретного банка и его стратегию, должны изучаться СД и ВРБ и подвергаться соответствующему стратегическому и затратно-доходному анализу. Без адекватного непредвзятого изучения и текущей деятельности по планированию процедур оценивания банки рискуют недооценить затраты и (или) переоценить доходы от своих инициатив в области ЭБ.

Помимо этого, СД и ВРБ следует удостовериться в том, что их банк не включается в новый бизнес в сфере ЭБ или не внедряет новые технологии без наличия необходимых знаний для обеспечения компетентного наблюдения за управлением рисками. Знания руководства и персонала должны быть соразмерны технической природе

65 Были рассмотрены в разделе 2.2.

и сложности применяемых данным банком технологий ЭБ и соответствующих приложений. Адекватная квалификация является принципиально важной независимо от того, находятся СЭБ и соответствующие виды обслуживания под собственным управлением банка или эти функции переданы третьим сторонам. Процессы наблюдения со стороны ВРБ следует вести на динамической основе, чтобы осуществлять эффективное вмешательство и коррекцию любых материальных проблем с СЭБ или недостатков в обеспечении безопасности, которые могут иметь место. Повышенный репутационный риск, связанный с использованием технологии ЭБ, приводит к необходимости непрерывного мониторинга системной функциональности и удовлетворения требований пользователей, так же как должного информирования о происшествиях ВРБ.

Наконец, СД и ВРБ следует убедиться в том, что организованные ими процессы управления рисками для деятельности в рамках ЭБ интегрированы в общий подход данного банка к управлению рисками. Существующие в банке политика и процессы управления рисками должны быть оценены с точки зрения гарантии того, что они достаточно устойчивы, чтобы парировать новые риски, возникающие из-за текущей или планируемой деятельности в области ЭБ. Дополнительные меры по наблюдению за управлением рисками, которые следует принять во внимание СД и ВРБ, включают:

- четкое определение приемлемого уровня риска для данной банковской организации в рамках ЭБ;
- определение ключевых механизмов распределения полномочий и предоставления отчетности, включая необходимые расширенные процедуры для тех случаев, которые влияют на безопасность, надежность или репутацию банка (к примеру, сетевое проникновение, нарушение правил безопасности со стороны работников и любое серьезное нарушение в использовании компьютерных средств)[66];
- обращение внимания на любые особенные факторы риска, ассоциируемые с гарантиями безопасности, целостностью

66 В дополнение к требованиям, касающимся внутренней отчетности, расширенные процедуры предоставления отчетности о происшествиях должны включать также подготовку необходимых отчетов для соответствующих надзорных органов.

и доступностью услуг и видов обслуживания в части ЭБ и требующие принятия адекватных мер со стороны тех контрагентов, которым банк доверил обслуживание ключевых систем или прикладного программного обеспечения;

- обеспечение осуществления необходимого анализа выполнения обязательств и рисков до того, как банк начнет осуществление транзакционных операций в рамках ЭБ.

Интернет в значительной степени расширяет возможности банков по распространению услуг и видов обслуживания на виртуально безграничную географическую территорию, включая пересечение национальных границ. Такая трансграничная деятельность на основе ЭБ, особенно при осуществлении ее без какого-либо лицензированного физического присутствия в «стране дислокации», потенциально подвергает банки повышенным рискам: правовому, нормативному и страновому — ввиду значительных различий, которые могут иметь место между разными юрисдикциями в части требований к лицензированию банковской деятельности, надзора и защиты потребителей. Чтобы избегать непреднамеренного несоответствия законам и правилам зарубежных государств, так же как и с точки зрения управления факторами риска, относящимися к той или иной стране, банки, совершающие трансграничные операции посредством ЭБ, должны полностью изучить такие риски еще до практической реализации операций такого рода и организовать эффективное управление ими.

В зависимости от масштаба и сложности деятельности в рамках ЭБ охват и структура программ управления рисками будут различными для разных банковских организаций. Ресурсы, требуемые для наблюдения за обслуживанием в части ЭБ, следует определять в соответствии с транзакционной функциональностью и значимостью систем, уязвимостью сетей связи и важностью передаваемой по ним информации.

Принцип 2: СД и ВРБ следует проверять и утверждать ключевые составляющие процессов контроля безопасности банка.

СД и ВРБ следует наблюдать за разработкой и поддержанием инфраструктуры контроля над безопасностью, которая обеспечивает должную защиту СЭБ и данных как от внутренних, так и от внешних

угроз. При этом следует установить соответствующие права авторизации, логические и физические средства контроля доступа, а также адекватную инфраструктуру обеспечения безопасности для поддержания должных возможностей и ограничений в отношении действий как внутренних, так и внешних пользователей.

Защита банковских активов является одной из областей ответственности ВРБ. В то же время защита банковских активов представляет собой одну из проблемных задач в условиях быстро развивающейся сферы ЭБ ввиду комплексного характера рисков для безопасности, связанных с работой через Интернет и применением все новых технологий.

Чтобы гарантировать наличие должных средств обеспечения безопасности для деятельности в рамках ЭБ, СД и ВРБ требуется удостовериться в существовании в их банке полноценного процесса обеспечения защиты, включая политику и процедуры, которые касаются потенциальных внутренних и внешних угроз безопасности как в части предотвращения инцидентов, так и в части реагирования на такие происшествия. Ключевыми компонентами эффективного процесса обеспечения безопасности ЭБ являются:

- установление однозначно определенной ответственности руководства/персонала за организацию и соблюдение корпоративной политики безопасности[67];
- наличие достаточно эффективных средств физического контроля для предотвращения несанкционированного физического доступа к компьютерному оборудованию;
- наличие достаточных средств логического контроля и процессов мониторинга[68] для предотвращения неавторизованного внутреннего[69] и внешнего доступа к прикладным программам и базам данных ЭБ;

67 Такая ответственность обычно не должна являться объектом внимания аудита, который отвечает за проверку того, что функция контроля безопасности реализована эффективно.

68 Включая права контролируемого доступа и полномочия, равно как и текущий мониторинг попыток сетевого проникновения.

69 Включая сотрудников, контрактников и тех, кто обладает правами доступа на основе контрагентских отношений.

- регулярный пересмотр и тестирование мер безопасности и средств контроля, включая постоянное отслеживание современных отраслевых разработок в области безопасности и инсталляцию обновленных версий соответствующего программного обеспечения, служебных пакетов и прочие необходимые меры[70].

Ниже приведены дополнительные примеры надежной организации при обеспечении безопасности операций ЭБ.

1. Следует разработать и соблюдать политику обеспечения безопасности, а также особые полномочия авторизации, назначаемые всем пользователям систем и прикладных программ в рамках ЭБ, включая всех клиентов, внутренних пользователей в банке и внешних провайдеров услуг. Также следует разработать средства контроля логического доступа в обеспечение должного разделения обязанностей[71].
2. Данные и системы, относящиеся к области ЭБ, следует классифицировать в соответствии с их значимостью и уязвимостью и обеспечить им адекватную защиту. Для защиты всех уязвимых и подверженных высокому риску систем, серверов, баз данных и прикладных программ, функционирующих в СЭБ, следует использовать соответствующие механизмы, такие как шифрование, управление доступом и планы восстановления данных.
3. В кредитной организации следует свести к минимуму хранение уязвимых или подверженных высокому риску данных в настольных и переносных компьютерах, а также должным

70 Включая меры по мониторингу сетевой активности, фиксации попыток проникновения и сведения о серьезных недостатках в обеспечении безопасности.

71 Определение стандартов безопасности и качества, а также надежности схем сертификации могут быть специфичными для отдельных учреждений или стандартизованными (то есть в пределах национальной банковской отрасли в целях повышения и совершенствования уровня безопасности деятельности в рамках электронного банкинга). Банки могут выбирать также назначение прав доступа как на централизованной, так и на распределенной основе. Например, может существовать единственный орган авторизации, ответственный за назначение прав доступа отдельным пользователям, группам пользователей, либо могут иметься несколько органов авторизации, организованных для упорядочения работы по разным направлениям ведения бизнеса.

образом защищать их с помощью шифрования, контроля доступа и планов восстановления данных.

4. Должны иметься в наличии достаточные физические средства контроля для предотвращения неавторизованного доступа[72] ко всем критичным системам, серверам, базам данных и прикладным программам, применяемым в системах области ЭБ.
5. Следует применять должные методы парирования внешних угроз СЭБ, включая использование:
   - программного обеспечения для обнаружения компьютерных вирусов во всех критических точках входа (к примеру, на серверах удаленного доступа, прокси-серверах электронной почты) и на каждой настольной системе;
   - программного обеспечения для обнаружения проникновения и другие инструментальные средства оценивания безопасности для периодической проверки сетей связи, серверов и брандмауэров на предмет наличия слабых мест и (или) нарушений политики и средств контроля безопасности;
   - тестирования вариантов проникновения во внутренние и внешние сети связи.

Все сотрудники и провайдеры услуг, занимающие ключевые позиции, должны проходить тщательный процесс проверки надежности.

Принцип 3: СД и ВРБ следует внедрить полноценные и непрерывные процессы наблюдения и контроля выполнения обязательств для управления отношениями банка с провайдерами услуг и другими сторонами, обеспечивающими поддержку выполнения операций ЭБ.

Повышенная зависимость от партнеров и сторонних провайдеров услуг при осуществлении критических функций в рамках ЭБ

72 Они должны включать средства защиты от неавторизованного доступа со стороны посторонних, таких как посетители, контрактники или техники, которые могут иметь доступ в помещения, не будучи непосредственно вовлеченными в обслуживание, осуществляемое в рамках электронного банкинга.

снижает возможности непосредственного контроля над ними со стороны руководства банка. Соответственно, оказывается необходимым всеобъемлющий процесс управления рисками, ассоциируемыми с заказной обработкой и зависимостью от других сторонних организаций. Этот процесс должен охватывать стороннюю деятельность партнеров и провайдеров обслуживания, включая субконтракты на заказную обработку, которые могут иметь материальные последствия для банков.

Исторически заказная обработка часто ограничивалась единственным провайдером обслуживания по заданному набору операций. Однако в последние годы масштаб и сложность связей банков в части заказной обработки значительно возросли, что явилось прямым результатом успехов в информационных технологиях и внедрения ЭБ. В дополнение к указанной сложности следует учитывать тот факт, что внешне обслуживание операций ЭБ может передаваться по субконтрактам дополнительным провайдерам услуг и (или) осуществляться в другой стране. Кроме того, по мере технологического развития и роста стратегической важности приложений и видов обслуживания ЭБ определенные функциональные участки ЭБ оказываются зависимыми от небольшого числа специализированных сторонних поставщиков и провайдеров услуг. Эти разработки могут привести к повышенной концентрации рисков, которая оправдывает внимание как со стороны одного банка, так и со стороны отрасли в целом.

В совокупности все эти факторы подчеркивают необходимость во всеобъемлющем и постоянном оценивании связей в рамках заказной обработки и других видов внешней зависимости, включая ассоциируемые с ними влияния на профиль риска конкретного банка и возможности надзора за управлением рисками[73]. Наблюдение со стороны СД и ВРБ за связями в части заказной обработки

73 При таком оценивании следует также учитывать степень контроля, реализуемого в отношении сторонних организаций. Основной акционер в совместном предприятии нередко может обладать большим контролем, чем в случае контрактных отношений с провайдером услуг. Однако из таких различий не следует, что акционерный контроль над совместным предприятием или товариществом будет всегда эффективным, особенно если технологии и обслуживание, необходимые для работы такой ассоциации, предоставляются акционером с малым числом акций. Такие различения бывают полезны в основном для того, чтобы обосновать проведение оценивания время от времени.

и зависимости от сторонних организаций следует особенно фокусировать на том, чтобы обеспечивались:

- полное понимание банком тех рисков, которые связаны с привлечением сторонних провайдеров услуг или партнеров в заказную обработку или партнерские отношения для работы его банковских систем или прикладных программ;
- должная своевременная проверка компетентности и финансовой устойчивости любых сторонних провайдеров услуг или партнеров, проводимая до заключения каких-либо контрактов на обслуживание в рамках ЭБ;
- точное определение контрактной подотчетности всех участников заказной обработки или партнерских отношений. К примеру, должны быть четко определены обязанности по предоставлению информации провайдеру услуг и получению информации от него;
- учет всех операций и СЭБ, связанных с заказной обработкой, в концепциях управления рисками, обеспечения безопасности и соблюдения конфиденциальности, которые удовлетворяют стандартам, принятым в данном банке;
- проведение периодического независимого внутреннего и (или) внешнего аудита заказных операций по меньшей мере в том же объеме, который требовался бы, если бы такие операции проводились в самом банке;
- наличие должных планов на случай непредвиденных обстоятельств для деятельности в рамках ЭБ, осуществляемой в заказном порядке.

Ниже приведены дополнительные примеры надежной организации при управлении внешними СЭБ и другими зависимостями от сторонних организаций.

1. Банкам следует внедрить необходимые процессы для оценивания решений, принимаемых в отношении внешних (заказных) систем и видов обслуживания, в части ЭБ:
    - руководству банка следует четко определить стратегические цели, выгоды и затраты, связанные с заключением соглашений с третьими сторонами на заказную обработку в рамках ЭБ;

- решения об использовании сторонней обработки для ключевых функций или видов обслуживания в части ЭБ должны быть согласованы с деловыми стратегиями данного банка, основываться на точно определенных деловых потребностях и учитывать специфические риски, обусловленные использованием заказной обработки;
- все заинтересованные стороны в банке должны понимать, каким образом провайдер(ы) услуг будет (будут) поддерживать стратегию самого банка в области ЭБ и обеспечивать соответствие его функциональной структуре.

2. Банкам следует проводить должный анализ рисков и выполнения обязательств до выбора какого-либо провайдера услуг в части ЭБ, и через соответствующие интервалы времени впоследствии:
   - банкам следует рассматривать процессы развития по конкурентным предложениям от нескольких провайдеров услуг в области ЭБ и критерии для выбора при наличии различных предложений;
   - после определения потенциального провайдера услуг банку следует провести проверку обеспечения соблюдения обязательств, включая анализ риска в отношении финансовых ресурсов данного провайдера услуг, репутации, политики управления рисками и средств управления, а также способности выполнять свои обязательства;
   - далее, банкам следует регулярно контролировать и при необходимости проводить проверку соблюдения обязательств относительно возможностей провайдера услуг в части выполнения им заданного обслуживания и связанных с ним обязательств по управлению рисками на протяжении всего срока действия заключенного контракта[74];
   - банкам необходимо гарантировать, что для наблюдения за соблюдением соглашений на заказную обработку

74 Масштаб проверок соблюдения обязательств следует определять исходя из финансовой значимости заказных операций и степени изменений в системах и управлении рисками с течением времени, включая любые последующие субконтрактные отношения, которыми может быть связан данный провайдер услуг.

в обеспечение операций ЭБ выделены адекватные ресурсы;

- обязанности по наблюдению за соблюдением соглашений на заказную обработку в рамках ЭБ должны быть четко распределены;
- должна быть разработана правильная стратегия ухода для банка с точки зрения управления рисками, если ему придется прервать договорные отношения по заказной обработке.

3. Банкам следует внедрить необходимые процедуры для обеспечения адекватности контрактов, в соответствии с которыми выполняются операции ЭБ. В контрактах, определяющих заказную деятельность в части ЭБ, должно учитываться, например, следующее[75]:
   - четкое определение контрактных обязательств договаривающихся сторон, равно как и ответственность за принятие решений, включая любые субконтрактные отношения по предоставлению реальных услуг;
   - четкое определение ответственности в части предоставления информации провайдеру услуг и получения информации от него. Информация от провайдера услуг должна быть своевременной и достаточно полной для того, чтобы банк имел возможности адекватного оценивания уровней обслуживания и рисков. Следует оговорить пределы затрат и процедуры, необходимые для уведомления банка о прерывании обслуживания, недостатках в обеспечении безопасности и других событиях, которые подвергают данный банк материальному риску;
   - четкое определение резервов, которые предназначены конкретно для страхового покрытия, прав собственности на данные, хранимые на серверах или в базах данных конкретного провайдера услуг, а также права банка

75 Как и в случае других законных контрактов, которые может заключать банк, его юрист или юридическое подразделение должны изучать все пункты и условия контрактов, определяющие соглашения по заказной обработке в рамках электронного банкинга.

на возвращение его данных по истечении или прекращении контрактных отношений;

- определение предполагаемого функционирования как при нормальных условиях, так и при чрезвычайных обстоятельствах;
- определение адекватных мер и гарантий, в частности, на основе аудиторских заключений, в обеспечение того, что провайдер услуг действует в соответствии с политикой банка;
- наличие возможностей для своевременного и уместного вмешательства и устранения ошибок в случае нестандартной работы провайдера услуг;
- в случае трансграничных соглашений о заказной обработке — определение того, законы и правила какой именно страны будут применимы, включая и те, которые относятся к обеспечению конфиденциальности и другим видам защиты прав клиентов;
- четкое определение права банка на проведение независимых проверок и (или) аудита обеспечения безопасности, средств внутреннего контроля и непрерывности деловых операций, а также планов на случай непредвиденных обстоятельств.

4. Банкам следует обеспечить периодическое проведение внутренних и (или) внешних аудиторских проверок заказных операций по меньшей мере в том же масштабе, который требовался бы, если бы такие операции проводились в самом банке[76]. В отношении внешних взаимодействий, включающих критичные или технологически сложные виды обслуживания / программные приложения, банкам может потребоваться организация других периодических проверок, выполняемых независимыми сторонними организациями, обладающими достаточной технической квалификацией.

76 Банкам, в которых отсутствует специализированная аудиторская служба, следует как минимум иметь сотрудников, не принимающих участия в управлении отношениями, связанными с заказной обработкой, и проверяющих эффективность наблюдения за соблюдением таких контрагентских отношений.

5. Банкам следует разработать необходимые планы на случай непредвиденных обстоятельств в связи с заказной деятельностью в области ЭБ:
   — банкам необходимо разрабатывать планы на случай непредвиденных обстоятельств для всех критичных систем и видов обслуживания в рамках ЭБ, которые были возложены на сторонние организации, осуществляющие заказную обработку, и периодически тестировать эти планы;
   — в планах на случай непредвиденных обстоятельств следует учитывать правдоподобные сценарии наихудшего развития событий с точки зрения обеспечения непрерывности обслуживания в рамках ЭБ, если произойдут нарушения в работе, влияющие на выполнение заказных операций;
   — банкам следует иметь точно определенную группу сотрудников, ответственную за обеспечение восстановления и оценивание физического результата на случай прерывания заказного обслуживания в рамках ЭБ.
6. Банкам, которые возлагают обслуживание в рамках ЭБ на сторонние организации, следует удостовериться в том, что их операции, ответственность и обязательства определены достаточно точно, так, чтобы обслуживаемые учреждения могли адекватно осуществлять эффективные проверки соблюдения обязательств и текущее наблюдение за действующими отношениями.
7. Банки несут ответственность за предоставление обслуживаемым учреждениям информации, необходимой для определения, контроля и мониторинга любых рисков, связанных с соглашениями по обслуживанию в рамках ЭБ.

3.2.2. Средства обеспечения безопасности (Принципы 4–10)

Ввиду того что СД банка несет ответственность за обеспечение наличия должных процессов контроля безопасности для операций ЭБ, содержание этих процессов требует особого внимания со стороны

органов управления из-за более сложных проблем с безопасностью, которые возникают при операциях ЭБ[77].

Следующие вопросы являются особенно значимыми:

- аутентификация;
- невозможность отказных операций;
- целостность данных и транзакций;
- разделение обязанностей;
- средства управления авторизацией;
- поддержание аудиторских записей;
- конфиденциальность важнейшей банковской информации.

Принцип 4: Банкам следует принимать должные меры по аутентификации идентичности и авторизации[78] клиентов, с которыми они осуществляют деловые операции через Интернет.

В банковском деле принципиально важно подтверждение того, что конкретный запрос на взаимодействие (связь), транзакцию или доступ имеет легитимный характер. Соответственно, банкам следует применять надежные методы для верификации идентичности и авторизации новых клиентов, так же как и для аутентификации идентичности и авторизации зарегистрированных клиентов, обращающихся за проведением электронных транзакций.

Верификация клиентов (при определении происхождения счета) важна для снижения риска хищений идентификационных данных, мошеннических действий со счетами и отмывания денег. Если банк не может адекватно аутентифицировать клиентов, то в результате возможны получение несанкционированного доступа к счетам по операциям ЭБ и в конечном итоге финансовые потери и ущерб

77 К примеру, в тех случаях, когда СД полагается на сторонних поставщиков в части обслуживания в рамках ЭБ, он должен убедиться в том, что данный поставщик адекватно относится к решению этих вопросов и как минимум удовлетворяет собственным стандартам деятельности банка.

78 В этом разделе под *аутентификацией* понимаются методы, процедуры и процессы, используемые для подтверждения идентичности и авторизации ожидаемых и установленных пользователей. Под *идентификацией* — процедуры, методы и процессы, используемые для установления идентичности клиентов при открывании счетов. Под *авторизацией* — процедуры, методы и процессы, используемые для определения того, обладает ли клиент или сотрудник разрешенным доступом или полномочиями для проведения транзакций, связанных с конкретными счетами.

для репутации банка из-за мошенничества, утечки конфиденциальной информации или непреднамеренного вовлечения в преступную деятельность.

Установление и аутентификация идентичности того или иного лица, а также авторизации доступа к банковским системам в условиях полностью электронной открытой сети связи может оказаться трудной задачей. Легитимная авторизация пользователя может быть фальсифицирована с помощью разнообразных методов, обычно называемых «мистификация»[79]. Онлайновые хакеры могут также перехватить сеанс легитимно авторизованного лица, используя «вынюхивателя»[80], и выполнять действия вредоносного или криминального характера. Помимо прочего, процессы контроля аутентификации могут быть обойдены посредством воздействия на базы данных, хранящие аутентификационные сведения.

Соответственно, критично, чтобы банки имели оформленные политику и процедуры, определяющие необходимую методологию (или методики), для того чтобы гарантировать, что отдельный банк должным образом осуществляет аутентификацию идентичности и авторизации прав того или иного лица, агента или системы[81] с помощью уникальных способов и настолько, насколько это практично, гарантирует исключение участия неавторизованных лиц или систем[82]. Банки могут применять разнообразные методы для осуществления аутентификации, включая ПИНы, пароли, микропроцессорные карты, биометрику и цифровые сертификаты[83]. Эти

79 Мистификация (spoofing) — это имитация легитимного клиента за счет использования его номера счета, пароля, персонального идентификационного номера (ПИН) и (или) адреса электронной почты.

80 Вынюхиватель (sniffer) — это устройство, которое способно просмотреть поток данных, передаваемых по каналу связи, перехватить пароли и данные при их передаче.

81 В число систем включаются и собственные web-сайты учреждений.

82 В системах должно быть предусмотрено определение того, что они работают с аутентифицированным лицом, агентом или системой и с действительной базой данных аутентификации.

83 Банк может выдавать цифровые сертификаты с использованием инфраструктуры открытых ключей (ИОК) для клиента, чтобы обеспечить безопасность связи с банком. Цифровые сертификаты и ИОК более полно рассмотрены в изложении Принципа 5.

методы могут быть однопараметрическими или многопараметрическими (имея в виду использование как пароля, так и биометрических технологий[84] для аутентификации). Многопараметрическая аутентификация в общем случае обеспечивает бóльшую уверенность в идентификации.

Банк должен определить, какие методы аутентификации использовать на основе оценки руководством банка риска, возникающего из-за применения СЭБ в целом или каких-либо ее составных компонентов. В процессе анализа риска следует оценивать пропускную способность[85] СЭБ (например, по переводам средств, платежам, запросам на ссуды, агрегации счетов и т. д.), значимость и значение хранимых данных по операциям ЭБ, а также удобства для клиентов при использовании принятого метода аутентификации.

Надежные процессы идентификации и аутентификации клиентов особенно важны в контексте трансграничных операций с применением технологий ЭБ, учитывая осложнения, которые могут возникнуть при осуществлении электронных операций с клиентами через национальные границы, включая повышенный риск обезличивания индивидуальности и большие затруднения в выполнении эффективных проверок при предоставлении кредита потенциальным клиентам.

Поскольку методы аутентификации продолжают совершенствоваться, банкам рекомендуется отслеживать и перенимать используемые в отрасли надежные методы работы в данной части, обеспечивающие:

- защиту аутентификационных баз данных, которые предназначены для организации доступа к счетам клиентов ЭБ или

84 Технология биометрики представляет собой автоматизированную проверку физиологических или бихевиорических характеристик, используемых для идентификации и (или) аутентификации личности. Общепринятые формы биометрических технологий включают портретное сканирование, распознавание отпечатков пальцев, сканирование радужной оболочки глаза, сканирование сетчатки глаза, сканирование рук, сканирование подписи, опознавание голоса и динамики нажатия клавиш. Системы биометрической идентификации обеспечивают очень точную аутентификацию, но вместе с тем могут значительно усложнить этот процесс по сравнению с другими методами идентификации/аутентификации.

85 Эффективные решения в части аутентификации могут также уменьшить риск отказа от операции, источником которого является то, что авторизованный пользователь через какое-то время может отрицать факт осуществления им авторизованной транзакции (см. также Принцип 5).

важным системам, от изменения и повреждения. Любое подобное воздействие должно обнаруживаться, при этом должны вестись аудиторские записи для документирования попыток такого рода;

- должную авторизацию любых добавлений, удалений или изменений в аутентификационной базе данных для того или иного лица, агента или системы с помощью какого-либо источника аутентификационных данных[86];
- осуществление должных мер для контроля подключений к СЭБ, таких, чтобы кто-то неизвестный со стороны не мог подменять известных клиентов;
- поддержание безопасности аутентификационного сеанса в рамках ЭБ во время всей его длительности или затребование повторной аутентификации в случае ошибок в защите.

Принцип 5: Банкам следует использовать методы аутентификации транзакций, которые способствуют невозможности отказа от операций (доказательного подтверждения операции) и обеспечивают возможность учета транзакций в рамках ЭБ.

Невозможность отказа от операции обеспечивается за счет формирования доказательства по ее источнику или предоставлению информации в электронной форме для защиты отправителя от ложного отрицания получателем того, что конкретные данные были получены, или для защиты получателя от ложного отрицания отправителем того, что конкретные данные были отправлены. Риск отрицания транзакций уже стал реальностью для обычных транзакций, которые осуществляются посредством кредитных карточек, или при транзакциях ценных бумаг. В то же время технология ЭБ увеличивает этот риск ввиду сложностей с положительной аутентификацией идентичности и полномочий тех, кто инициирует транзакции, возможностей воздействия на электронные транзакции и их перехват, а также возможностей для пользователей технологий ЭБ заявлять, что их транзакции подверглись мошенническому воздействию.

86 В некоторых случаях источниками аутентификационных данных могут быть электронные средства.

Для парирования описанных повышенных угроз банкам требуется предпринимать немалые усилия, соразмерные со значимостью и типами конкретных транзакций в рамках ЭБ, чтобы обеспечить:

- разработку СЭБ таким образом, чтобы уменьшить вероятность инициирования авторизованными пользователями непреднамеренных транзакций, и полное понимание клиентами особенностей рисков, которые связаны с любыми инициируемыми ими транзакциями;
- положительную аутентификацию всех участников конкретной транзакции и поддержание контроля над аутентифицированным каналом взаимодействия;
- защиту данных о финансовых транзакциях от воздействия извне и обнаружение любых воздействий такого рода.

Банковские организации начали применять разнообразные способы, содействующие обеспечению доказательности и гарантированной конфиденциальности транзакций в рамках ЭБ, такие как цифровые сертификаты с использованием инфраструктуры открытых ключей[87]. Банк может выдать цифровой сертификат клиенту или контрагенту для обеспечения их уникальной идентификации/аутентификации и уменьшить риск отрицания транзакций. Хотя в некоторых странах права клиента на отклонение транзакций предусмотрены в специальных нормативных актах, в отдельных национальных юрисдикциях приняты законодательные акты, признающие правомочность цифровых подписей. По мере продолжения развития технологий вероятно более широкое, глобальное правовое признание таких способов.

87 При использовании ИОК каждая сторона обладает парой ключей шифрования: личным и открытым. Личный ключ является скрытым, чтобы им мог пользоваться только один человек. Открытый ключ используется всеми участниками. С помощью личного ключа генерируется цифровая подпись к документу, а сама ключевая пара сконструирована таким образом, что сообщение, зашифрованное с личным ключом, может быть прочитано только с помощью второго ключа. Банк может сам действовать как орган сертификации (ОС) или полагаться на стороннюю доверенную организацию в части снабжения того или иного лица либо контрагента конкретным цифровым сертификатом. Однако если банк получает цифровой сертификат для обеспечения аутентичности со стороны, то он должен убедиться в том, что ОС, выдавший этот сертификат, обеспечивает тот же уровень аутентификации, который гарантировал бы сам банк при аутентификации личности. Основным недостатком системы аутентификации с ИОК является то, что ее сложнее реализовать.

Принцип 6: Банкам следует гарантировать наличие необходимых мер по адекватному разделению обязанностей в системах баз данных и прикладных программных комплексах ЭБ.

Разделение обязанностей представляет собой основную меру внутреннего контроля, предназначенную для уменьшения риска мошенничества в операционных системах и процессах, а также для обеспечения должной авторизации, фиксации и защищенности транзакций и активов своих компаний. Разделение обязанностей является критичным для гарантирования точности и целостности данных и используется для предотвращения проникновения злоумышленников. Если обязанности разделены правильно, то мошенничество может быть совершено только на основе тайного сговора.

Обслуживание в рамках ЭБ может привести к необходимости изменения тех способов, которыми осуществляется и поддерживается разделение обязанностей, поскольку транзакции выполняются через электронные системы, в которых действующих лиц легче замаскировать или подменить. Кроме того, в практических приложениях ЭБ операционные и транзакционные функции во многих случаях оказываются более комплексированными и интегрированными. Вследствие этого традиционно требуемые средства управления для поддержания разделения обязанностей следует пересмотреть и адаптировать в интересах обеспечения сохранения должного уровня контроля. Ввиду того что доступ к плохо защищенным базам данных гораздо легче получить через внутренние или внешние сети связи, необходимо сделать акцент на процедуры строгой авторизации и идентификации, безопасную и надежную архитектуру процессов сквозной обработки, а также на адекватные аудиторские записи.

В обычную практику организации и поддержания разделения обязанностей в комплексах ЭБ входят:

- разработка транзакционных процессов и систем таким образом, чтобы обеспечивалась невозможность ввода, авторизации и завершения транзакций ни для какого работника или провайдера заказных услуг;
- соблюдение разделения функций между теми, кто работает со статичными данными (включая содержание web-страниц), и теми, кто отвечает за верификацию и целостность данных;

- тестирование с СЭБ на предмет проверки невозможности обхода установленного разделения обязанностей;
- соблюдение разделения функций между теми, кто разрабатывает, и теми, кто администрирует СЭБ[88].

Принцип 7: Банкам следует обеспечивать наличие должных средств авторизации и полномочий доступа для систем, баз данных и приложений ЭБ.

Для поддержания разделения обязанностей банкам необходимо строго контролировать авторизацию и полномочия доступа. Недостатки в обеспечении адекватного контроля авторизации могут дать возможность отдельным лицам расширить свои права авторизации, обойти разделение функций и получить доступ к системам, базам данных и прикладным программам ЭБ, к которым они не допущены.

В СЭБ права авторизации и доступа могут устанавливаться в банках как централизованно, так и распределенным образом, и соответствующие параметры обычно заносятся в базы данных. Защита таких баз данных от внешнего воздействия или повреждения является принципиально необходимой для эффективного контроля авторизации.

Ниже приведены дополнительные примеры надежной организации, которые могут помочь установить должный контроль над авторизацией и правами доступа к системам, базам данных и прикладным программам ЭБ.

1. Всем личностям, агентам или системам, участвующим в деятельности, осуществляемой в рамках ЭБ, следует назначить специальную авторизацию и полномочия доступа.
2. Все СЭБ следует проектировать таким образом, чтобы они гарантированно взаимодействовали с правильной базой данных авторизации.
3. Никакому отдельному агенту или системе не должна быть предоставлена возможность изменять его или ее собственные

88 Либо должны присутствовать альтернативные компенсирующие средства контроля.

права либо полномочия доступа, зафиксированные в базе данных авторизации, входящей в СЭБ[89].

Любые добавления персоналии, агента или системы либо изменения в полномочиях доступа, зафиксированных в базе данных авторизации, применяемой в рамках ЭБ, должны быть авторизованы в установленном порядке от аутентифицированного источника, наделенного соответствующими правами адекватным руководящим органом, и должны подлежать полноценному и своевременному наблюдению, а также отражению в аудиторских записях.

Должные меры следует принимать для обеспечения обоснованной устойчивости баз данных авторизации в части ЭБ к внешним воздействиям. Любое такое воздействие подлежит обнаружению с помощью процессов постоянного мониторинга. Следует обеспечить документирование в аудиторских записях всех попыток воздействия подобного рода.

Любую базу данных, используемую в СЭБ, которая подверглась внешнему воздействию, следует исключить из пользования до замены ее удостоверенной базой данных.

Следует обеспечить наличие средств контроля для предотвращения изменений в уровнях авторизации во время сеансов проведения транзакций в рамках ЭБ, кроме того, любые попытки внесения изменений в авторизацию должны фиксироваться и соответствующая информация должна предоставляться руководству банка.

Принцип 8: Банкам следует обеспечивать наличие должных мер защиты целостности данных в транзакциях, записях и информации ЭБ.

Под целостностью данных понимается гарантия того, что передаваемая или хранимая информация не подвергалась неавторизованному воздействию. Недостатки в обеспечении целостности данных в транзакциях, записях и информации могут привести банки к финансовым потерям, а также к возрастанию правового и репутационного риска.

89 Если это нереально для пользователей уровня системного администратора, следует обеспечить наличие других средств строгого внутреннего контроля и разделение обязанностей для мониторинга движения средств по счетам таких пользователей.

Сам характер сквозной обработки для операций ЭБ может затруднить обнаружение ошибок программирования или мошеннической деятельности на ранней стадии. Поэтому банкам следует реализовать сквозную обработку таким образом, чтобы гарантировать безопасность и идентичность, а также целостность данных.

Поскольку данные по операциям ЭБ передаются по открытым сетям связи, транзакции подвержены дополнительной опасности искажения данных, мошенничества и воздействия на записи. Соответственно, банкам следует обеспечивать наличие должных мер, позволяющих удостовериться в точности, полноте и надежности транзакций, записей и информации ЭБ, которые как передаются через Интернет, размещаясь во внутренних базах данных банков, так и передаются/хранятся сторонними провайдерами услуг по поручению конкретного банка[90]. Обычные меры, применяемые для поддержания целостности данных в комплексах ЭБ, включают:

- проведение транзакций ЭБ таким образом, который обеспечивает их высокую устойчивость к внешним воздействиям на протяжении всего процесса;
- хранение, предоставление и модификацию записей об операциях ЭБ таким образом, который обеспечивает их высокую устойчивость к внешним воздействиям;
- разработку процессов обработки транзакций и хранения записей ЭБ таким образом, чтобы было фактически невозможно избежать обнаружения неавторизованных изменений;
- наличие адекватной политики контроля над изменениями, включая процедуры мониторинга и тестирования, для защиты против любых изменений в СЭБ, которые могут из-за ошибочных или намеренных действий повредить средствам управления или снизить надежность данных;
- обнаружение любого воздействия на транзакции или записи ЭБ с помощью функций обработки транзакций, мониторинга и обеспечения сохранности данных.

90 Банкам следует удостовериться, что системы хранения записей разработаны и инсталлированы таким образом, что возможно восстановление записей, которые могли подвергнуться воздействию или порче.

Принцип 9: Банкам следует убедиться в формировании точных аудиторских записей по всем транзакциям в рамках ЭБ.

Предоставление финансовых услуг через Интернет может затруднить для банков внедрение и применение средств внутреннего контроля и поддержание точных аудиторских записей, если эти меры не адаптированы к комплексу ЭБ. Банки сталкиваются с проблемами обеспечения не только внутреннего контроля в условиях значительной автоматизации, но также независимого аудита средств контроля, особенно в части всех критичных для операций ЭБ событий и прикладных программ.

Условия работы внутреннего контроля банка могут быть ухудшены, если отсутствует возможность для формирования точных аудиторских записей по деятельности в рамках ЭБ. Это обусловлено тем, что многие, если не все, записи о таких операциях и фиксации событий осуществляются в электронной форме. При определении ситуаций, в которых следует обеспечивать наличие точных аудиторских записей, требуется рассматривать следующие типы транзакций в рамках ЭБ:

- открытие, изменение или закрытие счетов клиента;
- любые транзакции, влекущие финансовые последствия;
- любую авторизацию, модификацию или аннулирование прав доступа к системе или полномочий.

Ниже приведены дополнительные примеры надежной организации в целях обеспечения наличия точных аудиторских записей для транзакций, осуществляемых в рамках ЭБ.

1. В банках должны постоянно вестись электронные журналы, в которых осуществляется фиксация всех событий в системе и их описаний по всем транзакциям в рамках ЭБ, чтобы способствовать формированию четких аудиторских записей и аргументации в разрешении спорных вопросов.
2. СЭБ следует разрабатывать и внедрять таким образом, чтобы обеспечивались фиксация и сохранение учитываемых в судебном разбирательстве свидетельств, а также предотвращения воздействия извне и получения фальшивых улик.
3. В случаях когда за системы обработки и связанные с ними аудиторские записи отвечает сторонний провайдер услуг:
   — банку следует обеспечить себе доступ к требуемым ему аудиторским записям, которые делает провайдер услуг;

— аудиторские записи, обеспечиваемые провайдером услуг, должны удовлетворять стандартам, установленным в данном банке.

Принцип 10: Банкам следует принимать должные меры для сохранения конфиденциальности важнейшей информации в области ЭБ. Меры, принимаемые для сохранения конфиденциальности, должны быть соразмерны значимости передаваемой и (или) хранимой в базах данных информации.

Конфиденциальность определяется как уверенность в том, что важная информация остается частной в банке и не просматривается или не используется никем, кроме имеющих на это право (авторизацию). Недопустимое использование или неавторизованное раскрытие данных подвергает банк как репутационному, так и правовому рискам. Внедрение технологии ЭБ приводит к появлению дополнительных проблем с безопасностью для банка, поскольку увеличивает возможности доступа к информации, передаваемой через открытую сеть связи или хранимой в базах данных, со стороны неавторизованных либо нежелательных лиц или же использования ее такими способами, которые не предполагались клиентом, предоставившим данную информацию. Кроме того, активное использование услуг провайдеров может привести к раскрытию важнейших банковских данных посторонним.

Для того чтобы парировать проблемы с сохранением конфиденциальности важнейшей банковской информации в части ЭБ, необходимо гарантировать, что:

- доступ ко всем конфиденциальным банковским данным и информации возможен только для должным образом авторизованных и аутентифицированных лиц, агентов или систем;
- для всех конфиденциальных банковских данных в процессе передачи через открытые, частные или внутренние сети связи обеспечиваются безопасность и защита от несанкционированного просмотра или изменения;
- в случаях использования заказной обработки обеспечивается соответствие стандартам и способам контроля банка над использованием данных и их защитой;

- весь доступ к данным ограниченного использования фиксируется и приняты необходимые меры по защите журналов регистрации доступа к этим данным от внешнего воздействия.

3.2.3. Управление правовым и репутационным рисками (Принципы 11–14)

Специфические законы и правила защиты клиента и обеспечения конфиденциальности варьируются от одной юрисдикции к другой. Как бы то ни было, банки в общем случае несут четко определенную ответственность за обеспечение своим клиентам соответствия некоторым уровням требований относительно раскрытия информации, защиты клиентских данных и доступности деловых операций, которые были бы близки к тем уровням, которые они обеспечивали бы, если бы осуществляли деловые операции через традиционные каналы предоставления банковских услуг.

Принцип 11: Банкам следует убедиться в том, что на их web-сайтах представлена правильная информация, позволяющая потенциальным клиентам сделать обоснованные заключения относительно самого банка и его организационно-правовой формы еще до проведения транзакций через СЭБ.

Для того чтобы минимизировать правовой и репутационный риски, связанные с деятельностью в области ЭБ, осуществляемой как локально, так и трансгранично, банкам еще до того, как начать осуществлять транзакции в рамках ЭБ, следует удостовериться, что на их web-сайтах представлена правильная информация о самом банке и его правовом статусе.

В число примеров информации такого рода, которую банк может представить на своем web-сайте, входят:

- название банка и сведения о местоположении его головного офиса (а также региональных офисов, если они существуют);
- указание на основной орган (или органы) надзора за банком, ответственный за осуществление надзора за головным офисом данного банка;

- способы контакта клиентов банка с его центром обслуживания клиентов, решающим проблемы с услугами, рассматривающим жалобы, подозрения в неправомочном использовании счетов и т. п.;
- способы контакта клиентов и общения с соответствующим наблюдательным органом или структурами, отвечающими за определение правил обслуживания потребителей;
- способы получения клиентами доступа к информации о возможных государственных компенсациях или страховом покрытии депозитов (или же указание на web-сайт с такой информацией);
- другая информация, которая может быть полезна или затребована в рамках конкретных юрисдикций[91].

Принцип 12: Банкам следует принимать должные меры в обеспечение следования требованиям гарантии конфиденциальности для клиентов, применимым в той юрисдикции, в пределах которой данный банк предоставляет услуги и виды обслуживания, относящиеся к ЭБ.

Соблюдение конфиденциальности клиентской информации представляет собой важнейшую ответственность для банка. Ненадлежащее использование или неавторизованное раскрытие конфиденциальных клиентских данных подвергает банк как правовому, так и репутационному рискам. Для решения проблем, относящихся к сохранению конфиденциальности клиентской информации, банкам следует прилагать разумные усилия в обеспечение того, чтобы:

- в политике и стандартах банка, описывающих соблюдение конфиденциальности для клиента, были учтены и соблюдены требования всех законов и правил, касающихся конфиденциальности и применимых в пределах той юрисдикции, в рамках которой предоставляются услуги и виды обслуживания, относящиеся к ЭБ;

91 Например, банк может, при желании, указать те страны, в которых он намеревается предоставлять обслуживание в рамках электронного банкинга, или, напротив, те страны, в которых он не собирается предлагать такие виды обслуживания.

- клиенты были поставлены в известность о политике соблюдения конфиденциальности банком и соответствующих вопросах соблюдения конфиденциальности, относящихся к использованию услуг и видов обслуживания в рамках ЭБ;
- клиенты могли отклонять («вычеркивать») разрешения на предоставление банком третьим сторонам в целях перекрестного маркетинга любой информации о персональных потребностях, интересах, финансовом положении или банковской деятельности клиента;
- клиентские данные не использовались для целей, выходящих за пределы разрешенного использования, или вне целей, которые были авторизованы клиентом[92];
- стандарты банка в отношении использования клиентских данных соблюдались при доступе третьих сторон к клиентским данным на основе отношений в рамках заказной обработки.

Ниже приведены дополнительные примеры надежной организации в помощь обеспечению конфиденциальности клиентской информации в рамках осуществления ЭБ.

1. Банкам следует применять необходимые криптографические методы, специальные протоколы или другие средства контроля безопасности в обеспечение конфиденциальности клиентских данных в операциях ЭБ.
2. Банкам следует разработать необходимые процедуры и средства контроля для периодического оценивания своей инфраструктуры обеспечения безопасности клиентов и протоколов, применяемых в операциях ЭБ.
3. Банкам следует убедиться в том, что сторонние провайдеры услуг имеют разработанные политики соблюдения конфиденциальности клиентских данных.

92 В рамках некоторых юрисдикций законы и правила могут не обязывать банки запрашивать разрешение клиента на использование клиентских данных для собственных целей. Однако они могут обязывать банк предоставлять клиенту возможности отмены разрешения банку на обмен такой информацией с третьими сторонами и аффилированными организациями. В других же юрисдикциях клиенты могут обладать правом запрета банку на использование их данных для любых внутренних или внешних целей.

4. Банкам следует обеспечить информирование клиентов, пользующихся услугами ЭБ, о конфиденциальности и сохранности их информации. Такие меры могут включать:
   — информирование клиентов о политике данного банка в части соблюдения конфиденциальности (например, на web-сайте этого банка). Четкое лаконичное изложение положений о конфиденциальности необходимо, чтобы обеспечить уверенность в том, что отдельные клиенты полностью понимают данную политику. Пространные описания законодательных норм, сколь угодно точные, скорее всего не будут прочитаны большинством клиентов;
   — инструкции для клиентов относительно необходимости держать в секрете свои пароли, персональные идентификационные номера и другие банковские и (или) личные данные;
   — предоставление клиентам информации об обеспечении общей безопасности их персональных компьютеров, включая преимущества использования программ защиты от компьютерных вирусов, средств физического контроля доступа и персональных брандмауэров для статичных интернет-соединений.

Принцип 13: Банкам следует иметь эффективные процессы планирования производительности, непрерывности бизнеса и реакции на непредвиденные обстоятельства, чтобы способствовать обеспечению доступности систем и видов обслуживания в части ЭБ.

Для защиты банков от делового, правового и репутационного рисков обслуживание в рамках ЭБ должно предоставляться на основе непрерывности и своевременности в соответствии с ожиданиями клиентов. Поддержание требуемой доступности зависит также от способности резервных систем обеспечивать непрерывность функционирования и парировать атаки типа «Отказ в обслуживании» или другие события, которые потенциально могут вызвать прерывание деловых операций.

Проблема поддержания непрерывной доступности систем и приложений ЭБ может оказаться значительной с учетом возможного

высокого спроса на проведение транзакций, особенно в периоды пиковой нагрузки. Кроме того, высокие ожидания клиентов относительно короткого цикла обработки транзакций и постоянной доступности (24×7) также повысили важность надежного планирования производительности, непрерывности деловых операций и реакции на непредвиденные ситуации. Для обеспечения такой непрерывности обслуживания клиентов в рамках ЭБ, которую они ожидают, банкам необходимо гарантировать, что:

- существующая в настоящий момент производительность СЭБ и ее перспективная масштабируемость анализируются с учетом общей динамики данного рынка электронной коммерции, а также предполагаемого темпа восприимчивости клиентами услуг и видов обслуживания в области ЭБ[93];
- оценки производительности обработки транзакций в рамках ЭБ выполнены, проверены на максимальную нагрузку и периодически пересматриваются;
- имеются в наличии и регулярно проверяются соответствующие планы по поддержанию непрерывности деловых операций и действий при непредвиденных обстоятельствах для критических систем обработки и доведения услуг в рамках ЭБ.

Ниже приведены дополнительные примеры правильной организации планирования производительности, непрерывности деловых операций и действий при непредвиденных обстоятельствах.

1. Следует идентифицировать и критично оценивать все виды обслуживания и прикладные программы, используемые в области ЭБ, включая те, которые предоставляются сторонними провайдерами услуг.
2. Следует осуществлять оценивание рисков для всех критичных видов обслуживания и прикладных программ в части ЭБ, включая потенциальное влияние любых случаев прерывания деловых операций на кредитный, рыночный, правовой, операционный, а также репутационный риски и риск ликвидности для данного банка.

93 Текущую и перспективную производительность критических систем доведения услуг в рамках электронного банкинга следует оценивать на постоянной основе.

3. Следует установить функциональные критерии для каждого критичного вида обслуживания и программного приложения в рамках ЭБ, а также организовать мониторинг уровней обслуживания в сопоставлении с такими критериями. Следует принять должные меры для обеспечения того, чтобы СЭБ могли обрабатывать как малые, так и большие объемы транзакций и чтобы функционирование систем и их производительность согласовывались с предположениями данного банка относительно перспективного развития СЭБ.
4. Следует принять во внимание разрабатываемые альтернативные варианты обработки для управления спросом при достижении СЭБ установленных заранее номинальных показателей производительности.
5. Планы обеспечения непрерывности операций в части ЭБ следует составлять таким образом, чтобы учитывалось все, что возложено на сторонних провайдеров услуг, а также прочие внешние зависимости, связанные с необходимостью применения процедур восстановления работоспособности.
6. В планах реагирования на непредвиденные обстоятельства при осуществлении обслуживания в рамках ЭБ следует определить какие-либо процессы для возобновления или замещения существующих средств обработки в части ЭБ, реконструирования информации в обеспечение выполнения транзакций, а также описать те меры, которые должны быть приняты для восстановления доступности критичных систем и прикладных программ ЭБ в случае прерывания деловых операций.

Принцип 14: Банкам следует разработать должные планы реагирования на случайные происшествия для выявления, учета и минимизации проблем, обусловленных неожиданными событиями, включая внутренние и внешние атаки, которые могут ухудшить обеспечение систем и видов обслуживания в рамках ЭБ.

Эффективные механизмы реагирования на случайные происшествия являются принципиально важными для минимизации операционного, правового и репутационного рисков, обусловливаемых неожиданными событиями, такими как внутренние и внешние

атаки, которые могут оказать влияние на функционирование систем и предоставление услуг ЭБ. Банкам следует разработать соответствующие планы реагирования на случайные происшествия, включая стратегию обеспечения связи, которая гарантирует непрерывность деловых операций, контроль над репутационным риском и ограничивает обязательства, ассоциируемые с прерыванием осуществляемого ими обслуживания в рамках ЭБ, включая те, которые связаны с использованием систем и операций в рамках заказной обработки.

Для обеспечения эффективного реагирования на непредвиденные происшествия банкам следует сформировать:

- планы реагирования на происшествия, описывающие восстановление систем и обслуживания в области ЭБ для различных сценариев, деловых операций и географических зон. Анализ сценариев развития событий должен включать рассмотрение вероятности возникновения риска и его влияния на конкретный банк. СЭБ, которые переданы сторонним провайдерам услуг, должны учитываться в таких планах как неотъемлемая часть;
- механизмы оперативного выявления происшествий или кризисных ситуаций, оценивания их материального эффекта и контроля над репутационным риском, ассоциируемым с любым прерыванием в обслуживании[94];
- стратегию обеспечения связи для адекватного реагирования на внешние проблемы рыночного или информационного характера, которые могут возникнуть в случае нарушений безопасности, онлайновых атак и (или) отказов СЭБ;
- четкий процесс, организованный для уведомления соответствующих регулятивных органов в случае происшествий, связанных с реальным ущербом безопасности или прерыванием работы;
- группу реагирования на происшествия, наделенную полномочиями экстренного реагирования и имеющую

94 Мониторинг «горячей линии» и работы службы обеспечения клиентов, а также регулярный обзор жалоб клиентов могут способствовать выявлению пробелов в информации, обнаруживаемых и регистрируемых средствами обеспечения безопасности, в сопоставлении с реальными случаями вмешательства извне.

достаточную подготовку в части анализа систем выявления/парирования происшествий и оценивания значимости связанных с ними результатов;

- четкую последовательность обязательных действий, охватывающую как внутренние, так и заказные операции, чтобы гарантировать, что осуществляются должные действия, соответствующие значимости происшедшего. Кроме того, следует разработать процедуры распространения сведений и связи, а также учесть информирование СД банка в случае необходимости;
- процесс, гарантирующий, что все имеющие отношение к делу внешние участники, включая клиентов банка, контрагентов и информационные органы, будут правильно и своевременно информированы о реальных прерываниях в операциях ЭБ и о работах по восстановлению данной деятельности;
- процесс для сбора и накопления учитываемых в судебных разбирательствах свидетельств в обеспечение должного последующего анализа любого происшествия в связи с операциями ЭБ, а также для содействия судебному преследованию нарушителей.

4. ВОЗМОЖНЫЕ РИСКИ ПРИ ИСПОЛЬЗОВАНИИ ТЕХНОЛОГИИ ИНТЕРНЕТ-БАНКИНГА[95]

«Безопасные корабли — это вытащенные на берег корабли».

Анахарсис Скифский,
древнегреческий философ

Введение

Понятие «интернет-банкинг» относится к системам, которые позволяют клиентам получать доступ к счетам и общей информации по банковским услугам и видам обслуживания с помощью персонального компьютера или другого «интеллектуального» устройства.

Услуги и обслуживание в рамках интернет-банкинга могут включать оптовые услуги для корпоративных клиентов и розничные услуги для частных клиентов.

В число некоторых примеров оптовых услуг и обслуживания входят:

- управление наличностью;
- электронные переводы;
- автоматические клиринговые операции;
- предъявление счетов к оплате.

В число примеров розничных и фидуциарных услуг входят:

- запрос баланса;
- перевод средств;
- затребование информации о транзакциях;
- предъявление счетов к оплате;

95 Данный раздел подготовлен по материалам специализированной брошюры в составе «Справочника контролера» Управления контролера денежного обращения США (Office of the Comptroller of the Currency, OCC).

- запросы на ссуды;
- инвестиционная деятельность;
- другие виды обслуживания, приносящие доход.

Прочие варианты обслуживания в рамках интернет-банкинга могут включать предоставление доступа к Интернету в качестве провайдера интернет-обслуживания (ISP — Internet Service Provider). Управление контролера денежного обращения США (OCC) установило, что дочерние организации национальных банков могут предоставлять банковские услуги на дому через интернет-соединения с системой домашнего банковского обслуживания конкретного банка и в качестве дополнения к такому обслуживанию могут также предоставлять доступ к интернет-клиентам банка через посредство этого обслуживания (см. OCC Interpretative Letter № 742, так называемое письмо Apollo). Исторически банки использовали технологию информационных систем для обработки чеков (обработка требований), управления банкоматами (обработка транзакций) и подготовки отчетов (информационные системы управления). В прошлом компьютерные системы, составлявшие функциональную основу информационных систем, почти не привлекали внимание клиентов. Сегодня же web-сайты, электронная почта и системы предъявления/оплаты электронных счетов являются важными средствами работы банков со своими клиентами.

Национальные банки экспериментировали с различными формами оперативного удаленного банковского обслуживания (on-line banking) в течение многих лет. Некоторые из первоначальных экспериментов проводились с закрытыми системами, в которых клиенты получали доступ к банку через посредство телефонного набора или кабельного телевизионного соединения. Эти системы ограничивали потенциальную клиентскую базу банка, поскольку для доступа к банку было необходимо, чтобы клиентам, находящимся вне данного региона, приходилось либо оплачивать телефонные счета за удаленные соединения, либо становиться абонентами конкретной системы кабельного телевидения. При общем росте Интернета клиенты могут воспользоваться этой технологией в любом месте мира для того, чтобы получить доступ к сети связи какого-либо банка. Интернет как обеспечивающая технология сделал банковские услуги и обслуживание доступными для большого числа клиентов и устранил барьеры,

обусловленные географическими факторами и правами собственности на системы. При наличии расширенного рынка банки могут иметь возможности распространения или модификации своих услуг и предложений по обслуживанию.

4.1. Развитие интернет-банкинга

Количественные факторы, включая конкурентные затраты, обслуживание клиентов и демографические условия, стимулируют банки к оцениванию используемых технологий и пересмотру своих стратегий в части электронной коммерции и интернет-банкинга. Многие исследователи ожидают быстрого увеличения числа клиентов, использующих банковские услуги и обслуживание в режиме on-line. Сложная задача для банков заключается в том, чтобы убедиться, что выгоды от применения технологии интернет-банкинга превышают потери из-за затрат и рисков, связанных с ведением бизнеса в киберпространстве.

Стратегии маркетинга будут варьироваться по мере стремления национальных банков к расширению своих рынков и задействованию более дешевых каналов доведения услуг. Чтобы оценить риск, менеджерам потребуется понимание применяемых стратегий и используемых технологий на основе сопоставления банков. Оценивание данных по конкретным банкам в части использования их web-сайтов может помочь инспекторам в определении стратегических целей конкретного банка, того, насколько хорошо банк выполняет свой план по предоставлению услуг интернет-банкинга, а также насколько доходным может считаться данный вид бизнеса.

В число ряда рыночных факторов, которые могут определять стратегию того или иного банка, входят следующие:

1. **Конкуренция.** Исследования показывают, что конкурентное давление является движущей силой роста применения технологии интернет-банкинга; двумя другими факторами, вторым и третьим по значимости, являются снижение затрат и повышение рентабельности. Банки рассматривают интернет-банкинг как способ сохранения существующей клиентуры и привлечения в банк новых клиентов.

2. **Эффективность затрат.** Национальные банки могут обеспечить банковское обслуживание через Интернет с гораздо более низкими операционными затратами, чем в рамках традиционных стационарных филиалов. Реальная стоимость проведения транзакций будет варьироваться в зависимости от используемого канала доведения услуги. К примеру, в соответствии с данными, которые приводили Booz, Allen & Hamilton, в середине 1999 г. стоимость ручной обработки транзакции в филиале обычно составляла более доллара, транзакции через банкомат и клиринговые центры стоили около 25 центов, а транзакция через Интернет обходилась в цент (рис. 9). Предполагается, что эти затраты будут снижаться.

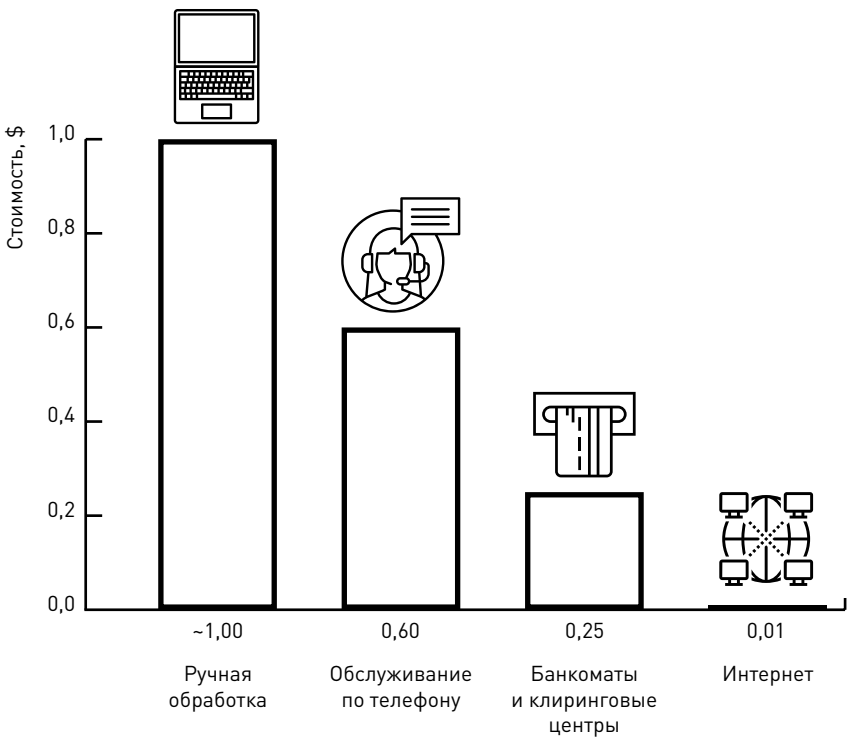

Рис. 9. Изменение затрат на банковские технологии, применяемые для обработки транзакций

Национальные банки имеют весомые причины для разработки технологий, которые помогут им предоставлять банковские услуги и обслуживание по наиболее экономически выгодным каналам. Многие банкиры считают, что перенос только небольшой доли платежей, осуществляемых в США по почте и оцениваемых в 19 млрд долл., на электронные каналы доведения данных мог бы сэкономить банкам и другим организациям значительные суммы денег. Однако национальным банкам следует учитывать при принятии решений собственно разработку и текущую стоимость, связанную с новой услугой или видом обслуживания, включая технологию, маркетинг, сопровождение и функции поддержки клиентов. Это будет способствовать руководству банков в части выполнения обязательств, принятия более обоснованных решений и оценивания успеха своих деловых мероприятий.

3. **Географический охват.** Интернет-банкинг обеспечивает расширение контактов с клиентами за счет увеличения географического охвата и снижения стоимости каналов доведения услуг. Фактически некоторые банки осуществляют свою деятельность исключительно через Интернет — у них нет традиционных банковских офисов и они работают со своими клиентами только в режиме on-line. Другие финансовые учреждения используют Интернет в качестве альтернативного канала для взаимодействия с имеющимися клиентами и привлечения новых.
4. **Торговая марка.** Формирование отношений представляет собой стратегический приоритет для многих национальных банков. Технология и услуги интернет-банкинга могут обеспечить национальным банкам средства для создания и поддержки непрерывных отношений со своими клиентами за счет предоставления легкого доступа к широкому кругу услуг и видов обслуживания.

   За счет акцентирования своей торговой марки и предоставления широкого спектра финансовых услуг банки рассчитывают завоевать преданность клиентов, осуществлять перекрестные продажи услуг и повысить обращаемость за дополнительными услугами.

5. **Демография клиентуры.** Интернет-банкинг позволяет национальным банкам предлагать широкий набор вариантов своим клиентам, осуществляющим банковские деловые операции. Некоторые клиенты будут полагаться при осуществлении своей банковской деятельности на традиционные филиалы. Для многих это наиболее удобный способ осуществления своих банковских деловых операций. Такие клиенты отдают предпочтение межличностным контактам. Другие клиенты относятся к тем, которые рано восприняли новые технологии, появляющиеся на рынках. Эти клиенты были первыми, кто приобрел персональные компьютеры, и первыми, кто стал использовать их для проведения банковских деловых операций. Демография банковской клиентуры будет продолжать меняться. Проблема для национальных банков состоит в понимании своей клиентской базы и поиске правильного сочетания каналов доведения для выгодного предоставления услуг и видов обслуживания на различных сегментах своего рынка.

4.2. Типы интернет-банкинга

Понимание сути различных типов услуг интернет-банкинга будет способствовать оцениванию менеджерами банка сопутствующих им рисков. В настоящее время на рынках используются три основных варианта интернет-банкинга.

Информационный — базовый уровень интернет-банкинга. Как правило, банк при этом дает маркетинговую информацию о банковских услугах и обслуживании на обособленном сервере. Соответствующий риск довольно низок, поскольку информационные системы обычно не имеют непосредственной связи между таким сервером и внутренней вычислительной сетью банка. Этот уровень интернет-банкинга может быть обеспечен как самим банком, так и сторонней организацией. Хотя риск для банка сравнительно невелик, соответствующий сервер или web-сайт может оказаться уязвимым для воздействий. Поэтому следует предусмотреть должные средства

контроля для предотвращения неавторизованных (несанкционированных) воздействий на упомянутый сервер или web-сайт банка.

Коммуникационный — тип системы интернет-банкинга, позволяющий реализовать некоторые виды взаимодействия между системами конкретного банка и его клиентом. Такое взаимодействие может быть ограничено электронной почтой, запросами справок о счетах, заявками на ссуды или обновлением стандартных файлов (изменение имени и адреса). Поскольку соответствующие сервера в этом варианте могут иметь какую-то связь с внутренними вычислительными сетями банка, сопутствующий риск при такой конфигурации выше, чем в случае чисто информационных систем. Требуются должные средства контроля для предотвращения, мониторинга и оповещения руководства о любой попытке неавторизованного доступа к внутренним сетям и компьютерным системам банка. В таких условиях становится существенно более важным вирусный контроль.

Операционный — уровень интернет-банкинга, позволяющий клиентам выполнять транзакции. Поскольку обычно существует непосредственная связь с сервером и внутренней вычислительной сетью банка или обслуживающей его организации, такой архитектуре сопутствует наивысший риск и в ней должны существовать самые серьезные средства контроля. Транзакции клиента могут включать доступ к счетам, осуществление платежей, перевод средств и т. п.

4.3. Риски интернет-банкинга

Интернет-банкинг создает для банков новые проблемы, связанные с контролем над рисками. Риск представляет собой возможность ситуации, когда ожидаемые или непредвиденные события смогут оказать негативное влияние на доходы или капитал конкретного банка. В интересах банковского надзора OCC определило девять категорий риска. Этими рисками являются: кредитный, процентный, ликвидности, ценовой, валютный, операционный, несоответствия, стратегический и репутационный. Данные категории не считаются исчерпывающими, и все перечисленные риски связываются с интернет-банкингом.

4.3.1. Кредитный риск

Кредитный риск — это риск для доходов или капитала, возникающий из-за неспособности лица, принявшего на себя обязательства (должника), выполнить требования какого-либо контракта, заключенного с банком, или действовать в соответствии с какой-то еще договоренностью. Кредитный риск обнаруживается во всех видах деятельности, в которых успех зависит от действий партнера, эмитента или заемщика. Он возникает каждый раз, когда фонды банка распределяются, передаются или иным образом подвергаются опасности через явные или подразумеваемые контрактные соглашения независимо от того, учитываются они на балансе или вне баланса.

Интернет-банкинг предоставляет банку возможность расширения географии своей работы. Клиенты могут работать с данным учреждением практически из любого места в мире. При взаимодействии с клиентами через Интернет, когда отсутствует какой-либо личный контакт, для учреждений возникает проблема верификации (подтверждения) истинности личностей их клиентов, что является важным элементом при принятии правильных решений в части кредитования. Подтверждение залога и выполнение соглашений об обеспечении безопасности также могут оказаться проблемными в случаях работы с удаленными заемщиками. При отсутствии правильного управления интернет-банкинг может привести к концентрации кредитов у таких заемщиков или кредитов в отдельной отрасли производства. Более того, вопрос о том, под контролем юрисдикции какого штата или государства находятся взаимоотношения через Интернет, остается пока в стадии решения.

Эффективное управление кредитным портфелем, организованным через Интернет, требует, чтобы совет директоров и руководство банка осознавали и контролировали профиль риска своего банка в части кредитования и культуру кредитования. Они должны гарантировать наличие эффективной политики, процессов и практики контроля риска, связанного с такими кредитами.

4.3.2. Процентный риск

Процентный риск — это риск для доходов или капитала, возникающий из-за движения процентных ставок. С точки зрения экономической перспективы банк акцентирует свое внимание на чувствительности размера своих активов, обязательств и доходных статей к изменениям в значениях процентных ставок. Процентный риск возникает из различий между моментами изменения ставок и моментами движения средств (риск переоценки), из меняющихся соотношений процентных ставок между разными кривыми доходности, влияющими на деятельность банка (базовый риск), а также из вариантов процентного дохода, заложенных в услугах конкретного банка (опционный риск). При оценивании процентного риска должно рассматриваться влияние стратегии и услуг комплексного неликвидного хеджирования, а также потенциальное влияние, которое окажут на коммерческий доход изменения процентных ставок. В тех случаях, когда трейдинг управляется независимо, это относится к структурным позициям, а не к трейдинговому портфелю.

Интернет-банкинг может способствовать формированию депозитных, кредитных и других отношений с более широким кругом потенциальных клиентов, чем другие формы маркетинга. Расширенный доступ к клиентам, заинтересованным преимущественно в наиболее высоких процентных ставках или сроках, усиливает потребность руководства в поддержании должных систем управления активами/пассивами, включая способность быстрого реагирования на меняющиеся рыночные условия.

4.3.3. Риск ликвидности

Риск ликвидности — это риск для доходов или капитала, обусловленный неспособностью банка выполнять свои обязательства при наступлении соответствующих сроков без неприемлемых для него потерь. Риск ликвидности включает неспособность управлять незапланированными изменениями в источниках финансирования. Риск ликвидности возникает также из-за ошибок в распознавании

изменений рыночных условий, влияющих на способность банка быстро реализовать активы с минимальными потерями в их стоимости.

Интернет-банкинг увеличивает изменчивость в депозитах, поступающих от клиентов, которые держат свои счета только из соображений ставок или сроков. Системы управления активами/пассивами и кредитным портфелем должны соответствовать услугам, предлагаемым в рамках интернет-банкинга. Усиленный мониторинг ликвидности и изменений в депозитах и ссудах может быть оправдан в зависимости от объема и характера действий со счетами через Интернет.

4.3.4. Ценовой риск

Ценовой риск — это риск для доходов или капитала, возникающий из-за изменений в стоимости торговых портфелей финансовых инструментов. Этот риск появляется из рыночных предположений, сделок и позиций, занимаемых на рынках процентных ставок, акций и товаров.

Банки могут оказаться подвержены ценовому риску, если они начинают или расширяют депозитный брокеринг, торговлю кредитами или программу страхования от риска в результате деятельности в рамках интернет-банкинга. Если осуществляется активный трейдинг активов, то следует обеспечивать наличие необходимых систем управления для мониторинга, измерения ценового риска и управления им.

4.3.5. Валютный риск

Валютный риск имеет место, когда некая ссуда или кредитный портфель деноминируется в валюте или финансируется за счет займов в другой валюте. В некоторых случаях банки вовлекаются в мультивалютные кредитные обязательства, которые позволяют заемщикам выбирать ту валюту, которую они предпочитают использовать в каждом периоде пролонгации ссуды. Валютный риск может

увеличиться за счет действия политических, социальных или экономических факторов. Соответствующие последствия могут оказаться неблагоприятными, если обмен одной из используемых валют будет подчинен строгому регулированию или если наблюдаются сильные колебания ее обменного курса.

4.3.6. Операционный риск

Операционный риск является постоянным и перспективным риском для доходов и капитала, обусловленным мошенничеством, ошибками и невозможностью предоставления услуг или видов обслуживания, поддержания конкурентной позиции и управления информацией. Операционный риск явно проявляется в каждой услуге и виде обслуживания, предлагаемых банком, и охватывает организацию услуг и их предоставление, обработку транзакций, разработку систем, компьютерные системы, сложность услуг и обслуживания, а также условия осуществления внутреннего контроля.

Высокий уровень операционного риска может иметь место при оказании услуг интернет-банкинга, особенно если такие направления бизнеса неадекватно спланированы, реализованы и контролируются. Банки, предоставляющие услуги и обслуживание через Интернет, должны быть способны удовлетворять ожиданиям своих клиентов. Банки должны также гарантировать, что им удалось организовать правильное сочетание услуг и что они имеют возможности предоставления полного, своевременного и надежного обслуживания для формирования высокого уровня доверия к своей торговой марке. Клиенты, осуществляющие деловые операции через Интернет, скорее всего не потерпят ошибок или промахов со стороны финансовых учреждений, которые не обладают специализированными средствами внутреннего контроля для управления проведением операций в рамках интернет-банкинга. Подобным образом клиенты ожидают непрерывной доступности конкретной услуги и web-страниц с простой навигацией (ориентацией) по ним.

Программное обеспечение для поддержки различных функций интернет-банкинга поставляется клиентам из разнообразных источников. Банки могут осуществлять поддержку клиентов,

используя затребуемое клиентами или поставляемые банком программное обеспечение браузеров или персональных финансовых помощников (PFM — Personal Financial Manager). Хорошая связь между банками и их клиентами будет способствовать отслеживанию соответствия различных программных продуктов PFM желаниям их пользователей.

Основного внимания заслуживают атаки или попытки проникновения в банковские компьютерные и сетевые системы. Исследования свидетельствуют, что системы более уязвимы к внутренним атакам, чем к внешним, поскольку пользователи внутренних систем обладают знанием этих систем и доступом к ним. Банкам следует иметь надежные средства защиты и обнаружения, чтобы обезопасить свои системы интернет-банкинга от вторжений как изнутри, так и снаружи. Для того чтобы банки могли гарантировать предоставление услуг и обслуживания в случае неблагоприятных обстоятельств, необходимо планирование в части обеспечения непрерывности и возобновления деловых операций. Предоставление услуг интернет-банкинга с использованием устойчивой сети связи может реально облегчить решение этой задачи, поскольку резервные возможности могут быть распространены в широкой географической зоне. К примеру, если основной сервер неработоспособен, то сеть связи могла бы автоматически переадресовывать поток данных на резервный сервер, размещенный в другом месте. При разработке учреждением своих планов по обеспечению непрерывности и возобновлению деловых операций следует рассматривать вопросы безопасности. В ситуациях такого рода средства обеспечения безопасности и внутреннего контроля на резервных позициях должны быть такими же по сложности, как и те, которые имеются на основном месте обработки. Ключевым требованием клиентов будут высокие степени доступности систем, и в соответствии с ними будут, вероятно, различаться степени успеха финансовых учреждений в Интернете.

Национальным банкам, которые предлагают предъявление и оплату счетов, потребуется осуществление клиринга транзакций между самим банком, его клиентами и третьими сторонами. В дополнение к операционному риску ошибки в клиринге могут усугубить репутационный риск, риск ликвидности и кредитный риск.

4.3.7. Риск несоответствия

Риск несоответствия — это риск для доходов или капитала, возникающий из-за нарушений законов, правил, инструкций, предписанной практики или этических стандартов либо не соответствующих им действий. Риск несоответствия возникает также в ситуациях, когда законы или правила, регламентирующие отдельные услуги или действия клиентов банка, оказываются неопределенными или непроверенными. Риск несоответствия подвергает учреждение опасности штрафов, административных денежных взысканий, компенсации ущерба и нарушения контрактов. Риск несоответствия может привести к ухудшению репутации, сокращению льгот, ограничению деловых возможностей, снижению возможностей расширения, а также неполному исполнению договоров. Большинство клиентов интернет-банкинга будут продолжать пользоваться другими каналами доведения банковских услуг. Соответственно, банкам потребуется пояснять, что информация, которую они дают по каналам интернет-банкинга, включая web-сайты, продолжает соответствовать другим каналам предоставления услуг, чтобы гарантировать доведение достоверных и точных сведений до клиентов.

Регулярный мониторинг банковских web-сайтов позволит гарантировать соответствие применяемым законам, правилам и инструкциям[96].

4.3.8. Стратегический риск

Стратегический риск отражает текущее и перспективное влияние на доходы или капитал неправильных деловых решений, несоответствующей реализации решений или недостаточной способности

96 Одним из первых документов Центрального банка Российской Федерации по тематике интернет-банкинга было Письмо Банка России от 3 февраля 2004 г. № 16-Т «О Рекомендациях по информационному содержанию и организации web-сайтов кредитных организаций». В настоящее время действует обновленная версия данного документа — Письмо Банка России от 23 октября 2009 г. № 128-Т «О Рекомендациях по информационному содержанию и организации Web-сайтов кредитных организаций в сети Интернет».

к ответным действиям на изменения в отрасли. Этот риск зависит от совместимости стратегических целей той или иной организации, деловых стратегий, разработанных для достижения этих целей, ресурсов, отведенных для данных целей, и качества реализации стратегий. Ресурсы, требуемые для осуществления деловых стратегий, делятся на материальные и нематериальные. Они включают каналы связи, операционные системы, сети доведения услуг, а также управленческие способности и возможности. Собственные характеристики конкретной организации должны быть оценены в сопоставлении с воздействием экономических, технологических, конкурентных, регулятивных и других внешних факторов.

Руководство банка должно осознать риски, связанные с интернет-банкингом, до принятия решения о разработке конкретного вида деятельности. В некоторых случаях банки могут предлагать новые типы услуг и обслуживания через Интернет. При этом важно, чтобы руководство понимало риски и последствия таких решений. Для поддержки деловых предприятий такого рода необходимы достаточные уровни развития технологий и информационных систем управления. Поскольку многие банки будут конкурировать с финансовыми учреждениями вне их настоящей области деятельности, те организации, которые вовлечены в интернет-банкинг, должны тесно увязывать применяемые технологии и процесс стратегического планирования в конкретном банке.

До внедрения услуги интернет-банкинга руководству следует рассмотреть вопрос, насколько данная услуга и технология согласуются с «материальными» деловыми целями в стратегическом плане банка. Банку следует также оценить, располагает ли он достаточной квалификацией и ресурсами для идентификации, мониторинга и контроля рисков в деловых операциях интернет-банкинга. Процесс планирования и принятия решений следует фокусировать на том, как услуга интернет-банкинга удовлетворяет тем или иным конкретным деловым потребностям, а не на самой услуге как независимой цели. Банковские эксперты в области технологий совместно с маркетинговым и операционным персоналом должны участвовать в данном процессе планирования и принятия решений. Им следует удостовериться в том, что план согласуется с общими деловыми целями своего банка и не выходит за пределы устойчивости банка к риску.

Новые технологии, особенно Интернет, способны быстро внести изменения в конкуренцию. Соответственно, стратегическое видение должно определять тот способ, с помощью которого бизнес через Интернет будет разрабатываться, реализовываться и контролироваться.

4.3.9. Репутационный риск

Репутационный риск представляет собой то текущее и перспективное влияние на доходы и капитал, которое может оказать отрицательное общественное мнение. Он воздействует на способность учреждения устанавливать новые взаимоотношения или предлагать обслуживание либо продолжать обслуживать существующую клиентуру. Данный риск может привести к судебному преследованию учреждения, его финансовым потерям или к сокращению его клиентской базы. Подверженность репутационному риску связана со всей деятельностью организации, в том числе с ответственностью за повышенную осторожность при работе с клиентами и взаимодействии с общественностью.

Репутация банка может пострадать, если он не способен удовлетворить требованиям рынка или обеспечить точное, своевременное обслуживание. Это может выражаться в невозможности адекватно отреагировать на потребности клиентов в кредитах, в применении ненадежных или неэффективных систем доведения услуг, несвоевременном отклике на запросы клиентов или невыполнении норм соблюдения конфиденциальности, которого ожидают клиенты.

Репутации банка может быть нанесен ущерб при обслуживании в рамках интернет-банкинга, если оно плохо организовано или как-то иначе отталкивает клиентов и общественность. Хорошо организованный маркетинг, включая раскрытие информации, является одним из способов обучения потенциальных клиентов и помогает ограничить репутационный риск. Клиенты должны понять, что́ именно они могут обоснованно ожидать от той или иной услуги либо вида обслуживания, а также каким рискам они могут подвергаться и какие выгоды получить в случае использования данной системы. Концепции маркетинга необходимо четко координировать с адекватными заявлениями относительно раскрытия информации.

Банкам не следует рекламировать свою систему интернет-банкинга, основываясь на тех свойствах или параметрах, которыми данная система не обладает. Маркетинговая программа должна представлять продукт честно и точно.

Банкам следует тщательно продумывать представление на своих web-сайтах связей с третьими сторонами. Гипертекстовые связи часто используются для того, чтобы дать возможность клиенту связаться с другими организациями. Такие связи могут означать в глазах пользователя предпочтение именно этим организациям или услугам. Клиентам должно быть ясно, когда они покидают web-сайт банка, что здесь не возникает неясности относительно провайдера конкретных услуг и обслуживания, которые там предлагаются, или относительно применяемых стандартов обеспечения безопасности и конфиденциальности. Подобным образом должно осуществляться представление информации, чтобы клиенты смогли отличить страхуемые услуги от услуг, которые не страхуются.

Банкам необходимо быть уверенными в том, что их планы по обеспечению непрерывности деловых операций учитывают те, которые проводятся в рамках интернет-банкинга. Регулярная проверка плана по обеспечению непрерывности операций, включая стратегии взаимодействия с прессой и общественностью, поможет банку гарантировать, что он способен эффективно и должным образом реагировать на любые негативные проявления со стороны клиентов и средств массовой информации.

4.4. Управление рисками

Банкам следует организовать процесс управления технологическими рисками для того, чтобы они могли идентифицировать, измерять, контролировать свою подверженность технологическому риску и управлять ею. Управление рисками, связанными с новыми технологиями, включает три принципиально важных компонента:

1) процесс планирования использования данной технологии;
2) реализацию этой технологии;
3) средства измерения и мониторинга сопутствующего риска.

Процесс планирования риска является обязанностью СД и ВРБ. Им потребуется обладание квалификацией и знаниями, необходимыми для управления применением их банком технологии интернет-банкинга и связанными с этой технологией рисками. СД должен проверять, утверждать и контролировать проекты, относящиеся к технологии интернет-банкинга, которые могут оказать влияние на профиль риска банка. Его членам следует определить, соответствуют ли применяемые технологии и услуги стратегическим целям банка и удовлетворяют ли они потребностям их рынка. ВРБ следует обладать квалификацией, достаточной для оценивания применяемой технологии и предполагаемого риска. Периодическое независимое оценивание данной технологии интернет-банкинга и услуг аудиторами или консультантами может помочь СД и ВРБ справиться со своими обязанностями.

Реализация технологии является обязанностью руководства. Руководителям банка следует обладать квалификацией, достаточной для эффективного оценивания технологий и услуг интернет-банкинга, выбора правильных сочетаний и контроля над их правильным внедрением. Если сотрудникам банка не хватает опыта для самостоятельного выполнения таких обязанностей, то им следует рассмотреть возможность заключения контракта с тем поставщиком, который специализируется на данном типе бизнеса, или организовать совместную работу с другими провайдерами, обладающими комплексными технологиями и опытом.

Измерение и мониторинг риска являются обязанностями руководства банка. Руководителям банка следует обладать квалификацией, достаточной для эффективной идентификации, измерения, мониторинга и контроля рисков, ассоциируемых с интернет-банкингом. СД банка должен получать регулярные отчеты по применяемым технологиям, предполагаемым рискам и тому, как эти риски управляются. Мониторинг функционирования систем является ключевым фактором успеха. Национальные банки должны включить в свою систему интернет-банкинга эффективные процессы подтверждения качества и аудита как часть процесса разработки. Банкам следует периодически проверять свои системы, чтобы определить, удовлетворяют ли они стандартам функционирования.

4.5. Внутренний контроль

Внутренний контроль над системами интернет-банкинга должен быть соразмерен уровню риска банка. Как и в любой другой области банковского дела, руководство несет итоговую ответственность за разработку и реализацию надежной системы внутреннего контроля над технологией и услугами интернет-банкинга в своем банке.

Регулярный аудит указанных систем контроля поможет гарантировать, что эти средства контроля соответствуют назначению и функционируют должным образом. К примеру, контроль для технологии интернет-банкинга какого-либо банка может быть нацелен:

- на согласование технологического планирования и стратегических целей, включая эффективность и экономичность операций, а также соответствие корпоративной политике и законодательным требованиям;
- доступность данных, включая планирование восстановления деловых операций;
- целостность данных, включая обеспечение защищенности активов, должную авторизацию транзакций, а также надежность соответствующего процесса и результата;
- конфиденциальность данных и защищенность прав личности;
- надежность информационной системы управления.

При наличии установленных целей контроля руководство несет ответственность за внедрение необходимого внутреннего контроля для того, чтобы убедиться, что установленные цели достигаются. Руководство также несет ответственность за оценивание соответствия средств контроля на основе определения экономического эффекта. При этом анализе может учитываться эффективность каждого средства контроля в процессе, денежный эквивалент объема потока средств, задействованных в данном процессе, а также стоимость самих средств контроля.

5. ОРГАНИЗАЦИЯ ВНУТРЕННЕГО АУДИТА И ВНУТРЕННЕГО КОНТРОЛЯ В КРЕДИТНЫХ ОРГАНИЗАЦИЯХ ПРИ ИСПОЛЬЗОВАНИИ СИСТЕМ ЭЛЕКТРОННОГО БАНКИНГА

«Дело должно соответствовать возможностям, действие должно соответствовать времени».

Лао-Цзы (Ли Эр),
древнекитайский философ

В части организации (адаптации) и реализации процессов внутреннего контроля в кредитных организациях, применяющих в своей деятельности технологии ЭБ, целесообразно базироваться не только на общепринятом подходе к процессу управления[97], но и на рекомендациях Базельского комитета по банковскому надзору. В частности, БКБН определяет необходимость принятия четких стратегических решений относительно предоставления банковских услуг посредством электронных технологий, организации процессов должного контроля и мониторинга и парирования рисков.

5.1. Качество корпоративного управления в части развития и применения систем электронного банкинга

5.1.1. Ориентированность кредитной организации на развитие технологий электронного банкинга

В соответствии с рекомендациями Базельского комитета по банковскому надзору «Совершенствование корпоративного управления в кредитных организациях» и другими международными документами

97 Речь идет о подходе, который включает в себя стратегическое и тактическое управление.

по корпоративному управлению, деятельность организации, не имеющей стратегических целей или корпоративных ценностей, крайне затруднена. С учетом отмеченного целесообразной является разработка кредитной организацией стратегии развития, которой она будет руководствоваться в своей повседневной деятельности.

Поскольку СД и ВРБ отвечают за разработку стратегии развития кредитной организации, СД необходимо уделять достаточно времени обсуждению стратегии развития, в том числе на этапе ее утверждения, включая определение приоритетных направлений развития в области технологий ЭБ.

Важным элементом корпоративного управления кредитной организации является установление во внутренних документах порядка разработки, утверждения и при необходимости уточнения (корректировки) стратегии развития ее деятельности (далее — Стратегия развития).

Кредитной организации следует утверждать стратегию развития общим собранием акционеров или СД.

Учитывая рекомендации зарубежных органов банковского надзора, предполагается, что в оптимальном варианте в стратегическом плане кредитной организации излагаются, в том числе, планы внедрения, применения и развития технологий ЭБ, количественные и качественные показатели, позволяющие оценить деятельность кредитной организации в целом, ее отдельных подразделений и служащих и сравнить достигнутые в соответствующем плановом периоде результаты с запланированными показателями.

В целях обеспечения эффективности управления рисками, возникающими при осуществлении кредитной организацией операций с применением СЭБ, органам управления кредитной организации рекомендуется обеспечить соответствие планов внедрения и развития клиентского обслуживания с использованием СЭБ стратегическим целям.

Кредитной организации целесообразно осуществлять контроль за соблюдением сроков реализации мероприятий по развитию ЭБ, предусмотренных в планах по реализации целей, определенных стратегией развития.

В соответствии с рекомендациями БКБН, кредитным организациям перед внедрением технологий ЭБ необходимо осуществлять

предварительный анализ особенностей вновь внедряемых технологий ДБО, оценивать потенциальные факторы риска, связанные с этими технологиями, а также рассматривать альтернативы стратегического развития данного направления деятельности, в том числе наихудший, наилучший и наиболее вероятный варианты развития событий.

При этом возможные последствия решений в области технологий ЭБ необходимо соизмерять с предельно допустимым совокупным уровнем риска, который может принять кредитная организация.

Ошибочные решения органов управления кредитной организации в отношении внедрения, сопровождения и развития СЭБ могут привести к возникновению убытков, причинами которых могут быть:

- высокие затраты на внедрение и сопровождение СЭБ;
- невозможность достижения поставленных кредитной организацией стратегических целей в связи с отсутствием или обеспечением в неполном объеме необходимыми ресурсами (финансовыми, техническими, материальными, человеческими);
- невыполнение организационных мер в области применения технологий ЭБ;
- ошибки в реализации организационно-технических решений при внедрении СЭБ.

Стратегия развития должна предусматривать процедуры своевременного и адекватного реагирования на возможные действия конкурентов кредитной организации или появление новых технологических решений. Отсутствие такого положения может стать причиной потери кредитной организацией своего конкурентного преимущества в данной области и привести к оттоку клиентов, применяющих технологии ЭБ.

При оценке ориентированности кредитной организации на развитие технологий ЭБ необходимо обращать внимание на следующее:

- имеется ли у кредитной организации Стратегия развития?
- установлен ли во внутренних документах кредитной организации порядок разработки, утверждения, уточнения (корректировки) Стратегии развития?
- определены ли в Стратегии вопросы развития ЭБ?

- выполняются ли планы, разработанные кредитной организацией, по развитию ЭБ?
- проводится ли кредитной организацией регулярный мониторинг степени достижения поставленных в Стратегии развития банка целей по развитию ЭБ?
- предусмотрены ли Стратегией развития процедуры своевременного реагирования на возможные действия конкурентов кредитной организации или появление новых технологических решений?

5.1.2. Роль совета директоров кредитной организации в организации внутреннего контроля

Важная роль в создании эффективной системы внутреннего контроля принадлежит СД кредитной организации. Поэтому, с учетом Положения Банка России от 16 декабря 2003 г. № 242-П «Положение о порядке организации внутреннего контроля в кредитных организациях и банковских группах» (далее — Положение № 242-П), к компетенции совета директоров рекомендуется относить вопросы, приведенные в п. 1 Приложения 1 к Положению № 242-П.

С 2014 г. изменились требования Банка России к организации внутреннего контроля в кредитных организациях. В соответствии с новыми подходами, заложенными в разделах 4 и 4(1) Положения № 242-П, выделяются два уровня внутреннего контроля:

1) служба внутреннего аудита (СВА), подотчетная СД банка;
2) служба внутреннего контроля (СВК), подотчетная исполнительному органу кредитной организации.

Основной функцией СВК является выявление комплаенс-риска, то есть риска возникновения у кредитной организации убытков из-за несоблюдения законодательства Российской Федерации, внутренних документов кредитной организации, стандартов саморегулируемых организаций (если такие стандарты или правила являются обязательными для кредитной организации), а также в результате применения санкций и (или) иных мер воздействия со стороны надзорных органов (регуляторный риск). Таким образом, СВК призвана

решать тактические задачи предотвращения возможных рисков банка в помощь менеджерам кредитной организации.

Инструментом контроля за эффективностью действий органов управления банка для акционеров является СВА. К ее функциям, в частности, относятся:

- проверка и оценка эффективности системы внутреннего контроля в целом, выполнения решений органов управления кредитной организации (общего собрания акционеров (участников), СД (наблюдательного совета), исполнительных органов кредитной организации);
- проверка эффективности методологии оценки банковских рисков и процедур управления банковскими рисками, установленных внутренними документами кредитной организации, и полноты применения указанных документов;
- проверка надежности функционирования системы внутреннего контроля за использованием автоматизированных информационных систем;
- проверка процессов и процедур внутреннего контроля.

Таким образом, в целях обеспечения эффективности мониторинга внутреннего контроля в области ЭБ со стороны СД, СВА обязана информировать СД о выявляемых при проведении проверок нарушениях (недостатках) по вопросам применения ЭБ, а также представлять СД информацию о принятых мерах по выполнению рекомендаций и устранению выявленных нарушений в данной области. Для этого СВА разрабатывает планы проведения проверок, которые утверждаются СД.

В СД и СВА целесообразно присутствие специалистов, имеющих образование в области информационных технологий.

При наличии в составе СД специалистов, имеющих образование в области информационных технологий, члены СД могут проверить и оценить соответствие организации и функционирования внутреннего аудита в области ЭБ содержанию деятельности кредитной организации, а также смогут принять обоснованные стратегические решения относительно:

- внедрения в кредитной организации новых технологий ЭБ;
- ведения соответствующей маркетинговой политики;
- определения тарифных планов;

- содержания договоров с клиентами, контрагентами и провайдерами.

Внедрение технологий ЭБ существенно повышает квалификационные требования к высшему руководству кредитной организации. Поэтому сотруднику из состава высшего руководства кредитной организации, в круг ответственности которого входят вопросы организации управления информационными технологиями, рекомендуется проходить периодическую подготовку (переподготовку) по вопросам ДБО и особенностей его применения.

Оценивая роль СД кредитной организации в организации внутреннего контроля, необходимо учитывать следующее:

- предусмотрено ли внутренними документами кредитной организации отнесение к компетенции СД вопросов, приведенных в п. 1 Приложения 1 к Положению № 242-П?
- проводится ли рассмотрение СД вопросов организации внутреннего аудита и внутреннего контроля и мер повышения их эффективности с учетом особенностей деятельности кредитной организации с применением СЭБ?
- принимались ли СД решения (меры) для обеспечения оперативного выполнения исполнительным органом кредитной организации рекомендаций и устранения замечаний СВА по применению СЭБ?
- утверждены ли СД планы проверок СВА?
- предоставляет ли СВА не реже одного раза в год отчет о выполнении плана проверок?
- осуществляется ли информирование СВА совета директоров о выявляемых при проведении проверок нарушениях (недостатках) по вопросам, связанным с применением СЭБ?
- представляет ли СВА совету директоров информацию о принятых мерах по выполнению рекомендаций и устранению выявленных нарушений в области применения СЭБ?
- имеется ли в составе высшего руководства банка куратор по информационным технологиям, получивший образование в области информационных технологий или прошедший специальную переподготовку по данному направлению деятельности?

5.1.3. Общие процедуры организации внутреннего аудита и внутреннего контроля

5.1.3.1. Документарное обеспечение системы внутреннего контроля

В руководствах зарубежных органов банковского регулирования надзора и нормативных актах Банка России особое внимание уделяется качеству документов, которые необходимо разработать в обеспечение банковской деятельности.

В соответствии со статьями 10 и 24 Федерального закона от 2 декабря 1990 г. № 395–1 «О банках и банковской деятельности» в Уставе кредитной организации должны содержаться сведения о системе органов внутреннего контроля, порядке их образования и полномочиях.

Для организации эффективной работы системы внутреннего контроля должны быть утверждены Положение о системе внутреннего контроля, Положение о СВА и Положение о внутреннем контроле.

Положение о СВА должно определять:

- цели и сферу деятельности СВА;
- принципы и методы деятельности СВА, отвечающие требованиям данного Положения;
- статус СВА в организационной структуре кредитной организации, ее задачи, полномочия, права и обязанности, а также взаимоотношения с другими подразделениями кредитной организации, в том числе осуществляющими контрольные функции;
- подчиненность и подотчетность руководителя СВА совету директоров банка;
- обязанность руководителя СВА информировать о выявляемых при проведении проверок нарушениях и недостатках совет директоров, единоличный и коллегиальный исполнительные органы и руководителя структурного подразделения кредитной организации, в котором проводилась проверка;
- обязанность руководителя СВА информировать совет директоров, единоличный и коллегиальный исполнительные органы о всех случаях, которые препятствуют осуществлению СВА своих функций;

- обязанность служащих СВА информировать руководителя СВА о всех случаях, которые препятствуют осуществлению СВА своих функций.

В соответствии с Положением № 242-П кредитная организация обязана обеспечить постоянство деятельности, независимость и беспристрастность СВА, профессиональную компетентность ее руководителя и служащих, создать условия для беспрепятственного и эффективного осуществления СВА своих функций.

СВА должна состоять из служащих, входящих в штат кредитной организации. При этом должна быть обеспечена независимость СВА, то есть должен быть определен порядок, при котором СВА:

- действует под непосредственным контролем СД;
- не осуществляет деятельность, подвергаемую проверкам;
- по собственной инициативе докладывает совету директоров о вопросах, возникающих в ходе осуществления СВА своих функций, и предложениях по их решению, а также раскрывает эту информацию единоличному и коллегиальному исполнительным органам кредитной организации.

Во внутренних документах кредитной организации должны быть предусмотрены:

- подотчетность руководителя СВА совету директоров кредитной организации;
- право руководителя СВА взаимодействовать с соответствующими руководителями кредитной организации (ее подразделений) для оперативного решения вопросов и устанавливать порядок такого взаимодействия;
- невозможность функционального подчинения руководителю (его заместителям) СВА иных подразделений кредитной организации, а также совмещения служащими СВА (включая руководителя и его заместителей) своей деятельности с деятельностью в других подразделениях кредитной организации.

Кредитная организация должна обеспечить беспристрастность СВА, в том числе решение поставленных перед СВА задач без вмешательства со стороны органов управления, подразделений и служащих кредитной организации, не являющихся служащими СВА.

Положение о СВК[98], регулирующее деятельность данного подразделения, утверждается единоличным исполнительным органом кредитной организации. Положение о СВК должно определять:

- цели, функции (права и обязанности) СВК;
- статус СВК в организационной структуре кредитной организации;
- методы деятельности СВК;
- подчиненность и подотчетность руководителя СВК;
- распределение обязанностей между осуществляющими функции СВК служащими (далее — служащие СВК) в структурных подразделениях кредитной организации;
- обязанность руководителя СВК информировать о выявленных нарушениях при управлении регуляторным риском единоличный и коллегиальный исполнительные органы кредитной организации;
- обязанность руководителя СВК незамедлительно информировать единоличный и коллегиальный исполнительные органы кредитной организации о возникновении регуляторного риска, реализация которого может привести к возникновению существенных убытков у кредитной организации;
- обязанность руководителя СВК информировать единоличный и коллегиальный исполнительные органы кредитной организации о всех случаях, которые препятствуют осуществлению ими своих функций;
- обязанность служащих СВК информировать руководителя СВК о всех случаях, которые препятствуют осуществлению ими своих функций.

Перечисленные выше требования могут быть основой для оценки качества документарного обеспечения организации системы внутреннего контроля в кредитной организации.

98 В соответствии с требованиями, изложенными в Положении № 242-П.

5.1.3.2. Особенности подбора кадров в службу внутреннего аудита и службу внутреннего контроля

Кредитной организации следует установить численный состав, структуру и материально-техническую обеспеченность СВА и СВК в соответствии с характером и масштабом осуществляемых операций, уровнем регуляторного риска, принимаемого кредитной организацией.

СВА и СВК должны состоять из служащих, входящих в штат кредитной организации.

Руководитель СВК может являться членом коллегиального исполнительного органа кредитной организации. Если руководитель СВК не является членом коллегиального исполнительного органа кредитной организации, он подотчетен единоличному исполнительному органу кредитной организации (его заместителю, являющемуся членом коллегиального исполнительного органа и не участвующему в принятии решений, связанных с совершением кредитной организацией банковских операций и других сделок).

СВА и СВК осуществляют свои функции в кредитной организации на постоянной основе. Важным условием эффективности системы внутреннего аудита и контроля выступают достаточно высокая профессиональная квалификация и подготовка специалистов кредитной организации, которые участвуют в работе данных служб, поскольку многие недостатки в организации и особенно функционировании системы внутреннего контроля могут быть обусловлены недостаточным вниманием руководства кредитной организации к профессиональному составу служб.

Когда функции СВК исполняются служащими разных структурных подразделений, кредитная организация должна установить распределение обязанностей между указанными структурными подразделениями кредитной организации по осуществлению внутреннего контроля.

Опыт и знания сотрудников СВА и СВК должны позволять им использовать адекватные методы анализа и прогнозирования факторов риска, эффективности операций, проводить оценку процедур принятия решений, используемых в кредитной организации.

Профессиональную подготовку (переподготовку) руководителей и служащих СВА и СВК рекомендуется осуществлять на регулярной основе.

Руководители СВА и СВК должны соответствовать требованиям, установленным Указанием Банка России № 3223-У, и установленным п. 1 ч. 1 статьи 16 Федерального закона от 02.12.1990 № 395–1 «О банках и банковской деятельности» требованиям к деловой репутации.

Лицо при назначении его на должность руководителя СВА или СВК кредитной организации должно соответствовать следующим квалификационным требованиям:

1) иметь высшее юридическое или экономическое образование, а при отсутствии такого образования — иное высшее образование и квалификацию в области управления рисками или внутреннего контроля, аудита;
2) иметь стаж работы не менее одного года в качестве руководителя (его заместителя) подразделения внутреннего контроля, внутреннего аудита или по другим направлениям контроля, осуществления банковских операций, являющихся основными в структуре операций; не менее трех лет в качестве специалиста подразделения кредитной организации по одному из указанных направлений.

С внедрением передовых технологий банковского обслуживания возникает необходимость в пересмотре технологии внутреннего контроля в кредитных организациях и ее адаптации к инновациям в предоставлении банковских услуг. Поэтому целесообразно пересмотреть штатное расписание кредитной организации, включив в состав СВК и СВА сотрудников, удовлетворяющих квалификационным требованиям, позволяющим обеспечивать понимание причин возникновения рисков ЭБ.

Для реализации эффективного внутреннего контроля над операциями, осуществляемыми в рамках ЭБ, сотрудники, занимающиеся вопросами проверок функционирования систем ДБО, должны быть подготовлены на уровне самых квалифицированных специалистов кредитной организации в данной области.

В связи с введением кредитными организациями новых банковских технологий и реализующих их систем необходимо обеспечивать

повышение квалификации специалистов, отвечающих за внутренний аудит и контроль в области применения информационных технологий, и осуществлять на регулярной основе их переподготовку, в том числе в рамках взаимодействия с компаниями — разработчиками программно-информационного обеспечения ЭБ и провайдерами интернет-услуг для кредитных организаций.

Органам управления кредитной организации рекомендуется обеспечить участие во внутреннем контроле служащих СВА и СВК в соответствии с обязанностями, регламентированными должностными инструкциями.

Основываясь на сказанном выше, следует отметить, что в части оценки роли Совета директоров кредитной организации и исполнительных органов управления в организации внутреннего аудита и контроля необходимо обращать внимание на следующие вопросы:

- Имеются ли в кредитной организации документы, определяющие численный состав, структуру и техническую обеспеченность СВА и СВК в соответствии с масштабами деятельности, характером совершаемых банковских операций и применяемых технологий?
- Соответствует ли фактическая численность СВА и СВК штатной численности?
- Вносились ли изменения в штатное расписание СВА и СВК в связи с применением новых банковских технологий и увеличением объемов проводимых операций?
- Определены ли в должностных инструкциях сотрудников СВА и СВК функции контроля за рисками при осуществлении операций ЭБ?
- Укомплектованы ли СВА и СВК служащими, удовлетворяющими квалификационным требованиям, позволяющим обеспечивать решение задач по применению и развитию ЭБ, а также понимание причин возникновения рисков при использовании данного вида ДБО?
- Обучаются ли (проходят переподготовку) сотрудники СВА и СВК, отвечающие за внутренний контроль в области применения информационных технологий (включая тематику ЭБ)?

5.1.3.3. Методологическое обеспечение службы внутреннего аудита и службы внутреннего контроля

Основой для эффективного существования системы внутреннего аудита и контроля являются регламентирующие документы, которые должны содержать достаточно ясное описание порядка проведения конкретных процедур внутреннего аудита и контроля, установление уровней ответственности и разделение обязанностей между подразделениями и сотрудниками кредитной организации, чтобы исключить возможность возникновения конфликта интересов.

Объектом проверок являются любое подразделение и любой служащий кредитной организации. В связи с этим внутренними документами кредитной организации следует предусмотреть порядок планирования работ СВА и СВК.

План проведения проверок должен включать график осуществления проверок, учитывать изменения в системе внутреннего контроля и новые направления деятельности кредитной организации. При подготовке годового плана проверок целесообразно учитывать требования Банка России к работе СВА и СВК, условия договора с внешним аудитором кредитной организации, рекомендации внешних надзорных органов.

При составлении графика осуществления проверок должна учитываться установленная в кредитной организации периодичность проведения проверок по направлениям деятельности структурных подразделений и кредитной организации в целом.

Также внутренними документами кредитной организации рекомендуется регламентировать работу СВА и СВК в части определения порядка организации, проведения, оформления и реализации материалов проверок.

Во внутренних документах кредитной организации рекомендуется отразить, что состав группы для проверки правильности функционирования СЭБ определяется с учетом объема и особенностей деятельности проверяемого подразделения. В случае привлечения к проверке работников других подразделений такое решение должно быть заблаговременно согласовано с их непосредственными руководителями. При выполнении служебных обязанностей в ходе проверок сотрудники (входящие в рабочую группу СВК) подчиняются

только руководителю группы, проводящей проверку (руководителю проверки).

Внутренние документы кредитной организации должны предусматривать разработку отдельной программы проверки каждого направления (вопроса) деятельности кредитной организации в области технологий ЭБ. Данная программа должна содержать цели проверки и определять ключевые банковские риски и механизмы обеспечения полноты и эффективности контроля в области технологий ЭБ. Программа может быть скорректирована в ходе проверки с учетом предложений руководства кредитной организации или же по предложению руководителя рабочей группы.

При оформлении результатов проверок каждому члену рабочей группы рекомендуется подробно документировать свою работу и по каждому из проверяемых вопросов делать заключения. Рабочие материалы по проверке отдельных участков (отчеты) до их включения в общий акт проверяющим целесообразно согласовать с сотрудниками проверяемого подразделения. Отчет с визами члена рабочей группы и сотрудника проверяемого подразделения следует передавать руководителю рабочей группы и хранить в последующем в деле по проверке.

Результаты проверок оформляются общим актом, который подписывается руководителем рабочей группы и руководителем проверяемого подразделения. При наличии разногласий по акту со стороны представителей проверяемого подразделения составляется протокол разногласий, в котором указываются возражения. Протокол разногласий подписывается руководителем подразделения. О наличии разногласий делается пометка в акте рядом с подписью руководителя проверяемого подразделения. О проведенных в период проверки мероприятиях по устранению выявленных нарушений и недостатков в работе делается соответствующая запись в акте.

Отдельно следует выделять повторяющиеся недостатки и нарушения, выявленные в ходе предыдущей проверки.

В целях повышения качества проверок рекомендуется разрабатывать внутренние методики проверки вопросов в разрезе направлений контроля над отдельными областями технологий ЭБ.

Согласно рекомендациям зарубежных органов банковского регулирования и надзора, при применении кредитной организацией технологий ЭБ необходимо/следует разрабатывать методики

проверок по отдельным направлениям ДБО, включая следующие вопросы контроля:

- над подразделениями информационных технологий;
- содержанием и ведением web-сайта, используемого кредитной организацией;
- бухгалтерским учетом операций, совершаемых через Интернет, и отражением соответствующих данных в отчетности кредитной организации;
- функционированием, финансовым состоянием и аппаратно-программным обеспечением провайдеров необходимых кредитной организации услуг;
- поставщиками программного обеспечения СЭБ;
- мероприятиями, осуществляемыми службой обеспечения информационной безопасности кредитной организации.

Перечень основных вопросов, связанных с осуществлением внутреннего контроля, по которым кредитная организация должна принять внутренние документы, предусмотрен Приложением 2 к Положению № 242-П. Основные способы (методы) осуществления проверок СВА, которые следует использовать кредитной организации, предусмотрены Приложением 3 к Положению № 242-П. При этом основными и минимально необходимыми являются следующие вопросы:

- Имеется ли в кредитной организации внутренний документ, определяющий порядок планирования работы СВА и СВК?
- Определен ли во внутреннем документе порядок организации, проведения, оформления и реализации материалов проверок?
- Разработаны ли методики проверки вопросов, связанных с применением кредитной организацией технологий ЭБ?

5.1.3.4. Организация работы службы внутреннего аудита и службы внутреннего контроля с результатами проверок применения технологий электронного банкинга

С учетом требований Положения № 242-П необходимо регламентировать порядок доведения результатов проверок до сведения руководства кредитной организации, что может быть реализовано следующим образом.

Руководитель СВК после анализа результатов проверки и плана мероприятий по устранению выявленных недостатков представляет руководству кредитной организации служебную записку, в которой кратко освещаются состояние дел в проверенном подразделении, принятые меры по устранению вскрытых недостатков. Серьезные упущения и нарушения должны получать в записке исчерпывающее отражение с указанием характера нарушения, его последствий, причин появления, конкретных должностных лиц, в результате действия или бездействия которых они были допущены. В записке излагаются также рекомендации руководству кредитной организации и подразделения, в котором проведена проверка, предложения по совершенствованию внутреннего контроля, предлагаются меры по устранению выявленных недостатков. К записке прилагаются: акт проверки, разработанный план мероприятий, в необходимых случаях — другие документы.

СВА осуществляется контроль за эффективностью принятых подразделениями и органами управления по результатам проверок мер, обеспечивающих снижение уровня выявленных рисков, или документирование принятия руководством подразделения и (или) органами управления решения о приемлемости уровня и сочетания выявленных рисков для кредитной организации.

В кредитной организации должен быть установлен порядок представления не реже одного раза в полгода СВА информации об эффективности организации процедур внутреннего контроля, в том числе об эффективности принятых мер по выполнению рекомендаций и устранению выявленных нарушений совету директоров (наблюдательному совету), единоличному исполнительному органу (его заместителям).

После окончания проверки проверенное подразделение кредитной организации составляет план мероприятий по устранению выявленных недостатков (далее по тексту — план мероприятий) в области ЭБ. В плане мероприятий рекомендуется отражать конкретные действия по устранению выявленных нарушений, при необходимости запланировать обучение сотрудников подразделения, разработку новых (дополнение, изменение действующих) нормативных документов, внесение изменений в действующую технологию работы. В плане необходимо указывать сроки исполнения мероприятий и ответственных за исполнение.

При необходимости проводится деловое совещание с участием всего коллектива проверенного подразделения, где обсуждаются допущенные недостатки, принятые меры по их устранению, причины, по которым недостатки стали возможными, меры, которые необходимо принять для недопущения подобных недостатков, рассматриваются рекомендации управления внутреннего контроля. По результатам обсуждения вносятся изменения, дополнения в план мероприятий.

В соответствии с требованиями Положения № 242-П СВА должен осуществляться контроль за эффективностью принятых подразделениями и органами управления по результатам проверок мер, обеспечивающих снижение уровня выявленных рисков, и кредитная организация должна установить порядок контроля (включая проведение повторных проверок) за принятием мер по устранению выявленных СВК нарушений.

Одним из возможных вариантов реализации СВА выполнения подразделениями кредитной организации плана мероприятий может являться предоставление после окончания проверки подразделением в СВА отчета о выполнении плана мероприятий. В случае невыполнения отдельных мероприятий по объективным причинам подразделению рекомендуется своевременно информировать СВА о ходе выполнения плана до наступления сроков исполнения.

При необходимости руководитель СВА может назначить внеплановую тематическую проверку выполнения подразделением плана мероприятий.

Перечисленные выше мероприятия могут быть использованы для оценки качества работы СВА и СВК (в части функционирования СЭБ), при этом основными и минимально необходимыми являются следующие вопросы:

- Установлен ли порядок доведения результатов проверок до сведения руководства и совета директоров кредитной организации?
- Установлен ли кредитной организацией порядок контроля за выполнением подразделениями мероприятий по результатам проверок в части снижения уровня выявленных рисков?

- Принимаются ли подразделениями меры по результатам проверок в части снижения уровня выявленных рисков в области ЭБ?
- Контролируют ли СВА и СВК выполнение подразделениями мероприятий по результатам проверок вопросов в области ЭБ?
- Проводит ли СВА оценку эффективности принимаемых мер по устранению выявленных нарушений и недостатков?

5.1.4. Организация управления рисками, связанными с использованием системы электронного банкинга

К банковским рискам, связанным с применением СЭБ, относятся: операционный, правовой, стратегический риски, риск потери деловой репутации (репутационный риск) и риск ликвидности.

Распределение подчиненности и подотчетности в рамках управления рисками ЭБ рекомендуется организовывать таким образом, чтобы обеспечить своевременность, полноту и адекватность информирования органов управления кредитной организации:

- о состоянии и характеристиках аппаратно-программного обеспечения СЭБ;
- о выявленных недостатках в функционировании информационного контура ЭБ;
- о связанных с ЭБ 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, и результатах их выполнения.

Хорошей практикой является, когда в кредитной организации назначается ответственное лицо (лица) за реализацию процессов управления рисками ЭБ и их мониторинг.

Целесообразно к этим процессам привлекать структурные подразделения (службы, служащих кредитной организации), прямо или косвенно участвующие в функционировании СЭБ подразделений

или сотрудников, отвечающих за внедрение и применение информационных технологий, за обеспечение информационной безопасности, правовое обеспечение деятельности кредитной организации, ответственного за соблюдение правил внутреннего контроля в целях противодействия легализации (отмыванию) доходов, полученных преступным путем, и финансированию терроризма, за операционную работу с клиентами.

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

Во внутренних документах кредитной организации, связанных с управлением ЭБ и контролем за функционированием реализующих его систем, рекомендуется определить роль органов управления и структурных подразделений кредитной организации:

- в распределении полномочий между органами управления кредитной организации (советом директоров, единоличным и коллегиальным исполнительными органами);
- распределении прав и обязанностей, ответственности, подчиненности и подотчетности структурных подразделений кредитной организации, служащих кредитной организации, в обязанности которых входит выполнение функций в рамках ЭБ и управление связанными с данным видом ДБО рисками;
- реализации учетной политики кредитной организации во внутрибанковских автоматизированных системах с учетом особенностей применения СЭБ;
- определении допустимых уровней банковских рисков, принимаемых кредитной организацией при использовании СЭБ;
- определении порядка информирования органов управления кредитной организации о выявленных источниках (факторах) банковских рисков и принятии мер, обеспечивающих снижение уровня рисков.

В целях создания условий для эффективного управления рисками кредитной организации рекомендуется разработать внутренние документы, в которых необходимо реализовать основные принципы

управления каждым видом риска, в том числе с учетом применения СЭБ. Утверждение внутренних документов по управлению рисками с учетом применения технологий ЭБ необходимо осуществлять совету директоров.

Управление рисками, связанными с применением СЭБ, состоит из выявления, оценки, мониторинга, контроля и (или) минимизации операционного риска. Во внутренних документах кредитной организации рекомендуется определить основные принципы управления рисками:

- методики выявления, оценки и мониторинга рисков;
- основные методы контроля и (или) минимизации рисков (принятие мер по поддержанию риска на уровне, не угрожающем интересам кредиторов и вкладчиков, устойчивости кредитной организации);
- порядок доведения результатов мониторинга до руководства кредитной организации.

Кредитные организации могут разрабатывать методы оценки риска самостоятельно либо использовать методы, принятые в международной банковской практике.

В целях предупреждения возможности повышения уровня рисков рекомендуется проводить мониторинг рисков, связанных с применением ЭБ.

Контроль за функционированием системы управления банковскими рисками рекомендуется осуществлять на постоянной основе в порядке, установленном внутренними документами кредитной организации.

Кредитной организации рекомендуется определять периодичность осуществления мониторинга рисков на основе его существенности для обеспечения непрерывности финансово-хозяйственной деятельности при совершении банковских операций и других сделок кредитной организации.

Обеспечение контроля за своевременной идентификацией, оценкой и принятием мер по минимизации банковских рисков в области технологий ЭБ, а также выработку рекомендаций по минимизации банковских рисков рекомендуется возложить на СВА.

Процедуры оценки рисков возможно разделить на два направления: оперативное и последующее. В рамках оперативного

направления производится регулярная оценка уровня основных рисков. При этом уровень рисков оценивается с использованием тех показателей, расчет которых возможен в текущем режиме. Результаты оценки уровня рисков представляются руководству банка и СВК. Последующая оценка рисков проводится СВА и включает в себя анализ показателей оперативной оценки.

При внедрении новых информационных технологий и модернизации используемых в банковской деятельности методология оценки управления банковскими рисками, а также иные внутренние документы, регламентирующие порядок управления рисками, подлежат пересмотру и внесению соответствующих изменений.

Во внутреннем документе по управлению операционным риском рекомендуется отразить вопросы с учетом рекомендаций, изложенных в Письме Банка России от 24 мая 2005 г. № 76-Т «Об организации управления операционным риском в кредитных организациях».

В соответствии с рекомендациями БКБН кредитной организации следует во внутренних документах по операционному риску в области применения ЭБ предусмотреть следующие организационные вопросы:

- по аутентификации идентичности и авторизации клиентов;
- доказательному подтверждению операций;
- обеспечению целостности данных в транзакциях, записях и информации ЭБ;
- обеспечению должных средств авторизации и полномочий доступа к системам, базам данных и приложений ЭБ;
- организации документирования аудита транзакций ЭБ;
- обеспечению конфиденциальности наиболее значимой банковской и клиентской информации;
- должному раскрытию информации об обслуживании в рамках ЭБ на web-сайтах кредитной организации;
- планированию производительности, непрерывности операций и учету непредвиденных обстоятельств при обеспечении доступности систем и услуг ЭБ;
- планированию мероприятий на случай аварийных ситуаций.

Минимизация операционного риска, связанного с применением СЭБ, предполагает осуществление комплекса мер, направленных на снижение вероятности наступления событий или обстоятельств,

приводящих к операционным убыткам, и (или) на уменьшение (ограничение) размера потенциальных операционных убытков. Методы минимизации операционного риска рекомендуется применять с учетом характера и масштабов деятельности кредитной организации.

В целях обеспечения условий для эффективного выявления операционного риска, а также его оценки кредитной организацией следует вести аналитическую базу данных о понесенных операционных убытках, в которой отражаются сведения об их видах и размерах в разрезе уровней выявления риска, обстоятельств возникновения операционных убытков.

Во внутренних документах рекомендуется установить порядок рассмотрения и расследования фактов операционных убытков и причин их возникновения, периодичность оценки органами управления кредитной организации результатов указанных расследований, а также оценки достигнутого уровня управления операционным риском в кредитной организации.

В целях ограничения операционного риска рекомендуется предусмотреть комплексную систему мер по обеспечению непрерывности финансово-хозяйственной деятельности при совершении банковских операций и других сделок, включая планы действий на случай непредвиденных обстоятельств (планы по обеспечению непрерывности и (или) восстановления финансово-хозяйственной деятельности).

Кредитной организации рекомендуется разработать программу мер, направленную на снижение и минимизацию риска потери ликвидности при использовании технологий ЭБ, включающую, в частности, следующие мероприятия:

- противодействия хищению денежных средств;
- действия по снижению вероятности возникновения сбоев в работе автоматизированных систем кредитной организации (или по принятию мер на случай возникновения таких ситуаций);
- действия по снижению вероятности возникновения сбоев в работе автоматизированных систем провайдеров и других поставщиков услуг (или по принятию мер на случай возникновения таких ситуаций).

Во внутренних документах по управлению правовым риском и риском потери деловой репутации с учетом применения

технологий ЭБ целесообразно учесть рекомендации, изложенные в Письме Банка России от 30 июля 2005 г. № 92-Т «Об организации управления правовым риском и риском потери деловой репутации в кредитных организациях и банковских группах».

Во внутреннем документе по управлению правовым риском в области применения ЭБ рекомендуется предусмотреть процедуры выявления, идентификации и оценки рисков, в том числе по рискам, возникающим по причине:

- несоблюдения требований нормативно-инструктивных документов, регламентирующих банковскую деятельность;
- несовершенства правовой системы;
- несоответствия внутренних документов кредитной организации законодательству Российской Федерации;
- неэффективной организации правовой работы, приводящей к ошибкам в действиях служащих и органов управления кредитной организации при разработке и внедрении новых технологий ЭБ;
- нарушения кредитной организацией условий договоров (включая договоры с клиентами на обслуживание с применением СЭБ и договоры с провайдерами услуг);
- нарушения клиентами кредитной организации условий договоров;
- нарушения провайдерами услуг условий договоров.

В целях снижения риска потери деловой репутации кредитной организации следует предусмотреть процедуры выявления, идентификации и оценки, в том числе:

- с учетом принципа «знай своего клиента»;
- с учетом принципа «знай своего работника»;
- связанные с содержанием и ведением web-сайта кредитной организации;
- связанные с обеспечением защиты конфиденциальности клиентской и банковской информации;
- связанные с обеспечением непрерывности функционирования СЭБ.

Во внутренних документах по управлению стратегическим риском в условиях применения технологий ЭБ рекомендуется отразить вопросы с учетом рекомендаций, изложенных в Письме Банка России

от 13 сентября 2005 г. № 119-Т «О современных подходах к организации корпоративного управления в кредитных организациях».

Кредитным организациям, предполагающим оказание клиентам трансграничных банковских услуг посредством технологий ЭБ, рекомендуется предварительно изучить возможные дополнительные источники (факторы) банковских рисков, связанные с нарушением законодательства зарубежных государств, а также возможности учета факторов риска, относящихся к той или иной стране или юрисдикции.

5.2. Организация (адаптация) процедур внутреннего аудита и контроля в части системы электронного банкинга

Относительно рекомендаций об организации (адаптации) процедур внутреннего аудита и контроля в части использования технологий ЭБ необходимо учитывать, что они основываются на рекомендации БКБН о непригодности «единого» подхода к решению вопросов управления рисками в области ЭБ по причине специфичности архитектуры внутрибанковских распределенных компьютерных систем, а соответственно, и профиля сопутствующих рисков для каждой кредитной организации, методов и средств внутреннего контроля.

Существенной необходимостью для кредитных организаций является самостоятельный индивидуальный учет всех особенностей реализации своих или приобретенных ими и интегрированных в уже имеющиеся банковские автоматизированные системы программно-аппаратных комплексов ЭБ.

Применительно же к большинству кредитных организаций обобщенное описание совокупности процедур внутреннего контроля должно учитывать основные особенности, возникающие в содержании и выполнении функций внутреннего контроля в кредитной организации, применяющей технологии ЭБ.

Такая обобщенная реализация (адаптация) процедур внутреннего контроля может базироваться на модели непрерывного

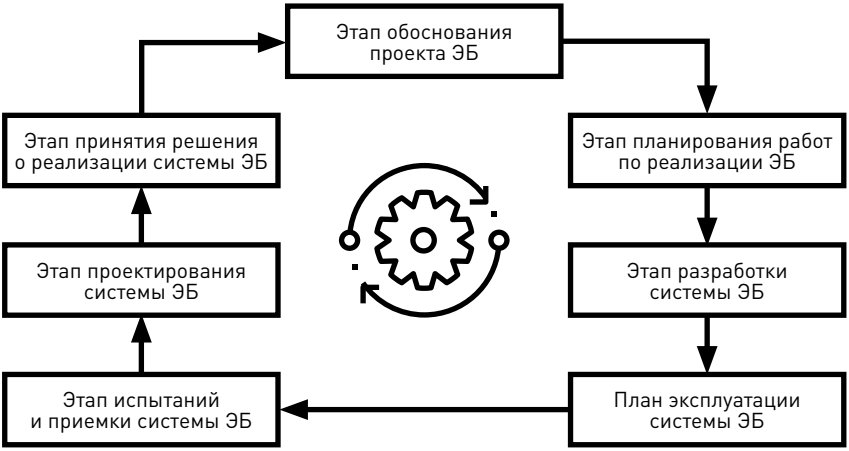

Рис. 10. Жизненный цикл системы ЭБ

циклического процесса менеджмента (модели Деминга)[99] и предполагать детализацию стадий модели этапами жизненного цикла системы ЭБ, часто выделяемыми при разработке и использовании таких систем. Составляющие комплекса процедур внутреннего контроля могут быть реализованы на следующих этапах жизненного цикла системы ЭБ:

- этап обоснования проекта системы ЭБ;
- этап принятия решения о новом проекте системы ЭБ;
- этап планирования реализации системы ЭБ;
- этап проектирования системы ЭБ;
- этап разработки системы ЭБ;
- этап испытаний, сдачи и приемки в эксплуатацию системы ЭБ;
- этап эксплуатации системы ЭБ;
- этап вывода из эксплуатации системы ЭБ.

Подразумевается, что доработка и модификация системы ЭБ должны осуществляться после обоснования соответствующего проекта, в связи с чем в жизненном цикле не выделяется отдельный

99 Стандарт Банка России «Обеспечение информационной безопасности организаций банковской системы Российской Федерации. Общие положения» СТО БР ИББС-1.0–2014.

этап, а предполагается осуществление соответствующих действий и процедур в ходе описанного выше жизненного цикла.

Специфика адаптации процедур внутреннего аудита и контроля к условиям эксплуатации систем ЭБ в кредитных организациях должна обеспечивать непрерывность процесса внутреннего контроля на всех участках информационного контура системы ЭБ, во всех задействованных в работе системы ЭБ структурных подразделениях кредитной организации, а также должна охватывать ее взаимодействие с:

- клиентами (как с юридическими, так и с физическими лицами), использующими системы ЭБ;
- контрагентами, к которым могут быть отнесены провайдеры (организации, предоставляющие кредитным организациям услуги по выполнению функций обработки, передачи, хранения банковской и другой информации, а также обеспечивающие доступ к информационно-телекоммуникационным сетям), поставщики программного обеспечения и оборудования, задействованного в информационном контуре системы ЭБ, а также другие сторонние организации, например, обеспечивающие консультационные услуги в части ЭБ, ремонтно-настроечные услуги модулей или системы ЭБ, продвигающие услуги кредитной организации в форме ЭБ на рынке банковских услуг среди юридических лиц и населения посредством специализированных маркетинговых пиар-акций и программ.

С другой стороны, все указанные особенности внутреннего аудита и контроля должны распределять его процедуры по соответствующим этапам жизненного цикла системы ЭБ.

5.2.1. Организация процедур внутреннего аудита и контроля на этапе обоснования нового проекта системы электронного банкинга

Содержание этапа обоснования нового проекта системы ЭБ, как и любой другой электронной технологии, заключается в осознании экономической целесообразности реализации определенных, уже существующих или планируемых функций, услуг кредитной организации посредством технологии ДБО.

В основе осознания целесообразности могут лежать:

- очевидное снижение затрат на осуществление соответствующих банковских операций;
- экономия времени кредитной организации на обработку внутренних документов и документов клиентов;
- расширение числа потенциальных клиентов за счет преодоления географических ограничений и связанного с этим снижения затрат на открытие филиалов и дополнительных офисов, представительств кредитной организации;
- дополнительная самореклама, продвижение индивидуальных преимуществ кредитной организации.

С организационной точки зрения должен быть четко определен инициатор или группа инициаторов (коллегиальный инициатор) внедрения в практику кредитной организации систем ЭБ, состоящая из конечного числа специалистов или структурных подразделений.

Инициатор в данном случае должен выступать в роли заказчика системы ЭБ и выполнять соответствующие функции на всех последующих этапах вплоть до приема данной системы в эксплуатацию.

Функции заказчика на первоначальном этапе заключаются в формализации данной идеи в виде документарно оформленной заявки на разработку системы ЭБ.

Заявка не является детализированным заданием на разработку, которое должно быть подготовлено на последующих этапах, а представляет собой краткое обоснованное изложение необходимости разработки или приобретения системы ЭБ.

Заявка должна отражать основные цели реализации такой системы, определять круг задач, решение которых может быть более эффективным с использованием системы, и иметь краткое экономическое, функциональное и технологическое обоснование.

Обоснование является исходным материалом, необходимым для принятия решения соответствующим полномочным органом кредитной организации относительно целесообразности реализации системы ЭБ, и поэтому должно по возможности всесторонне отражать все аспекты нововведения.

Если экономическое и функциональное обоснование составляется «заказчиком» системы, то технологическое обоснование является приложением к заявке и составляется структурным подразделением

кредитной организации, ответственным за эксплуатацию информационных систем.

В случае отсутствия такого специализированного подразделения в кредитной организации технологическое обоснование может сформировать специально созданная для данной цели рабочая группа из числа специалистов различных подразделений кредитной организации по направлению автоматизации деятельности.

Важным с точки зрения исключения конфликта интересов также является нормативное закрепление за таким подразделением функции экспертизы подобных заявок на развитие информационных систем и подготовку технологического обоснования.

Итоговое обоснование должно отражать различные аспекты возможного применения ЭБ, в том числе такие, как:

- оценка возможности (технологичности и удобства) интеграции с действующими автоматизированными системами. При этом необходимо оценивать такие возможности с учетом планов развития действующих в банке автоматизированных систем — их доработки, замены и т. д. В противном случае обоснование может оказаться объективным на конкретный момент времени и недостоверным на ближайшие последующие периоды, что может привести к стратегически неверным решениям руководства кредитной организации на следующем этапе — этапе принятия решения о новом проекте системы ЭБ;
- вопросы адекватной организации распределения информационных ресурсов, определения круга подразделений, которые могут быть задействованы в реализации и последующей эксплуатации системы ЭБ, сопоставление с имеющимися штатными ресурсами, организационной структурой кредитной организации. Необходимо также оценить основные роли и распределение прав доступа с точки зрения соответствия действующей в кредитной организации Политики информационной безопасности (ПИБ) и т. д.;
- оценка стоимости разработки, внедрения и сопровождения СЭБ. При этом следует учитывать, что СЭБ может быть приобретена у сторонней организации-разработчика или поставщика, представляющего интересы разработчика, как

целиком, так и в виде отдельных модулей и технических средств либо разработана кредитной организацией (при этом приобретается только соответствующее оборудование). В последнем случае дополнительные затраты могут вызвать расширение штатной численности специалистов подразделения автоматизации. В обосновании может быть также отражена информация об объеме затрат, связанных с модернизацией СЭБ и т. д.;

- оценка трудоемкости и сроков исполнения всех работ, связанных с разработкой (закупкой) и внедрением СЭБ. Такая оценка должна основываться на штатном расписании кредитной организации, принятых нормах и внутренних правилах осуществления подобных работ;
- общий перечень рисков и их источников, с которыми может столкнуться кредитная организация, используя СЭБ, и которым необходимо будет уделять внимание на всех этапах жизненного цикла;
- оценка информационной безопасности.

Обоснование проекта СЭБ должно представлять собой документ общего характера, не предполагающий глубокой детализации всех рассматриваемых аспектов. Вместе с тем информация, изложенная в данном документе, должна быть достаточной для объективного, взвешенного принятия решения.

После составления заявки и обоснования по проекту документы визируются руководителем подразделения-заказчика или группой руководителей соответствующих подразделений.

Все отмеченные аспекты являются основой для оценки качества организации этапа обоснования нового проекта СЭБ службами внутреннего аудита и контроля. При этом основными и минимально необходимыми являются следующие вопросы:

- Начинается ли процедура принятия решения о внедрении нового проекта (модернизации) СЭБ с формирования подразделением-заказчиком документарно оформленной заявки на разработку (доработку) СЭБ?
- Наделено ли подразделение информатизации (или иное подразделение) функциями анализа поступивших заявок

и подготовки обоснования по проекту или иного аналитического документа по итогам рассмотрения заявки?

- Производится ли ответственным подразделением (специалистом) анализ заявки (и отражается ли в обосновании по проекту) в части необходимости реализации нового проекта? В том числе с точки зрения:
  - — технологичности и удобства эксплуатации готового решения;
  - — информационной безопасности, необходимости и достаточности прав доступа для пользователей потенциальной разработки;
  - — стоимости внедрения и сопровождения;
  - — трудоемкости, сроков реализации и внедрения;
  - — выявления и парирования источников внутренних и внешних рисков, сопутствующих внедрению и эксплуатации проекта.
- Согласуется ли документ «Обоснование по проекту» с руководителями подразделения информатизации и подразделения-заказчика?

5.2.2. Организация процедур внутреннего контроля на этапе принятия решения о новом проекте системы электронного банкинга

Содержание данного этапа предполагает детализированный анализ всей информации, подготовленной на этапе обоснования нового проекта системы ЭБ с целью принятия взвешенного, объективного стратегического решения о целесообразности реализации системы.

С точки зрения достижения объективности и обеспечения всестороннего анализа необходимости внедрения и использования кредитной организацией системы ЭБ видится целесообразным организация коллективного совещательного органа — так называемого комитета по технологиям, функциональное назначение которого заключается в анализе такого массива информации (заявки и обоснования по проекту) и принятия соответствующего решения.

Комитет по технологиям или иной коллегиальный орган с обозначенными функциями может быть сформирован решением СД (наблюдательного совета) на постоянной основе либо формироваться избирательно (в зависимости от масштаба рассматриваемого вопроса) на временной основе.

И в том и в другом случае решение о формировании комитета по технологиям закрепляется документарно.

В состав комитета по технологиям могут входить следующие специалисты:

- представители подразделения автоматизации;
- представители подразделения информационной безопасности;
- представители подразделения управления банковскими рисками;
- представители юридической службы;
- представители СВА и СВК;
- представитель или представители коллегиального органа управления кредитной организацией (правления).

Исходя из основной функции комитета по технологиям (выработка коллективного решения рекомендательного характера о целесообразности внедрения и эксплуатации той или иной автоматизированной системы или о ее значительной доработке) хорошей практикой является формирование этого органа из числа руководителей соответствующих подразделений.

Обязанности по координации деятельности комитета по технологиям возлагаются на представителя коллегиального органа управления кредитной организацией. При этом предполагается, что такой член правления кредитной организации обладает знаниями и навыками (обладает соответствующим образованием или имеет опыт руководящей работы) в области построения и эксплуатации распределенных компьютерных систем, программного и аппаратного обеспечения.

В соответствии с рекомендациями БКБН в составе коллегиального органа управления кредитной организации на такого руководителя могут быть возложены функции координации работы подразделений автоматизации, то есть функции куратора по информационным технологиям.

Предполагается, что деятельность комитета по технологиям регламентируется внутренним банковским документом, который определяет порядок проведения заседаний комитета по технологиям и содержит следующие данные:

- численный и персональный состав комитета по технологиям;
- периодичность проведения заседаний;
- круг рассматриваемых вопросов;
- распределение ответственности между членами комитета по технологиям;
- порядок взаимодействия со структурными подразделениями кредитной организации;
- порядок взаимодействия со сторонними организациями (оказывающими консультационные и аудиторские услуги);
- порядок ознакомления членов комитета по технологиям с заявкой на проект разработки (доработки) и внедрения в эксплуатацию автоматизированных систем, в том числе системы ЭБ;
- порядок ознакомления членов комитета по технологиям с экономическим и технологическим обоснованием на проект разработки (доработки) и внедрения в эксплуатацию автоматизированных систем, в том числе СЭБ;
- порядок и форма оформления результатов рассмотрения вопросов, входящих в компетенцию комитета по технологиям.

Проведения заседаний комитета по технологиям должны быть своевременными, а также обеспечивать объективность и полноту анализа рассматриваемых его членами вопросов. Одним из возможных вариантов может быть разработка отдельного графика работы комитета по технологиям, согласующегося с планами перспективного развития автоматизированных технологий в кредитной организации, планами работы основных подразделений.

Круг рассматриваемых вопросов комитета по технологиям должен позволять осуществлять полноценный анализ заявки на разработку (доработку). К числу таких вопросов должны относиться:

- вопросы планирования развития автоматизированных систем кредитной организации;
- вопросы сопряжения и взаимодействия различных автоматизированных систем кредитной организации;

- вопросы экономического анализа работы комплекса автоматизированных систем кредитной организации, в том числе СЭБ;
- вопросы анализа и оценки процессов, работ, трудовых ресурсов требуемой для реализации планируемой автоматизированной системы организации;
- вопросы информационной безопасности использования автоматизированных систем во взаимодействии между собой;
- вопросы оценки потенциальных рисков, связанных с возможной эксплуатацией системы ЭБ и других автоматизированных систем, с учетом их взаимодействия с внутренней и внешней средой кредитной организации.

В целях обеспечения полноценной работы комитета по технологиям все его члены предварительно должны быть ознакомлены с заявкой на разработку (доработку) и эксплуатацию СЭБ, а также с экономическим и технологическим обоснованиями проекта.

Одним из вариантов документарного оформления ознакомления может быть собственноручная подпись члена комитета по технологиям на документе.

После ознакомления с заявкой и обоснованием по проекту комитет по технологиям приступает к обсуждению проекта СЭБ.

В случае необходимости обсуждения значительного числа вопросов, требующих глубокого изучения, например, при обсуждении нового проекта СЭБ, членами комитета по технологиям, в соответствии с распределением полномочий и ответственности, подготавливаются краткие заключения, содержащие основные выводы по каждому направлению и варианту реализации СЭБ.

Заседание комитета по технологиям протоколируется.

В протоколе также отражаются принятые решения относительно целесообразности разработки (приобретения) и эксплуатации системы ЭБ, о варианте ее реализации.

Протокол визируется всеми членами комитета по технологиям, принимавшими участие в заседании, и утверждается куратором по информационным технологиям.

Все отмеченные выше аспекты деятельности кредитной организации являются основой для оценки качества организации этапа принятия решения о новом проекте СЭБ службами внутреннего

аудита и контроля. При этом основными и минимально необходимыми являются следующие вопросы:

- Предусмотрен ли в кредитной организации коллегиальный или иной орган, ответственный за рассмотрение заявок на новые разработки (доработки) и за решение вопроса о необходимости реализации нового проекта (например, комитет по технологиям банка)?
- Входит ли в состав комитета по технологиям банка:
  - куратор по информационным технологиям;
  - представитель подразделения информационной безопасности?
- Разработан ли и утвержден документ (регламент комитета по технологиям), регламентирующий порядок проведения совещаний комитета по технологиям банка?
- Предусмотрено ли регламентом комитета по технологиям ознакомление с заявкой и обоснованием на проект?
- Предусмотрена ли регламентом комитета по технологиям оценка необходимости реализации проекта с учетом приоритетов, определенных в Стратегии по внедрению информационных технологий (или стратегическом плане по информационным технологиям) банка?
- Предусмотрена ли регламентом комитета по технологиям оценка вариантов реализации проекта с учетом:
  - анализа технологичности и удобства эксплуатации готового решения;
  - анализа интегрируемости с информационной системой банка;
  - анализа информационной безопасности;
  - анализа стоимости внедрения и сопровождения;
  - анализа трудоемкости, сроков реализации и внедрения;
  - анализа выявления и парирования источников внутренних и внешних рисков, сопутствующих внедрению и эксплуатации проекта?

5.2.3. Организация (адаптация) процедур внутреннего аудита и контроля на этапе планирования реализации системы электронного банкинга

Содержание этапа планирования реализации СЭБ предполагает проработку системы планов и распределения обязанностей между отдельными структурными подразделениями или сотрудниками, задействованными в разработке (приобретении) и эксплуатации СЭБ.

План разработки (приобретения) СЭБ должен представлять собой общий документ, содержащий описание основных процедур, распределение сроков исполнения и ответственности.

Проект плана разработки (приобретения) СЭБ обсуждается членами комитета по технологиям, по результатам обсуждения в план вносятся необходимые корректировки, он одобряется комитетом по технологиям и утверждается куратором по ИТ.

Общий план разработки (приобретения) СЭБ должен доводиться до руководителей всех задействованных в плане подразделений и соответствующих специалистов данных подразделений.

В связи с тем что разработка (приобретение отдельных модулей) СЭБ представляет сложный многозадачный последовательный процесс, требующий согласованности с существующими бизнес-процессами в кредитной организации, с архитектурой ее внутренних распределенных автоматизированных систем, целесообразным является включение пунктов, представляющих собой отчетные или контрольные мероприятия.

Включение таких контрольных точек позволит руководству кредитной организации, СВК и другим заинтересованным подразделениям осуществлять контроль исполнения плана и при необходимости своевременно вносить изменения в те или иные мероприятия.

Включение контрольных точек в план следует производить таким образом, чтобы они позволяли выделять и объединять функционально и технологически связанные между собой виды работ в группы, поддающиеся автономному анализу или тестированию с целью контроля качества их исполнения.

Например, включение в план непосредственно разработки системы ЭБ позволит осуществлять тестирование отдельных модулей программного обеспечения и комплексов аппаратного обеспечения

значительно раньше этапа контрольных испытаний системы ЭБ, что даст возможность выявить часть источников рисков, заложенных на первоначальных этапах, и вовремя устранить их.

Немаловажным является детальное распределение ответственности по исполнению плана работ. Такое распределение ответственности может содержаться в плане работ в форме отдельного документа либо в форме совокупности распорядительных документов.

Подготовка распределения ответственности возлагается на комитет по технологиям. При подготовке должны учитываться функции задействованных подразделений и обязанности их сотрудников, отраженные во внутренних документах кредитной организации, текущие планы деятельности данных подразделений и другие факторы, влияющие на текущую деятельность подразделений.

Распределение должно включать в себя, в частности, перечень подразделений или сотрудников кредитной организации, ответственных:

- за разработку описания комплекса требований (бизнес-требований) к программному обеспечению в рамках СЭБ;
- разработку технопроектной документации к программному и аппаратному обеспечению СЭБ;
- разработку технорабочей документации к программному и аппаратному обеспечению СЭБ;
- разработку программного обеспечения в рамках СЭБ;
- проведение конъюнктурного анализа и приобретение у сторонних организаций-разработчиков программного обеспечения в рамках СЭБ;
- организацию и проведение контрольных испытаний, периодического тестирования, мониторинг возникающих ошибок и сбоев СЭБ;
- сопровождение СЭБ.

Все отмеченные мероприятия являются основой для оценки качества организации этапа планирования реализации СЭБ службами внутреннего аудита и контроля. При этом основными и минимально необходимыми являются следующие вопросы:

- Утвержден ли план разработки, внедрения и эксплуатации новой разработки СЭБ?

- Утвержден ли приказ, распоряжение или иной документ «Распределение ответственности по проекту»?
- Определены ли ответственные за разработку описания комплекса требований (бизнес-требований) к программному обеспечению системы?
- Определены ли ответственные за разработку технорабочей документации к программному обеспечению в рамках СЭБ?
- Определены ли ответственные за разработку программного обеспечения СЭБ?
- Определены ли ответственные за проведение конъюнктурного анализа и приобретение у сторонних организаций-разработчиков программного обеспечения в рамках СЭБ?
- Определены ли ответственные за организацию и проведение контрольных испытаний, периодического тестирования, мониторинг возникающих ошибок и сбоев СЭБ?
- Определены ли ответственные за сопровождение СЭБ?

5.2.4. Организация (адаптация) процедур внутреннего аудита и контроля на этапе проектирования системы электронного банкинга

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

Учитывая, что система ЭБ 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 во взаимосвязи между собой по мере развития системы. В противном случае внесение изменений в отдельные документы

может привести к возникновению противоречий с положениями, отраженными в других документах.

В целях систематизации документарного обеспечения СЭБ должен быть разработан перечень необходимой проектной и рабочей документации[100] на СЭБ.

Перечень проектной документации на систему ЭБ 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 ЭБ.

Описание постановки комплекса задач может включать в себя следующее:

- информацию об основании разработки СЭБ — указывается документ (документы), на основе которого планируется разработка, орган или ответственное лицо кредитной организации, утвердивший данный документ;
- информацию о функциональном назначении предполагаемой системы или модуля СЭБ;
- в основной части документа должны быть отражены требования к системе или модулю СЭБ. 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 информации задействованных подразделений и функциональных узлов кредитной организации;
- также должны быть кратко описаны условия эксплуатации СЭБ, в том числе приведено количество клиентов, предполагаемое к подключению к работе с СЭБ на момент ввода ее

100 См. ГОСТ 34.003–90.

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, использующимся в деятельности кредитной организации, и т. д.

Описание постановки комплекса задач является основным проектным документом СЭБ, отражающим требования к информационному и функциональному контурам 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 СЭБ, 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 СЭБ на реализацию процедур и средств информационной безопасности в рамках информационного контура.

Документ содержит:

- перечень критически важной информации, обрабатываемой и генерируемой в среде СЭБ;
- перечень технических средств обеспечения информационной безопасности информационного контура СЭБ;
- описание организационных процедур обеспечения информационной безопасности;
- описание технологических средств и систем защиты и обеспечения целостности информации, варианты их сопряжения и функционирования в информационном контуре СЭБ;

- механизм организации парольной защиты, администрирования и систематизации данной работы;
- механизм реализации антивирусной защиты СЭБ.

Приложением к данному документу могут выступать:

- детальное распределение прав и обязанностей внутрибанковских пользователей СЭБ;
- 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 СЭБ, доступных как для клиентов кредитной организации в процессе их работы с программным комплексом, так и для внутренних пользователей, задействованных функционально в информационном контуре СЭБ. Документ содержит точное визуальное графическое отображение выходных форм 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 ввиду, как правило, сложной архитектуры внутрибанковских автоматизированных систем и необходимости описания правил и технологических решений по их взаимодействию между собой.

Интегрирование СЭБ 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 СЭБ;
- перечень аппаратных ресурсов информационного контура СЭБ, используемых в целях взаимодействия с другими внутрибанковскими автоматизированными системами;
- выбор (разработка) формата файлов для обмена данными СЭБ 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 СЭБ.

Помимо состава оборудования указываются:

- описание необходимых настроек аппаратных средств;
- описание условий эксплуатации каждого средства;
- описание вариантов проверки работоспособности средства.

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

6. Обобщающим проектным документом является **Схема функциональной структуры информационного контура СЭБ.** 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, при помощи которых программные и аппаратные средства взаимодействуют между собой.

Такой документ должен содержать информацию:

- о технологическом решении вычислительной сети, на которой основывается СЭБ. При этом в случае наличия альтер-

нативных вариантов взаимодействия элементов информационного контура такие варианты должны быть отражены и описаны;

- об аппаратных и программных средствах на стороне кредитной организации;
- об аппаратных и программных средствах на стороне клиента кредитной организации;
- об аппаратных и программных средствах 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 т. д.);
- о маршрутах прохождения информации при взаимодействии клиента и кредитной организации, об этапах ее преобразования, обработки и контроля.

Кроме данной информации позитивным является наличие общего описания внешнего информационного контура кредитной организации, в котором выделены участки взаимодействия непосредственно с информационным контуром СЭБ.

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 СЭБ, 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 СЭБ.

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 внутреннего аудита и внутреннего контроля на этапе проектирования СЭБ. При этом основными и минимально необходимыми являются следующие вопросы:

- Разработан ли перечень необходимой проектной документации?
- Разработаны ли следующие или подобные документы:
  - описание постановки комплекса задач;
  - описание системы защиты;
  - альбом выходных форм;
  - описание технологии взаимодействия с банковской автоматизированной системой;
  - описание комплекса технических средств;
  - схема функциональной структуры информационного контура СЭБ?
- Разработаны ли иные документы, предусмотренные перечнем проектной документации?

5.2.5. Организация (адаптация) процедур внутреннего аудита и контроля на этапе разработки системы электронного банкинга

На данном этапе производится непосредственно разработка системы ЭБ. Подразумевается:

- 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. Разрабатывается или приобретается: 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 т. д.;

- разработка (монтаж) сегментов электронной вычислительной сети, являющихся частью информационного контура СЭБ, в соответствии с подготовленной 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 т. д.;
- разработка необходимой эксплуатационной документации;
- разработка необходимой внутренней документации, регламентирующей обеспечение информационной безопасности и непрерывности функционирования СЭБ;
- заключение договоров (контрактов) с контрагентами — поставщиками программного обеспечения и оборудования для информационного контура СЭБ;
- заключение договоров (контрактов) с провайдерами на предоставление услуг связи;
- разработка типовых договоров с клиентами на обслуживание посредством СЭБ.

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

К числу аспектов, которым следует уделять внимание, относится наличие в договоре (контракте) с поставщиком описания программного и аппаратного обеспечения СЭБ, положения о сопровождении поставляемого программного обеспечения или иных технических 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:

- 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 конфиденциальности информации.

Следует отметить, что содержание документов, регламентирующих порядок взаимодействия кредитной организации и провайдеров по вопросам обеспечения информационной безопасности и конфиденциальности информации, 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 СВК 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 СВК или Службы информационной безопасности (СИБ) к актам или другим документам, подготовленным аудиторами.

Позитивным является наличие у организации-провайдера собственных СВК и СИБ 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 СВК и СИБ, 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 ЭБ.

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

- общий мониторинг источников рисков, связанных с деятельностью организации-провайдера;
- оценка и мониторинг финансового состояния провайдера, в том числе:
  - оценка частоты сменяемости топ-менеджмента 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 ЭБ;

— разработка и использование специализированных процедур оценки технологических особенностей провайдера, возможностей его оборудования и т. д.;
— совместная или согласованная между кредитной организацией и провайдером политика обеспечения информационной безопасности и конфиденциальности информации;
— 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 СЭБ, 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 ЭБ 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, необходимо отразить следующие моменты:

- конкретные временные ограничения по устранению сбоев и неисправностей в поставленном ими по договору оборудовании или программном обеспечении;
- ответственность провайдера за предоставление, 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 кредитной организации в части обеспечения непрерывности функционирования системы ЭБ и процедуры реализации данных функций;
- порядок информирования органов управления кредитной организации и других структурных подразделений, а также клиентов кредитной организации о возникновении нештатных ситуаций, способных привести к нарушению непрерывности функционирования системы ЭБ, и мероприятий, направленных или необходимых для устранения причин;
- план обеспечения непрерывности и восстановления работоспособности системы ЭБ;
- методики стресс-тестирования кредитной организации в части непрерывности функционирования СЭБ.

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

- сетевые (хакерские атаки) на ресурсы кредитной организации или провайдера;
- механическое нарушение основного и дублирующего каналов связи с провайдером;
- выход из строя сервера баз данных СЭБ;
- выход из строя сервера приложений СЭБ;
- временное отключение электроэнергии в сети;
- отключение резервного источника электропитания СЭБ;
- воздействие компьютерных вирусов на СЭБ или на ее отдельные модули.

Ключевым документом в целях обеспечения непрерывности функционирования СЭБ является разработанный в кредитной организации соответствующий план обеспечения непрерывности и восстановления работоспособности системы.

План обеспечения непрерывности функционирования СЭБ должен основываться на перечне наиболее критичных для работоспособности СЭБ 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 СЭБ планом должны быть предусмотрены соответствующие действия кредитной организации, ее клиентов и организаций-провайдеров. Наиболее подробно должны быть прописаны 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 СЭБ план должен предусматривать также процедуры по организации проведения операций клиентов альтернативными способами (без использования СЭБ) в наиболее короткие сроки.

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

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 СЭБ в кредитной организации должны быть регламентированы:

- способы мониторинга СЭБ, 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 клиентов кредитной организации в случае нарушения непрерывности функционирования СЭБ.

Целесообразным является функционирование в кредитной организации Службы поддержки клиентов в части функционирования СЭБ.

Также в целях координации деятельности структурных подразделений кредитной организации в условиях возникновения сбоя и приостановки работы СЭБ (в соответствии с закрепленными за ними функциями по устранению нарушений в работе системы ЭБ 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 состав которой могут входить:

- руководитель службы информационных технологий:
- руководитель СИБ;
- руководитель службы операционной работы;
- руководитель службы хозяйственного обеспечения;
- руководитель службы по связям с общественностью;
- руководитель юридической службы;
- другие при необходимости.

Основной задачей членов комиссии является правильная классификация нештатных ситуаций[101] и выбор процедур реагирования в соответствии с планом обеспечения непрерывности функционирования системы ЭБ.

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

- по вопросам электроснабжения — члену антикризисного комитета, руководителю службы хозяйственного обеспечения;
- по вопросам качества систем связи — члену антикризисного комитета, начальнику управления информатики;
- по вопросам репутационного риска — члену антикризисного комитета, руководителю службы по связям с общественностью;

101 Речь идет о нештатных ситуациях, при которых может быть нарушена непрерывность функционирования системы электронного банкинга.

- по вопросам возникших правовых коллизий, связанных с обслуживанием клиентов посредством СЭБ, — руководителю юридической службы и т. д.

Окончательное решение о работе банка по антикризисному плану принимает председатель антикризисной комиссии. То есть поддержка функционирования банка во внештатной ситуации в соответствии с ее характером, координация деятельности структурных подразделений, руководителей и отдельных сотрудников возлагаются 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, необходимо 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.

Процедуры стресс-тестирования могут учитывать функционирование как отдельных участков информационного контура системы ЭБ (например, внешних участков — аппаратных и программных средств клиентов кредитной организации или ее провайдеров; внутренних участков — автоматизированного рабочего места 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 ЭБ, 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 ЭБ значительно повышает качество разрабатываемых процедур реагирования на такие воздействия в целях обеспечения непрерывности или восстановления функционирования системы.

Относительно **разработки типовых договоров с клиентами на обслуживание посредством СЭБ** следует отметить, что с точки зрения минимизации правового и репутационного рисков кредитной организации целесообразной является унификация договоров с клиентами о подключении к СЭБ. При этом унификация должна учитывать, что различным клиентам кредитной организации при работе с СЭБ могут быть предоставлены различные права и возможности, что делает необходимой разработку соответствующих типовых договоров.

Помимо типовых форм договора могут быть также разработаны типовые формы:

- заявления на предоставление услуг по СЭБ;
- заявления на изменение вариантов обслуживания.

В общем случае договор о подключении и обслуживании в СЭБ между кредитной организацией и ее клиентом может содержать следующие положения:

1. Предмет договора.
2. Права и обязанности сторон.
3. Ответственность сторон.
4. Стоимость услуг.
5. Срок действия договора.
6. 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 в банке счету;
- способ передачи от кредитной организации к клиенту необходимых программных или аппаратных средств, в том

числе используемых для генерирования ключей электронной цифровой подписи, состав передаваемых программных и аппаратных средств;

- способы обмена между кредитной организацией и ее клиентом электронными документами.

В разделе, раскрывающем **права и обязанности сторон**, могут быть отмечены:

- обязанность банка по обеспечению возможности передачи электронных документов в СЭБ по указанным клиентом адресам;
- перечень случаев, в которых банк имеет право на неисполнение электронных документов клиента;
- порядок уведомления клиента об изменениях размера и условий платы за услуги использования СЭБ;
- 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 СЭБ.

В разделе, посвященном **ответственности сторон**, в рамках действующего законодательства детально раскрывается ответственность клиентов и кредитной организации, в том числе могут оговариваться положения, согласно которым:

- 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 СЭБ, 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;

- клиент несет ответственность за правильность формирования документов, их достоверность и срочность передачи их банку;
- 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;
- разграничена ответственность в случае, если информация, передаваемая сторонами друг другу через электронную почту, стала доступна третьим лицам либо если ущерб возник из-за составляющей СЭБ, находящейся вне непосредственного контроля кредитной организации.

В отношении проектной документации, в соответствии с которой разрабатывается и монтируется СЭБ, следует иметь в виду, что на этапе разработки СЭБ по различным причинам **могут вноситься изменения в изначальный проект системы**, 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 СЭБ на предмет:

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

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

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

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

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

К числу разрабатываемой эксплуатационной документации могут относиться:

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

Первые два документа являются аналогичными «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 ЭБ, с учетом всех доработок в проектной документации и информационном контуре, внесенных на этапе разработки.

Инструкция по эксплуатации комплекса технических средств представляет собой документ, содержащий в соответствии со спецификацией программных средств и модулей и спецификацией аппаратных средств СЭБ описание основных особенностей, допустимого режима работы программных и аппаратных средств в составе информационного контура СЭБ, 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 автоматизированных рабочих мест специалистов кредитной организации, в том числе: автоматизированное рабочее место (АРМ) операционных работников; АРМ контроллера операций; АРМ администратора СЭБ; АРМ администратора информационной безопасности СЭБ; программных модулей и комплексов, обеспечивающих взаимодействие информационного контура СЭБ с другими банковскими автоматизированными системами; другого специализированного программного обеспечения;
- настройки аппаратного обеспечения информационного контура.

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

Руководство по сопровождению программного обеспечения СЭБ — документ, представляющий собой перечень и описание инструкций в части сопровождения программного и аппаратного обеспечения системы ЭБ. 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 функционирование 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);
- правила действий ответственных специалистов кредитной организации по устранению наиболее типичных случаев сбоев программного и аппаратного обеспечения СЭБ;
- правила действий ответственных специалистов кредитной организации по другим операциям, связанным с обслуживанием программного и аппаратного обеспечения информационного контура СЭБ.

Руководство пользователей программных компонентов СЭБ представляет собой документ, предназначенный непосредственно для пользователей СЭБ 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 СЭБ).

Такой документ на соответствующее программное обеспечение в составе информационного контура СЭБ может содержать следующую информацию, сгруппированную по разделам[102]:

- в разделе «Введение»:
  - — область применения программного обеспечения;
  - — краткое описание возможностей программного обеспечения;

102 Представлены условные названия разделов документа и их содержание.

- 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 средства 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.

При этом для каждой операции обработки данных могут 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;
- действия по восстановлению программного обеспечения или данных при отказе магнитных носителей или обнаружении ошибок в данных;
- действия в случаях обнаружения несанкционированного вмешательства в данные;
- действия в других аварийных ситуациях.

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 этапа разработки СЭБ. При этом основными и минимально необходимыми являются следующие вопросы:

- Производится ли разработка СЭБ в сроки, определенные планом на проект?
- Имеются ли в наличии отчеты о выполнении работ, определенных планом по проекту?
- Предусмотрен ли комплексный анализ специалистами СВК положений договора (контракта) о поставке программного обеспечения СЭБ или его части, а также иных технических средств?
- Предусмотрен ли комплексный анализ специалистами СВК положений договора (контракта) с организацией-провайдером о предоставлении услуг связи?
- Разработаны ли проекты типовых договоров с клиентами на обслуживание посредством СЭБ?
- Разработана ли необходимая внутренняя документация, регламентирующая обеспечение информационной безопасности и непрерывности функционирования системы ЭБ?
- 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;
  - — спецификация программных средств и модулей системы ЭБ;
  - — руководство по сопровождению программного обеспечения СЭБ;
  - — руководство по установке и настройке;
  - — руководства пользователей?
- Разработаны ли ответственными за документацию иные документы, предусмотренные перечнем эксплуатационной документации?

5.2.6. Организация (адаптация) процедур внутреннего аудита и контроля на этапе испытаний, сдачи и приемки в эксплуатацию системы электронного банкинга

Этап проведения испытаний и приемки в эксплуатацию является неотъемлемым с точки зрения организации корпоративного управления звеном в жизненном цикле любой автоматизированной системы, в том числе СЭБ.

Основной задачей данного этапа является установление соответствия разработанной СЭБ предъявляемым к ней требованиям функциональности, пользовательского интерфейса, надежности, совместимости с другими банковскими автоматизированными системами, информационной безопасности и т. д., отраженным в проектной документации, в частности в описании постановки комплекса задач на систему ЭБ.

В зависимости от индивидуальных особенностей организации корпоративного управления в кредитной организации и от особенностей

реализации системы ЭБ могут предусматриваться различные стадии испытаний СЭБ, такие как:

- предварительные испытания СЭБ;
- опытная эксплуатация СЭБ;
- приемочные испытания СЭБ.

Предварительные испытания автоматизированной системы проводят для определения ее работоспособности и решения вопроса о возможности приемки автоматизированной системы в опытную эксплуатацию. Предварительные испытания следует выполнять после проведения разработчиком отладки и тестирования поставляемых программных и технических средств системы и представления им соответствующих документов об их готовности к испытаниям, а также после ознакомления персонала автоматизированной системы с эксплуатационной документацией.

Опытную эксплуатацию автоматизированной системы проводят с целью определения фактических значений количественных и качественных характеристик автоматизированной системы и готовности персонала к работе в условиях функционирования автоматизированной системы, определения фактической эффективности автоматизированной системы, корректировки (при необходимости) документации.

Приемочные испытания автоматизированной системы проводят для определения соответствия автоматизированной системы техническому заданию, оценки качества опытной эксплуатации и решения вопроса о возможности приемки автоматизированной системы в постоянную эксплуатацию. Приемочным испытаниям автоматизированной системы, как правило, предшествует ее опытная эксплуатация в кредитной организации.

Положительной практикой является отмеченная многоуровневая организация испытаний системы ЭБ. При этом допускается дополнительное проведение других видов испытаний системы ЭБ или ее отдельных модулей, например, на этапе разработки по соответствующим «контрольным точкам» плана реализации системы ЭБ.

Вместе с тем, учитывая индивидуальные особенности внутренней структуры и деятельности каждой конкретной кредитной организации, отдельные виды испытаний системы ЭБ могут быть объединены в общий процесс приемочных испытаний.

Испытания могут быть автономные или комплексные.

Автономные испытания охватывают части автоматизированной системы. Их проводят по мере готовности частей автоматизированной системы к сдаче в опытную эксплуатацию.

Комплексные испытания проводят для групп взаимосвязанных частей автоматизированной системы или для автоматизированной системы в целом.

Вне зависимости от стадии испытаний системы ЭБ проверке или аттестации в ней подвергают:

- отдельный модуль СЭБ;
- СЭБ в целом;
- персонал кредитной организации (функциональные обязанности которого предполагают работу с СЭБ);
- эксплуатационную документацию, регламентирующую деятельность персонала при функционировании СЭБ.

При испытаниях системы ЭБ в целом рекомендуется уделять внимание:

- качеству выполнения комплексом программных и технических средств автоматических функций во всех режимах функционирования системы ЭБ согласно техническому заданию (описанию постановки комплекса задач) на создание системы ЭБ;
- знанию персоналом кредитной организации эксплуатационной документации и наличию у него навыков, необходимых для выполнения установленных функций во всех режимах функционирования СЭБ, согласно описанию постановки комплекса задач на создание СЭБ;
- полноте содержащихся в эксплуатационной документации указаний персоналу кредитной организации по выполнению им функций во всех режимах функционирования СЭБ согласно описанию постановки комплекса задач на создание СЭБ;
- количественным и (или) качественным характеристикам выполнения автоматизированных функций СЭБ в соответствии с описанием постановки комплекса задач;
- другим свойствам СЭБ, которым она должна соответствовать согласно требованиям описания постановки комплекса задач.

Испытания СЭБ следует проводить на стенде, подготовленном и приближенном к условиям работы подразделения-заказчика. По согласованию между подразделением-заказчиком и разработчиком предварительные испытания и приемку программных средств СЭБ допускается проводить при отсутствии стенда на технических средствах разработчика при создании условий получения достоверных результатов испытаний.

Допускаются последовательное проведение испытаний и сдача частей СЭБ в опытную и постоянную эксплуатацию при соблюдении установленной в техническом задании очередности ввода автоматизированной системы в действие.

В соответствии с классификацией стадий испытаний системы ЭБ предварительные испытания могут быть также:

- автономные;
- комплексные.

Автономные предварительные испытания СЭБ следует проводить в соответствии с программой и методикой автономных испытаний, разрабатываемых для каждой части СЭБ.

В программе автономных испытаний могут указываться:

- перечень функций, подлежащих испытаниям;
- описание взаимосвязей объекта испытаний с другими частями СЭБ и внутрибанковскими автоматизированными системами;
- условия, порядок и методы проведения испытаний и обработки результатов;
- критерии приемки частей СЭБ по результатам испытаний.

К программе автономных предварительных испытаний может быть приложен график проведения испытаний.

Подготовленные и согласованные тесты (контрольные примеры) на этапе автономных предварительных испытаний должны обеспечить:

- полную проверку функций и процедур по перечню, согласованному с заказчиком;
- необходимую точность вычислений, установленную в описании постановки комплекса задач;
- проверку основных временных характеристик функционирования программных средств (в тех случаях, когда это является существенным);

- проверку надежности и устойчивости функционирования программных и технических средств.

В целях обеспечения достоверности в качестве исходной информации для теста может быть использован фрагмент реального информационного массива данных в объеме, достаточном для обеспечения необходимой достоверности испытаний.

Результаты автономных испытаний частей СЭБ следует фиксировать в протоколах испытаний. Протокол должен содержать заключение о возможности (невозможности) допуска части СЭБ к комплексным испытаниям.

Если проведенные автономные испытания будут признаны недостаточными либо будет выявлено нарушение требований регламентирующих документов по составу или содержанию документации, испытываемая часть СЭБ может быть возвращена на доработку и назначен новый срок испытаний.

Любые испытания СЭБ должны проводиться соответствующей комиссией из числа руководителей и сотрудников основных подразделений, в чьи функции входит непосредственная работа с СЭБ: подразделения информационных технологий (ИТ-подразделения), подразделения информационной безопасности и т. д. Состав комиссии утверждается приказом или распоряжением, которое может содержать:

- наименование принимаемой СЭБ в целом или ее частей;
- сведения о составе комиссии;
- основание для организации комиссии;
- наименование подразделения-заказчика;
- наименование подразделения или организации-разработчика, подразделения или организации-соисполнителя;
- назначение и цели работы комиссии;
- сроки начала и завершения работы комиссии;
- указание о форме завершения работы комиссии.

Комплексные предварительные испытания СЭБ проводят путем выполнения комплексных тестов. Результаты испытаний отражают в протоколе. Работа завершается оформлением акта приемки в опытную эксплуатацию.

В программе комплексных испытаний СЭБ или ее частей могут указываться:

- перечень объектов испытания;
- состав предъявляемой документации;
- описание проверяемых взаимосвязей между объектами испытаний;
- очередность испытаний частей СЭБ.
- порядок и методы испытаний, в том числе состав программных средств и оборудования, необходимых для проведения испытаний, включая специальные стенды.

Для проведения комплексных предварительных испытаний должны быть подготовлены:

- программа комплексных предварительных испытаний;
- сводное заключение по автономным испытаниям соответствующих частей системы ЭБ и устранению ошибок и замечаний, выявленных при автономных испытаниях;
- комплексные тесты;
- программные и технические средства, соответствующая эксплуатационная документация.

В ходе комплексных предварительных испытаний может быть использована в качестве исходной информация, полученная на автономных испытаниях частей СЭБ.

Тесты и контрольные примеры, подготовленные для комплексных предварительных испытаний, должны:

- быть логически увязанными;
- обеспечивать проверку выполнения функций частей СЭБ во всех режимах функционирования, установленных в описании постановки комплекса задач на СЭБ, в том числе всех связей между ними;
- обеспечивать проверку реакции СЭБ на некорректную информацию и аварийные ситуации.

Протокол комплексных предварительных испытаний должен содержать заключение о возможности (невозможности) приемки СЭБ в опытную эксплуатацию, а также перечень необходимых доработок и рекомендуемые сроки их выполнения.

После устранения недостатков целесообразно проведение повторных комплексных испытаний в необходимом объеме.

Заканчиваются предварительные испытания подготовкой акта приемки в опытную эксплуатацию, который может содержать:

- наименование СЭБ (или ее части), принимаемой в опытную эксплуатацию;
- наименование документа, на основании которого разработана СЭБ;
- состав приемочной комиссии и основание для ее работы (наименование, номер и дату утверждения документа, на основании которого создана комиссия);
- период времени работы комиссии;
- наименование организации или подразделения-разработчика, организации или подразделения-соисполнителя и подразделения-заказчика;
- состав функций СЭБ (или ее части), принимаемых в опытную эксплуатацию;
- перечень составляющих технического, программного, информационного и организационного обеспечения, проверяемых в процессе опытной эксплуатации;
- перечень документов, предоставленных комиссии;
- оценку соответствия принимаемой СЭБ техническому заданию или описанию комплекса задач на ее создание;
- основные результаты приемки в опытную эксплуатацию;
- решение комиссии о принятии автоматизированной системы в опытную эксплуатацию.

Опытную эксплуатацию СЭБ проводят в соответствии с программой, в которой могут указываться:

- условия и порядок функционирования частей СЭБ и системы электронного банкинга в целом;
- продолжительность опытной эксплуатации, достаточной для проверки правильности функционирования СЭБ при выполнении каждой функции системы и готовности персонала кредитной организации к работе в условиях функционирования СЭБ;
- порядок устранения недостатков, выявленных в процессе опытной эксплуатации.

В период проведения опытной эксплуатации СЭБ должен поддерживаться в актуальном состоянии рабочий журнал, в который заносят сведения:

- о продолжительности функционирования СЭБ;
- отказах, сбоях, аварийных ситуациях;

- изменениях параметров объекта автоматизации;
- проводимых корректировках документации и программных средств;
- наладке технических средств.

Сведения должны фиксироваться в журнале с указанием даты и ответственного лица. В журнал могут быть занесены замечания персонала кредитной организации по удобству эксплуатации СЭБ.

По результатам опытной эксплуатации принимают решение о возможности (или невозможности) предъявления частей СЭБ и СЭБ в целом на приемочные испытания.

Опытная эксплуатация СЭБ завершается оформлением акта о завершении опытной эксплуатации и допуске СЭБ к приемочным испытаниям.

Приемочные испытания проводят в соответствии с программой, в которой могут указываться:

- перечень объектов, выделенных в СЭБ для испытаний, и перечень требований, которым должны соответствовать объекты (со ссылкой на пункты технического задания или описания постановки комплекса задач);
- критерии приемки СЭБ и ее частей;
- условия и сроки проведения испытаний СЭБ;
- средства для проведения испытаний;
- лица, ответственные за проведение испытаний;
- методики испытаний и обработки их результатов;
- перечень оформляемой документации.

Для проведения приемочных испытаний должна быть подготовлена следующая документация:

- техническое задание или описание постановки комплекса задач на создание СЭБ;
- акт приемки в опытную эксплуатацию;
- рабочие журналы опытной эксплуатации;
- акт завершения опытной эксплуатации и допуска СЭБ к приемочным испытаниям;
- программа и методика испытаний.

Приемочные испытания следует проводить на функционирующем оборудовании с реальными информационными данными или идентичными им.

Приемочные испытания, в первую очередь, должны включать проверку:

- полноты и качества реализации функций при штатных, предельных, критических значениях параметров объекта автоматизации и в других условиях функционирования автоматизированной системы, указанных в техническом задании;
- выполнения каждого требования, относящегося к интерфейсу системы;
- работы персонала в диалоговом режиме;
- средств и методов восстановления работоспособности автоматизированной системы после отказов;
- комплектности и качества эксплуатационной документации.

Проверку полноты и качества выполнения функций СЭБ целесообразно осуществлять в два этапа:

1) на первом этапе проводят испытания отдельных функций (задач, комплексов задач). При этом проверяется выполнение требований технического задания или описания постановки комплекса задач к функциям (задачам);
2) на втором этапе проводят проверку взаимодействия задач в системе и выполнения требований описания комплекса задач к СЭБ в целом.

По согласованию с подразделением-заказчиком проверка задач в зависимости от их специфики может проводиться автономно или в составе комплекса задач. Объединение задач при проверке в комплексах целесообразно проводить с учетом общности используемой информации и внутренних связей.

Проверку работы персонала в диалоговом режиме проводят с учетом полноты и качества выполнения функций системы в целом.

Проверке подлежат:

- полнота сообщений, директив, запросов, доступных оператору, и их достаточность для эксплуатации системы;
- сложность процедур диалога, возможность работы персонала без специальной подготовки;
- реакция СЭБ и ее частей на ошибки оператора, средства сервисного обслуживания автоматизированных средств.

Проверка средств восстановления работоспособности СЭБ после отказов ЭВМ может включать проверку:

- наличия в эксплуатационной документации рекомендаций по восстановлению работоспособности и полноты их описания;
- практической выполнимости рекомендованных процедур;
- работоспособности средств автоматического восстановления функций (при их наличии).

Проверку комплектности и качества эксплуатационной документации следует проводить путем анализа документации на соответствие требованиям нормативно-технических документов и описания постановки комплекса задач.

Результаты испытаний объектов СЭБ, предусмотренных программой, могут фиксироваться в протоколах, содержащих следующие разделы:

- назначение испытаний;
- состав технических и программных средств, используемых при испытаниях;
- указание методик, в соответствии с которыми проводятся испытания, обработка и оценка результатов;
- условия проведения испытаний и характеристики исходных данных;
- обобщенные результаты испытаний;
- выводы о результатах испытаний и соответствии созданной системы или ее частей определенному разделу требований технического задания на автоматизированную систему.

Протоколы испытаний объектов СЭБ по всей программе могут обобщаться в едином протоколе, на основании которого делают заключение о соответствии СЭБ требованиям описания постановки комплекса задач на СЭБ и возможности оформления акта приемки СЭБ в постоянную эксплуатацию.

Протокол испытаний может содержать:

- наименование объекта испытаний;
- список должностных лиц, проводивших испытания;
- цель испытаний;
- сведения о продолжительности испытаний;
- перечень пунктов технического задания или описания постановки комплекса задач на создание СЭБ, на соответствие которым проведены испытания;

- перечень пунктов программы испытаний, по которым проведены испытания;
- сведения о результатах наблюдений за правильностью функционирования СЭБ;
- сведения об отказах, сбоях и аварийных ситуациях, возникающих при испытаниях СЭБ;
- сведения о корректировках параметров объекта испытания и технической документации.

Приемочные испытания завершаются оформлением **акта о приемке СЭБ** в эксплуатацию, который может содержать:

- наименование объекта в составе информационного контура СЭБ или всей СЭБ, принимаемой в эксплуатацию;
- сведения о статусе приемочной комиссии, ее составе и основание для работы;
- период времени работы комиссии;
- наименование организации-разработчика, организации-соисполнителя и организации-заказчика либо соответствующих подразделений кредитной организации;
- наименование документа, на основании которого разработана СЭБ;
- состав функций СЭБ (или ее части), принимаемой в эксплуатацию;
- перечень составляющих технического, программного, информационного и организационного обеспечения СЭБ, принимаемых в эксплуатацию;
- перечень документов, предъявляемых комиссии;
- заключение о результатах опытной эксплуатации СЭБ в случае ее осуществления;
- оценку соответствия принимаемой СЭБ техническому заданию на ее создание;
- краткую характеристику и основные результаты выполненной работы по созданию СЭБ;
- оценку экономической эффективности от внедрения СЭБ (по проектным данным);
- решение комиссии;
- рекомендации комиссии по дальнейшему развитию СЭБ.

К акту приемки в эксплуатацию могут прилагаться: программа и протоколы испытаний, протоколы заседания комиссии, акты приемки в эксплуатацию принятых ранее частей СЭБ, перечень технических средств, которые использовала комиссия при приемке СЭБ. По усмотрению комиссии в приложение могут включаться дополнительные документы.

Для планирования проведения всех видов испытаний кредитной организации должен быть разработан документ **«Программа и методика испытаний»,** разработчиком которого является ответственное лицо из числа членов комитета по технологиям кредитной организации. К разработке данного документа могут быть также привлечены: подразделение — заказчик СЭБ, ИТ-подразделение и подразделение информационной безопасности кредитной организации.

Программа и методика испытаний должна устанавливать необходимый и достаточный объем испытаний, обеспечивающий заданную достоверность получаемых результатов.

Этот документ может разрабатываться как на СЭБ в целом, так и на отдельный модуль СЭБ. Приложение к Программе и методике испытаний может включать контрольные примеры, детально описывающие тесты, осуществляемые в ходе испытаний системы.

Основным документом, регламентирующим любые виды испытаний СЭБ, является **Программа и методика испытаний**.

Программа и методика испытаний СЭБ предназначена для установления технических данных, подлежащих проверке при испытании компонентов СЭБ, а также порядка испытаний и методов их контроля.

Документ должен содержать перечень конкретных проверок, которые следует осуществлять при испытаниях для подтверждения выполнения требований описания постановки комплекса задач, со ссылками на соответствующие методики (разделы методик) испытаний.

Перечень проверок (на этапе испытаний) включает:

- соответствие СЭБ требованиям описания постановки комплекса задач;
- комплектность СЭБ;
- комплектность и качество документации на СЭБ;
- комплектность, достаточность состава и качество программных средств и программной документации;

- количество и квалификация персонала, обслуживающего СЭБ;
- степень выполнения требований функционального назначения СЭБ;
- контролепригодность СЭБ.

В общем случае программа испытаний может содержать разделы:

- объект испытаний;
- цель испытаний;
- общие положения;
- объем испытаний;
- условия и порядок проведения испытаний;
- материально-техническое обеспечение испытаний;
- отчетность.

В документ также могут включаться приложения.

В зависимости от особенностей СЭБ отдельные разделы могут объединяться или исключаться при условии изложения их содержания в других разделах программы испытаний, в нее также могут включаться дополнительные разделы (при необходимости).

В разделе «Объект испытаний» могут указываться:

- полное наименование системы, обозначение;
- комплектность испытательной системы.

В разделе «Цель испытаний» указываются конкретные цели, которые должны быть достигнуты, и задачи, которые должны быть решены в процессе испытаний.

В разделе «Общие положения» указываются:

- перечень руководящих документов, на основании которых проводят испытания;
- место и продолжительность испытаний;
- организации, участвующие в испытаниях;
- перечень ранее проведенных испытаний;
- перечень предъявляемых на испытания документов, откорректированных по результатам ранее проведенных испытаний.

В разделе «Объем испытаний» указывают:

- перечень этапов испытаний и проверок, а также количественные и качественные характеристики, подлежащие оценке;

- последовательность проведения и режима испытаний;
- требования по испытаниям программных средств СЭБ;
- перечень работ, проводимых после завершения испытаний, требования к ним, объем и порядок проведения.

В разделе «Условия и порядок проведения испытаний» указывают:

- условия проведения испытаний;
- условия начала и завершения отдельных этапов испытаний;
- имеющиеся ограничения в условиях проведения испытаний;
- требования к техническому обслуживанию системы;
- порядок взаимодействия подразделений и внешних организаций — контрагентов кредитной организации, участвующих в испытаниях;
- порядок привлечения экспертов для исследования возможных нарушений целостности данных, антивирусной защиты и т. д. в процессе проведения испытаний;
- требования к персоналу кредитной организации, проводящему испытания, и порядок его допуска к испытаниям с использованием действующей информационной базы данных.

В разделе «Материально-техническое обеспечение испытаний» указывают конкретные виды материально-технического обеспечения с распределением задач и обязанностей подразделений и организаций — контрагентов кредитной организации, участвующих в испытаниях.

В разделе «Отчетность» приводят перечень отчетных документов, которые должны оформляться как в процессе проведения испытаний, так и по их завершении, с указанием подразделений кредитной организации, разрабатывающих и согласующих сроки оформления этих документов. К отчетным документам могут относиться акт и отчет о результатах испытаний.

В приложения может включаться перечень методик испытаний, применяемых для оценки характеристик СЭБ.

Методики испытаний разрабатывают на основе описания постановки комплекса задач и утвержденных программ испытаний с использованием типовых методик испытаний (при наличии). Отдельные положения типовых методик испытаний могут уточняться и конкретизироваться в разрабатываемых методиках испытаний

в зависимости от особенностей СЭБ и условий проведения испытаний. Содержание разделов методик устанавливается подразделением-разработчиком совместно с подразделением — заказчиком СЭБ.

Все перечисленные выше аспекты могут являться основой для оценки качества организации этапа испытаний, сдачи и приемки в эксплуатацию СЭБ службами внутреннего аудита и внутреннего контроля. Основными и минимально необходимыми вопросами являются следующие:

- Разработана ли «Программа и методика испытаний СЭБ» или иной подобный документ?
- Разработан ли «Контрольный пример испытаний СЭБ» или иной подобный документ?
- Назначен ли ответственный за организацию испытаний СЭБ?
- Определены ли члены экспертной комиссии по проведению испытаний СЭБ?
- Входит ли в состав экспертной комиссии представитель подразделения-разработчика?
- Входит ли в состав экспертной комиссии представитель подразделения, ответственного за сопровождение СЭБ?
- Входит ли в состав экспертной комиссии представитель организации — поставщика системы или модулей СЭБ?
- Входит ли в состав экспертной комиссии представитель организации-провайдера?
- Входит ли в состав экспертной комиссии представитель подразделения информационной безопасности?
- Входит ли в состав экспертной комиссии представитель подразделения-заказчика?
- Отражены ли в протоколе результаты испытаний, а также выявленные ошибки и сбои?
- Согласован ли протокол испытаний членами экспертной комиссии?
- Производится ли оформление процедуры передачи в эксплуатацию СЭБ или модулей СЭБ актом приемки-передачи?
- Согласуется ли акт приемки-передачи подразделением-разработчиком, подразделением-заказчиком, куратором информационных технологий либо членами комитета по технологиям?

5.2.7. Организация (адаптация) процедур внутреннего контроля на этапе эксплуатации системы электронного банкинга

Качество организации процедур внутреннего аудита и контроля **в части организационных мер предоставления услуг и операций посредством СЭБ** зависит от следующих моментов:

- Предусматривается ли проверка СВА кредитной организации соответствия перечня услуг и операций, которые предоставляются клиентам, заявленному перечню в договорах с клиентами и технической документации?
- Разработаны ли и утверждены внутренние документы, определяющие порядок предоставления и изменения клиентам доступа к услугам и операциям по технологии ЭБ?
- Разработана ли и утверждена методика оценки и мониторинга источников рисков, связанных с использованием СЭБ?

Важной с точки зрения минимизации операционного и репутационного рисков кредитной **организации является качественная организация информационного обеспечения СЭБ.**

Целесообразной является разработка кредитной организацией внутреннего документа, регламентирующего процедуры изменения и дополнения публикуемой информации. При этом следует обращать внимание на то, что эффективность данного документа может зависеть от того, содержит ли он:

- порядок принятия решений о внесении изменений и дополнений в публикуемую информацию;
- порядок назначения сотрудников, ответственных за внесение изменений и дополнений в публикуемую информацию;
- порядок контроля своевременности и полноты внесения изменений и дополнений в публикуемую информацию.

В части правового обеспечения при организации соответствующих процедур внутреннего контроля следует обращать внимание:

- на наличие положений о предоставлении услуг в СЭБ в договорах о банковском обслуживании клиентов, определяющих перечень предоставляемых клиентам услуг в рамках СЭБ и обязанности клиентов по соблюдению порядка предоставления услуг;

- наличие установленного порядка внесения изменений в договоры с клиентами, который определяет унификацию договоров с клиентами на предоставление услуг посредством СЭБ.

Для повышения качества организации деятельности служб разработки и сопровождения СЭБ необходимо обращать внимание на следующие моменты:

- Регламентированы ли статус, подчиненность и подотчетность куратору информационных технологий руководителей службы разработки и службы сопровождения СЭБ?
- Регламентированы ли профессиональный уровень (профессиональная подготовка по технологии ЭБ) руководителей службы разработки и службы сопровождения ЭБ?
- Регламентированы ли организационно-штатная структура и персональный состав подразделений службы разработки и службы сопровождения СЭБ (численность, квалификация и др.)?
- Регламентированы ли профессиональный уровень сотрудников службы разработки и службы сопровождения СЭБ (профессиональная подготовка по технологии ЭБ)?
- Регламентировано ли закрепление обязанностей за сотрудниками службы разработки и службы сопровождения СЭБ?
- Регламентированы ли периодичность и формы отчетов о своей деятельности службы автоматизации кредитной организации?

Для повышения качества **планирования применения и развития СЭБ** необходимо:

- наличие тактических планов развития СЭБ, их соответствие стратегическому плану развития технологий, применяемых кредитной организацией;
- своевременность (актуальность) разработки (внесения корректировок) тактических планов развития СЭБ в соответствии с политикой управления электронными системами кредитной организации;
- определение статуса должностных лиц (куратора информационных технологий, членов комитета по технологиям), согласовывающих и утверждающих тактические планы (корректировки) развития СЭБ;

- наличие формализованных процедур внесения изменений (корректировки) в планы развития применяемой в кредитной организации СЭБ;
- обеспечение своевременности и периодичности проведения совещаний комитета по технологиям, на которых рассматриваются вопросы управления и развития применяемой в кредитной организации СЭБ;
- регулярность рассмотрения комитетом по технологиям кредитной организации отчетов о выполнении планов развития СЭБ.

Немаловажной с точки зрения организации процедур внутреннего контроля также является должная **организация учета информационных активов** (программных и аппаратных средств, других информационных ресурсов — источников данных), составляющих информационный контур СЭБ. Для этого необходимо:

- наличие реестра аппаратных средств в составе информационного контура СЭБ;
- наличие формализованных процедур внесения изменений в реестр аппаратных средств СЭБ;
- наличие ответственного лица за ведение реестра аппаратных средств в составе информационного контура СЭБ и внесение в него изменений;
- периодичность и наличие актов инвентаризации аппаратных средств в составе информационного контура СЭБ;
- наличие реестра программных средств в составе информационного контура СЭБ;
- наличие формализованных процедур внесения изменений в реестр программных средств в составе информационного контура СЭБ;
- наличие ответственного лица за ведение реестра программных средств в составе информационного контура СЭБ и внесение в него изменений;
- периодичность и наличие актов инвентаризации программных средств в составе информационного контура СЭБ;
- наличие реестра информационных ресурсов в составе информационного контура СЭБ;

- наличие формализованных процедур внесения изменений в реестр информационных ресурсов в составе информационного контура СЭБ;
- наличие ответственного лица за ведение реестра информационных ресурсов в составе информационного контура СЭБ и внесение в него изменений;
- периодичность и наличие актов инвентаризации информационных ресурсов в составе информационного контура СЭБ.

В части качества процессов контроля **функционирования аппаратных и программных средств СЭБ** необходимы:

- наличие процедур и средств контроля нагрузки и режимов функционирования аппаратных и программных средств кредитной организации;
- документарное отражение результатов контроля в специализированных электронных журналах и (или) на бумажных носителях;
- соблюдение своевременности и периодичности составления прогнозов будущих потребностей в аппаратных и программных средствах СЭБ;
- учет прогнозов при составлении и утверждении планов развития СЭБ.

В части качества организации процедур внутреннего контроля в отношении **сопровождения и реагирования на инциденты (сбои)** в процессе эксплуатации СЭБ целесообразно уделять внимание:

- обеспечению своевременности и регулярности проведения технического обслуживания компьютерного, телекоммуникационного и прочих видов оборудования информационного контура СЭБ согласно рекомендациям производителей для обеспечения его работоспособности;
- определению процедур реагирования на инциденты (сбои) в процессе эксплуатации аппаратных и программных средств СЭБ.
- закреплению обязанностей сотрудников регистрировать и сообщать обо всех случаях сбоев функционирования;
- наличию порядка (рекомендаций) действий пользователей системы ЭБ при возникновении инцидентов (сбоев);

- наличию в службе автоматизации лиц, ответственных за устранение последствий инцидентов (сбоев);
- наличию порядка регистрации случаев инцидентов (сбоев) в процессе эксплуатации аппаратно-программных средств, а также выбору корректирующих мер по недопущению в дальнейшем потенциальных сбоев в СЭБ;
- учету результатов анализа произошедших инцидентов (сбоев) при составлении планов развития СЭБ.

В части качества организации процедур **информационной безопасности** целесообразно уделять внимание:

- наличию в высшем руководстве кредитной организации собственного куратора СИБ (рекомендуется, чтобы служба автоматизации и СИБ не имели общего куратора);
- назначению лица, ответственного за реализацию защиты информации (администратора информационной безопасности) основных информационных ресурсов СЭБ;
- регламентации деятельности администраторов информационной безопасности нормативно-методическими документами, разработанными в кредитной организации;
- обеспечению своевременности и периодичности проведения специалистами СИБ или администраторами информационной безопасности проверок обеспечения режима информационной безопасности в функциональных подразделениях кредитной организации, задействованных в организации функционирования СЭБ;
- обеспечению своевременности и регулярности повышения квалификации представителей СИБ по направлению технологий ЭБ;
- исключению совмещения в одном лице функций администратора СЭБ и администратора информационной безопасности СЭБ;
- обеспечению распределения обязанностей между администраторами СЭБ и администраторами информационной безопасности СЭБ таким образом, чтобы исключить возможность обладания теми или другими всей полнотой полномочий для бесконтрольного создания, уничтожения

и изменения платежной информации, а также проведения операций по изменению состояния банковских счетов;

- оснащению средствами вычислительной техники (на которой осуществляются операции СЭБ) сертифицированными средствами защиты от несанкционированного доступа и средствами криптографической защиты информации;
- утверждению руководством кредитной организации перечня информации (в части ЭБ), содержащей сведения ограниченного распространения и подлежащей защите в соответствии с законодательством;
- ведению в СЭБ журналов регистрации действий, выполняемых пользователями;
- включению в трудовые договоры (соглашения, контракты), а также в должностные инструкции всех сотрудников кредитной организации, задействованных в организации функционирования СЭБ, обязанностей и ответственности за обеспечение информационной безопасности;
- наличию в кредитной организации действующих инструкций по антивирусной защите и порядка принятия мер при обнаружении компьютерного вируса, учитывающих особенности СЭБ;
- установлению в кредитной организации запрета на присутствие и использование в СЭБ несанкционированных программных средств и данных, не связанных с выполнением конкретных функций в банковских технологических процессах;
- наличию в кредитной организации организационно-распорядительных документов, устанавливающих порядок резервного копирования и хранения критически важных данных и программных средств СЭБ;
- обеспечению своевременности и регулярности резервного копирования критически важных данных СЭБ.

В рамках этапа эксплуатации СЭБ в кредитной организации должны быть также предусмотрены процедуры вывода из эксплуатации СЭБ в случаях изменения стратегии кредитной организации в части направления деятельности или ввода в эксплуатацию новой СЭБ, значительно отличающейся от первоначальной.

Качественная организация таких процедур предусматривает:

- наличие соответствующих распорядительных документов;
- наличие методологии осуществления вывода из эксплуатации;
- порядок действий отдельных подразделений кредитной организации;
- фиксацию данных мероприятий в учетной документации на электронные ресурсы и оборудование, задействованное в информационном контуре СЭБ, и т. д.

Рассмотренный подход может быть принят за основу при разработке конкретных методик и процедур внутреннего аудита и внутреннего контроля, так как направлен на достижение основных целей внутреннего контроля посредством сквозного применения его процедур и предполагает возможность учета специфики деятельности и организационной структуры кредитной организации, является одним из аспектов безопасного применения технологий ДБО.

6. ОБЕСПЕЧЕНИЕ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ ЭЛЕКТРОННОГО БАНКИНГА С УЧЕТОМ ТРЕБОВАНИЙ СТАНДАРТОВ БАНКА РОССИИ ПО ОБЕСПЕЧЕНИЮ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ

«Смотри на дело, как на трудное, и оно в итоге не будет трудным».

Лао-Цзы (Ли Эр),
древнекитайский философ

Особенности банковских систем таковы, что негативные последствия сбоев в работе отдельных организаций или отдельных сервисов, предоставляемых организацией (в том числе и технологии ЭБ), могут привести к быстрому развитию системного кризиса платежной системы, нанести ущерб интересам собственников и клиентов. В случаях возникновения инцидентов информационной безопасности значительно возрастают результирующий риск и возможность нанесения ущерба банку (или банковской группе). В связи с этим угрозы информационной безопасности представляют реальную опасность.

Для противостояния таким угрозам и обеспечения эффективности мероприятий по ликвидации неблагоприятных последствий инцидентов информационной безопасности (их влияния на операционные, кредитные и иные риски) в банковских организациях следует обеспечить достаточный уровень информационной безопасности. Необходимо также сохранить этот уровень в течение длительного времени. По этим причинам обеспечение информационной безопасности является для организаций банковской системы Российской Федерации одним из основополагающих аспектов их деятельности. При этом следует учитывать, что обеспечение информационной безопасности — это процесс, который охватывает все виды деятельности банковской организации, а не отдельные процессы, автоматизированные системы или комплексы. Таким образом, можно говорить, что управление информационной безопасностью рассматривается как часть общей системы управления банка.

Учитывая сложность вопросов информационной безопасности и мировой опыт стандартизации в этой сфере, Банк России разработал и ввел в действие комплекс стандартов по информационной безопасности.

В соответствии с положениями данных стандартов под информационной безопасностью понимается процесс, направленный на обеспечение доступности, целостности и конфиденциальности информационных активов банковской организации (рис. 11).

Информационная безопасность, помимо технической стороны вопроса, включает в себя технологическую и организационную стороны (рис. 12).

Информационная безопасность — метод, посредством которого организация обеспечивает контроль над своими информационными активами и поддержку бизнес-процессов.

Информационная безопасность включает в себя управление персоналом.

Персонал должен быть уведомлен о наличии проблемы информационной безопасности. Пользователи должны понимать необхо-

Рис. 11. Что такое информационная безопасность

димость информационной безопасности для целей бизнеса (зачем им пароли, антивирусы), а не просто быть поставлены перед фактом: «делай то-то».

Целесообразно, если управление информационной безопасностью основывается на риск-ориентированном подходе. Это означает, что информационная безопасность включает регулярную оценку риска.

Необходимо знать:

- что защищать (активы);
- от кого защищать (злоумышленник);
- от чего защищать (угрозы, уязвимости).

То есть для эффективной защиты необходимо определить зону риска (рис. 13).

Любая целенаправленная деятельность банка порождает риски, в том числе и риски информационной безопасности. Это — объективная реальность, и понизить эти риски можно лишь до уровня неопределенности сущностей, характеризующих природу бизнеса. Оставшаяся часть риска, определяемого факторами среды деятельности организации, на которые организация не в силах влиять, должна быть неизбежно принята.

Так, например, все знают, что электронная почта — потенциальный источник распространения вирусов и троянских программ. Но вместе с тем без электронной почты невозможно в настоящий

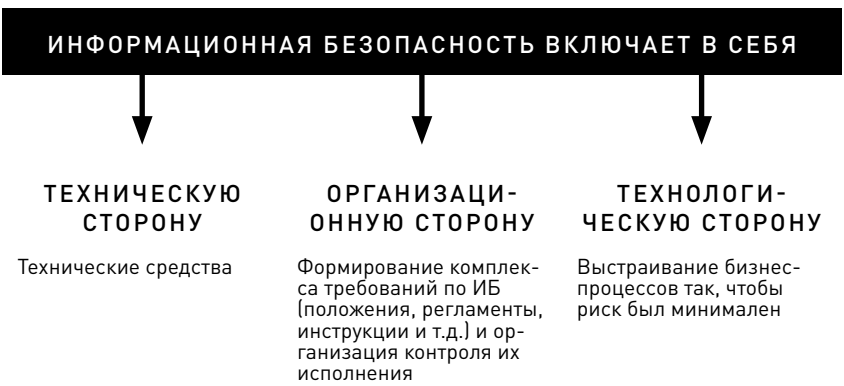

Рис. 12. Основные составляющие информационной безопасности

Рис. 13. Определение зоны риска

момент представить современный бизнес, так как это удобный и уже ставший привычным инструмент. Таким образом, риски, которые организация не в силах снизить путем использования антивирусных средств, организация должна принять.

Особо следует обращать внимание на опасность внутренней угрозы. Наибольшими возможностями для нанесения ущерба организации банковской системы Российской Федерации обладает ее собственный персонал. В этом случае содержанием деятельности злоумышленника является нецелевое использование предоставленного контроля над информационными активами, а также сокрытие следов своей деятельности. Внешний злоумышленник с очень большой вероятностью имеет сообщника (-ов) внутри организации.

По различным оценкам, от 50 до 80% атак, направленных на получение информации или хищение денежных средств со счетов клиентов, начинаются из локальной сети банка. Таким образом, одной из важнейших проблем, стоящих перед руководством и СИБ банка,

является проблема внутренних угроз информационной безопасности. Очевидно, что обиженный или недовольный сотрудник компании, имеющий легальный доступ к сетевым и информационным ресурсам и обладающий определенными знаниями о структуре корпоративной сети, может нанести своей компании гораздо больший ущерб, чем хакер, взламывающий корпоративную сеть через Интернет.

Подход к организации информационной безопасности, изложенный в комплексе стандартов Банка России, позволяет предотвратить возникновение подобных инцидентов, дополнительно предоставив банковской организации ряд преимуществ. Среди них особо стоит отметить:

- создание эффективной и управляемой системы ИТ-безопасности:
  - минимизация ущерба в результате успешной реализации внутренних и внешних угроз;
  - обеспечение непрерывности бизнес-процессов;
- эффективное управление операционными рисками;
- улучшение и защита имиджа банка;
- повышение прозрачности процесса управления информационной безопасностью в банке;
- выполнение требований и рекомендаций Банка России:
  - Положение Банка России от 16 декабря 2003 г. № 242-П «Об организации внутреннего контроля в кредитных организациях и банковских группах»;
  - Письмо Банка России от 13 мая 2002 г. № 59-Т «О рекомендациях Базельского комитета по банковскому надзору»;
  - Письмо Банка России от 30 июня 2005 г. № 92-Т «Об организации управления правовым риском и риском потери деловой репутации в кредитных организациях и банковских группах»;
  - Письмо Банка России от 24 мая 2005 г. № 76-Т «Об организации управления операционным риском в кредитных организациях» и ряд других документов;
  - Письмо Банка России от 27 апреля 2007 г. № 60-Т «Об особенностях обслуживания кредитными организациями клиентов с использованием технологии

дистанционного доступа к банковскому счету клиента (включая интернет-банкинг)»;

— Письмо Банка России от 7 декабря 2007 г. № 197-Т «О рисках при дистанционном банковском обслуживании»;
— Письмо Банка России от 31 марта 2008 г. № 36-Т «О Рекомендациях по организации управления рисками, возникающими при осуществлении кредитными организациями операций с применением систем Интернет-банкинга»;
— Письмо 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»;
— Письмо Банка России от 14 декабря 2012 г. № 172-Т «О Рекомендациях по вопросам применения статьи 9 Федерального закона «О национальной платежной системе»;
— Письмо Банка России от 10 июня 2013 г. № 104-Т «О повышении внимания кредитных организаций к отдельным операциям клиентов»;
— Письмо Банка России от 19 июня 2013 г. № 110-Т «О повышении внимания кредитных организаций к отдельным операциям клиентов»;
— Письмо Банка России от 24 марта 2014 г. № 49-Т «О рекомендациях по организации применения средств защиты от вредоносного кода при осуществлении банковской деятельности».

При создании системы информационной безопасности банковской организации должен быть проведен комплекс работ, включающий в себя выполнение последовательных этапов, обеспечивающих идентификацию информационных активов банка, анализ рисков информационной безопасности, характерных для банка, и предложений эффективных решений для создания системы управления информационной безопасности (СУИБ).

Примерный план выглядит следующим образом:

- создание рабочей группы (комитета) по вопросам обеспечения информационной безопасности;

- идентификация активов и анализ рисков информационной безопасности;
- формирование и внедрение документационной базы;
- информирование и обучение персонала;
- внедрение защитных мер;
- проведение независимой оценки соответствия (самооценки).

Целью создания рабочей группы (комитета) по информационной безопасности является выработка совместных с бизнес-подразделениями решений по обеспечению информационной безопасности. Такой вариант работы позволяет избежать излишней нагрузки на бизнес-подразделения при обеспечении достаточного уровня информационной безопасности. В состав такой группы целесообразно включать представителей следующих подразделений:

- информационной безопасности;
- информатизации;
- внутреннего контроля;
- риск-менеджмента;
- основных бизнес-подразделений.

Курирование деятельности рабочей группы должно осуществляться первым лицом банка или его первым замом.

Отдельный этап формирования надежной системы информационной безопасности — это создание документационного обеспечения СУИБ. Он включать в себя следующие работы:

- обследование информационной системы банка или идентификация активов, что необходимо для составления прогноза (модели угроз и нарушителя) информационной безопасности;
- составление прогноза (модели угроз и нарушителя) информационной безопасности;
- разработка организационно-распорядительной документации по обеспечению информационной безопасности (формирование ПИБ).

Целью обследования информационной системы банка или идентификации активов является сбор и анализ исходных данных об организационной и функциональной структуре информационной системы, необходимых для составления прогноза (модели угроз и нарушителя) информационной безопасности.

В процессе проведения обследования необходимо определить следующие объекты:

- бизнес-процессы;
- учетно-операционная информация;
- информация (данные) информационных, аналитических и иных систем;
- процессы управления;
- технологические процессы сбора, обработки, хранения и передачи информации;
- аппаратно-программные и технические комплексы, обеспечивающие реализацию функций организации, здания и сооружения, где установлены указанные комплексы.

Задачи, решаемые на данном этапе:

- разделение информационных активов на типы (классификация активов);
- отнесение конкретного информационного актива к ранее выделенному типу (типам).

Также на данном этапе проводятся проверка наличия и анализ существующей распорядительно-регламентирующей базы по обеспечению информационной безопасности банка, включающей документы по распределению ролей персонала, документированных правил обращения с информационными ресурсами, включая правила отнесения информации к определенным категориям.

При проведении идентификации активов возможно использовать следующий классификатор:

- платежная информация;
- финансово-аналитическая информация;
- открытая информация;
- управляющая информация общего и специального назначения;
- справочная информация.

При этом целесообразно учитывать степень тяжести последствий от потери значимых свойств информационной безопасности, то есть рассматривать следующие вопросы, возникающие вследствие потери значимых свойств безопасности (целостность, доступность, конфиденциальность) информационного актива:

- степень влияния на непрерывность деятельности организации;
- объем финансовых и материальных затрат, необходимых для восстановления свойств информационной безопасности и ликвидации последствий нарушения информационной безопасности;
- количество дополнительно привлекаемого персонала, необходимого для восстановления свойств информационной безопасности и ликвидации последствий нарушения информационной безопасности;
- объем дополнительных временных затрат, необходимых для восстановления свойств информационной безопасности и ликвидации последствий нарушения информационной безопасности;
- степень нарушения законодательных требований, требований регулирующих и контролирующих органов и (или) договорных обязательств организации.

Рассматривая каждый информационный актив и оценивая степень тяжести последствий, возможно использовать следующее значение величины:

- минимальная;
- средняя;
- высокая;
- критическая.

Такой подход позволит, не прибегая к сложным методикам оценки, выстроить приоритеты обеспечения информационной безопасности для каждого информационного актива в частности и для всех активов банка в целом.

По результатам идентификации активов возможно подготовить модели угроз, а также модели нарушителя. Модели информационной безопасности (угроз и нарушителей) предназначены отражать будущее, вследствие чего они носят прогнозный характер. Модели информационной безопасности разрабатываются на основе фактов прошлого и опыта, но ориентированы на будущее. Чем точнее сделан прогноз (составлены модель угроз и модель нарушителя), тем ниже риски нарушения информационной безопасности в организации

банковской системы Российской Федерации при минимальных ресурсных затратах.

Формируя модель нарушителя, необходимо учитывать следующее. Внутренние нарушители информационной безопасности — это сотрудники банка, осуществляющие в соответствии с предоставленными им правами и полномочиями деятельность по реализации функций и задач банка, а также персонал, обслуживающий аппаратно-программные комплексы (автоматизированные системы) или допущенный к ним, в здания и помещения банка в соответствии со своими служебными обязанностями. Это могут быть специалисты по эксплуатации автоматизированной системы (администраторы автоматизированной системы и их частей, сетевого оборудования, приложений, информационной безопасности и т. д.), пользователи автоматизированной системы, разработчики электронных технологий и программного обеспечения, руководящий и управленческий персонал.

Внешние нарушители информационной безопасности — это сотрудники банка, которым не предоставлены права по доступу к информационным ресурсам, в отдельные здания и помещения банка, а также субъекты, не являющиеся сотрудниками банка, но осуществляющие попытки несанкционированного доступа к указанным ресурсам. К таким нарушителям можно отнести террористов, криминальные элементы, компьютерных злоумышленников и монопольных поставщиков средств, расходных материалов, услуг. А также сотрудников банка — пользователей автоматизированной системы, пытающихся действовать вне рамок предоставленных полномочий.

Как правило, нарушитель имеет следующую мотивацию:

- материальное обогащение;
- морально-психологические мотивы (месть, обида, зависть, психическое расстройство и т. д.);
- идеологические причины (нанесение ущерба организации или банковской системе в целом).

На основе модели информационной безопасности разрабатывается ПИБ (политика информационной безопасности).

ПИБ представляет собой главный нормативный документ, утверждаемый высшим руководством банка. Документ разрабатывается с учетом особенностей деятельности банка, его организаци-

онной структуры, структуры и размещения корпоративной информационной системы и характера решаемых задач.

ПИБ представляет собой одно или несколько правил, процедур и руководящих принципов по информационной безопасности, которыми руководствуется организация в своей деятельности. Использование ПИБ позволяет добиться при минимальных расходах необходимого уровня безопасности, обеспечивающего требуемое доверие в бизнесе, в условиях воздействия актуальных для организации угроз.

ПИБ определяет на высоком (общем) уровне цели и задачи обеспечения информационной безопасности банка, включая способы контроля реализации требований ПИБ. ПИБ банка формируется как один из обязательных документов в соответствии с п. 3.5.5 Положения № 242-П.

ПИБ отражает вопросы обеспечения безопасности во всех областях деятельности банка и на всех участках корпоративной информационной системы:

- на каждом отдельном объекте (центральный офис, подразделения, региональные филиалы, дополнительные офисы);
- при взаимодействии между подразделениями банка;
- при общении с партнерами и клиентами;
- при использовании ресурсов открытых сетей.

При формировании ПИБ необходимо учитывать ряд специальных принципов:

- «Знать своего клиента» (Know your Customer): принцип, используемый регулирующими органами для выражения отношения к финансовым организациям с точки зрения знания деятельности их клиентов;
- «Знать своего служащего» (Know your Employee): принцип, демонстрирующий озабоченность организации по поводу отношения служащих к своим обязанностям и возможных проблем, таких как злоупотребление имуществом, аферы или финансовые трудности, которые могут приводить к проблемам с безопасностью;
- «Необходимо знать» (Need to Know): принцип безопасности, который ограничивает доступ к информации и ресурсам по обработке информации тем, кому требуется выполнять определенные обязанности;

- «Двойное управление» (Dual Control): принцип сохранения целостности процесса и борьбы с искажением функций системы, требующий того, чтобы два лица независимо предпринимали некое действие до завершения определенных транзакций.

ПИБ должна учитывать особенности бизнес-процессов банковской организации. Поэтому особенности ЭБ должны обязательно найти свое отражение в ПИБ:

- При осуществлении ДБО с использованием сети Интернет должны применяться защитные механизмы, предотвращающие возможность подмены авторизованного клиента неизвестным злоумышленником в рамках установленного сеанса работы. Все попытки таких подмен должны регистрироваться регламентированным образом.
- Все операции клиентов во время всего сеанса работы с системами ДБО должны выполняться только после выполнения процедур идентификации, аутентификации и авторизации. В случаях нарушения или разрыва соединения необходимо обеспечить повторное выполнение указанных процедур.
- Для доступа пользователей к системам ДБО рекомендуется использовать специализированное программное обеспечение клиентских мест.

Обязательно следует назначить лиц, ответственных за внедрение и реализацию ПИБ. Это должен быть не просто документ, который будет пылиться на полке до ближайшей проверки, а документ, который должен быть использован на практике. На основе ПИБ разрабатываются остальные документы: положения, регламенты, инструкции, должностные обязанности и т. д.

Таким образом, ПИБ является вершиной документационного обеспечения информационной безопасности в банковской организации. Следующий уровень документов по информационной безопасности — это уровень положений или частных политик, определяющих правила, требования и принципы, используемые применительно к отдельным областям информационной безопасности, видам и технологиям деятельности банка. Он может включать в себя следующие документы:

1. *Положение о конфиденциальной информации.*

Положение устанавливает порядок формирования и использования конфиденциальной информации банка, а также ответственность за ее разглашение.

2. *Положение об идентификации информационных активов.*

Положение о категорировании ресурсов определяет четкий порядок отнесения информации, хранимой и обрабатываемой в корпоративной информационной системе, к различным степеням конфиденциальности. Документ утверждается руководством банка и включает следующие основные разделы:

- категории защищаемой информации/сервисов/серверов (рабочих станций);
- порядок определения категорий защищаемых ресурсов автоматизированной системы;
- перечень должностных лиц, уполномоченных относить информацию к определенным категориям.

3. *ПИБ при использовании ресурсов сети Интернет.*

Данный документ содержит ПИБ при использовании ресурсов сети Интернет и определяет порядок подключения к сети Интернет, а также правила работы пользователей с ресурсами сети Интернет. Целесообразно предусмотреть процедуры контроля использования сети Интернет и ответственность персонала в случае выявления нарушений.

4. *Политика использования электронной почты.*

Документ содержит политику использования электронной почты банка. Он определяет права пользователей при использовании системы электронной почты, порядок использования системы электронной почты, порядок использования защищенных почтовых сообщений. Кроме того, документ должен закреплять порядок организации архива электронной почты и процедуры расследования инцидентов информационной безопасности с использованием этого архива.

Электронная почта — это один из потенциальных источников угроз утечки информации. Поэтому отдельный вопрос — это контроль за использованием электронной почты и уведомление об этом персонала.

5. *Порядок организации парольной защиты.*

Данный документ описывает порядок организации парольной защиты и отражает требования к качеству паролей (длина,

используемые символы, степень отличия от предыдущих паролей и т. п.), требования к частоте смены паролей, требования к сохранности паролей, порядок получения/изменения пароля пользователем, действия пользователя при компрометации пароля. Парольная защита и управление доступом в целом должны предусматривать контроль доступа к ресурсам со стороны подразделения информационной безопасности.

6. *Политика антивирусной защиты.*

Документ устанавливает политику антивирусной защиты банка и отражает требования к составу и размещению средств антивирусной защиты, порядок проведения антивирусных проверок компонентов информационной системы (рабочих станций, серверов), проверок используемых носителей и данных, получаемых извне, и порядок действий пользователей и администраторов в случае обнаружения вирусов. Целесообразно предусмотреть включение в должностные обязанности сотрудников обязанностей по антивирусной защите. При организации антивирусной защиты необходимо придерживаться принципа эшелонированной защиты, то есть, во-первых, использовать антивирусные средства разных вендоров, а во-вторых, устанавливать антивирусные средства во всех критичных точках сети: на средствах защиты периметра (межсетевые экраны), на почтовых и файловых серверах и на рабочих станциях пользователей.

7. *Положение по использованию средств криптографической защиты информации.*

Данное положение содержит основные правила использования средств криптографической защиты информации (СКЗИ) в банке, устанавливает общие требования, предъявляемые к действиям ответственных лиц при работе с СКЗИ — секретными и открытыми ключами шифрования, электронной цифровой подписью, а также аппаратными средствами для различных систем криптографической защиты электронного документооборота банка.

Особое внимание использованию СКЗИ следует уделить в условиях ЭБ.

Понятно, что схема ЭБ, помимо неоспоримых пользовательских преимуществ (отказ от бумажной технологии информационного обмена, отсутствие необходимости личного присутствия при обращении

за банковской услугой и т. п.), содержит значительные риски как для клиентов банка, так и для самой кредитной организации, связанные, в первую очередь, с попытками осуществления мошеннических банковских операций по счетам клиентов, проведения по клиентским счетам сомнительных операций, не соответствующих хозяйственной деятельности клиентов, осуществлением неправомерных попыток получения сведений, составляющих банковскую тайну или персональных данных клиентов, а также попыток дезорганизации бесперебойной работы системы банковского обслуживания.

Наличие указанных рисков требует от кредитных организаций, предоставляющих услуги ЭБ, создания специализированной эффективной системы обеспечения информационной безопасности процессов электронного взаимодействия с клиентом, включающей в себя как организационные и правовые аспекты, так и использование программно-технических средств защиты, включая средства криптографической защиты информации.

Наиболее трудной проблемой при ЭБ является проблема идентификации лица, отдающего распоряжение на проведение операции (проверка его полномочий), а также аутентификация электронного сообщения (ордера клиента), содержащего конкретные реквизиты, необходимые для проведения банковской операции (аутентификация электронного сообщения — процедура контроля целостности и подтверждения его подлинности). В определенных случаях для достижения целей безопасности при проведении операций ЭБ используются специальные выделенные телекоммуникационные сети, специализированные терминальные устройства и вводятся существенные ограничения на спектр банковских услуг, оказываемых при ЭБ, однозначно оговариваемых в заключаемых договорах на обслуживание с использованием СЭБ. В этих случаях достаточно эффективно могут работать системы обслуживания, использующие коды, пароли и другие некриптографические способы идентификации и аутентификации клиентов и электронных сообщений. Примеры таких систем ЭБ — банкоматы, услуги «мобильный банк» и т. п.

В тех случаях, когда услуги ЭБ предоставляются с использованием общедоступных сетей телекоммуникаций, например Интернета, обеспечение информационной безопасности без использования средств криптографической защиты практически невозможно. Для

обеспечения информационной безопасности в банковских системах в основном используются два типа средств криптографической защиты: средства шифрования и средства аутентификации типа электронной подписи.

Средства шифрования (программные и программно-аппаратные) применяются для целей обеспечения конфиденциальности передаваемой по каналам связи информации, а также для создания доверенных подсистем передачи на базе общедоступных сетей связи (так называемые VPN-сегменты). Средства шифрования зачастую включаются в состав межсетевых экранов, придавая системам обеспечения контроля доступа во внутренние локальные сети свойства организации VPN-систем.

Применение средств шифрования позволяет обеспечить как конфиденциальность всей передаваемой с их использованием информации, так и возможность идентификации лица, передавшего сообщение, то есть обеспечивается полная защита от третьих лиц. Вместе с тем шифрование не позволяет контролировать целостность передаваемой информации (при передаче возможны искажения шифртекста, приводящие к изменению смысла принятой информации, кроме того, получатель имеет возможность корректировать полученное электронное сообщение, выдавая его за принятое). Таким образом, шифрование не обеспечивает защиту сообщений «друг от друга».

Во многих западных системах ЭБ используются криптографические системы, основанные только на применении средств шифрования с введением дополнительной функции контроля целостности принятого сообщения за счет применения специальных криптографических контрольных сумм сообщений, называемых кодами аутентификации сообщений (MAC — messenger autentification cod), которые в нашей криптографической литературе называются имитовставками.

Отечественные системы криптографической защиты, как правило, механизм имитовставок используют только для контроля целостности служебных электронных объектов, возникающих в процессе эксплуатации криптосистемы (различные справочники и проч.). Для целей аутентификации электронных сообщений в отечественных криптосистемах применяется алгоритм электронной подписи,

изложенный в ГОСТ 28147–89. Использование алгоритма электронной подписи, обычно, приводит к удорожанию системы обеспечения информационной безопасности, так как по сравнению с имитовставками увеличивается время вычисления электронной подписи и ее проверки. Кроме того, для эффективного использования механизмов электронной подписи необходимо создание специальной системы управления ключами электронной подписи, что предполагает дополнительные затраты.

Использование отечественных сертифицированных средств шифрования и электронной подписи в сочетании с четко прописанными в договорах с клиентами правилами их использования и правилами разбора конфликтных ситуаций, основанных на проверке электронной подписи, позволяет надежно защитить систему ЭБ от попыток хищения денежных средств со счетов клиентов за счет использования фальшивых распоряжений клиентов, а также оградить кредитные организации от возможных мошеннических действий представителей клиента.

Выбор конкретных средств криптографической защиты определяется в первую очередь техническими характеристиками криптоустройств и их согласованием со средствами связи и обработки электронной информации. Кроме того, необходимо оценить систему управления ключами предлагаемой криптосистемы как с точки зрения возможностей ее технической реализации на существующей базе, так и с точки зрения обеспечения специалистами соответствующего уровня в узловых точках работы с клиентами.

Таким образом, при использовании телекоммуникационных сетей общего пользования (типа Интернет) доступ к СЭБ должен осуществляться с использованием отечественных сертифицированных средств шифрования и средств аутентификации, построенных на алгоритме электронной подписи.

Стойкость любой криптографической системы, реализованной на алгоритмах шифрования и электронной подписи, построенных на основании ГОСТ 28147-89 и ГОСТ 34.10-2001 соответственно, определяется выбором ключевой системы и сохранением в тайне действующих ключей шифрования и ключей кодов аутентификации. Наиболее предпочтительной является следующая организация ключевой системы:

- Ключи шифрования вырабатываются организатором связи централизованно (например, в головном офисе) в количестве, достаточном для обеспечения ими всех клиентов и наличия необходимого запаса для возможности подключения новых клиентов и для замены ключей у корреспондентов сети при возможной компрометации действующих ключей. Срок действия ключей шифрования определяет организатор связи, исходя из возможностей оперативной доставки их до корреспондентов, но не более одного года. Каждому клиенту выдается комплект ключей шифрования (включая резервные), необходимых для доступа к услугам ЭБ. Комплект ключей должен выдаваться представителю клиента, имеющему соответствующую доверенность на получение ключей, под роспись (в акте приема-передачи ключей либо в специальном журнале выдачи ключей). Каждому клиенту целесообразно вместе с ключами передавать памятку пользователя, содержащую основные требования обращения с ключевыми носителями.
- Ключи кодов аутентификации (электронную подпись) каждый клиент должен изготавливать самостоятельно. Целесообразно изготовление сразу двух комплектов ключей кодов аутентификации (КА) — один рабочий, другой — резервный, ввод в действие которого производится в случае компрометации рабочего ключа. Изготовленный ключ КА состоит из двух частей. Первая часть ключа — персональный ключ — является конфиденциальной частью ключа КА, известной только владельцу ключа КА. К этой части ключа должны быть допущены только те специалисты клиента, в отношении которых отдано особое распоряжение руководства клиента.

Вторая часть ключа КА — публичный (открытый) ключ — должен быть зарегистрирован в регистрирующем центре организатора связи и после регистрации помещен в справочник открытых ключей, предоставляемый всем участникам электронного обмена, которым по технологии поручена проверка корректности кодов аутентификации (электронной подписи) поступающих электронных сообщений. Для регистрации ключа изготавливается регистрационная карточка

в двух экземплярах, один из которых остается в регистрационном центре, другой возвращается клиенту. Регистрационные центры открытых ключей КА (электронной подписи) целесообразно организовать в каждом филиале кредитной организации, в котором будут заключаться договоры с клиентами на доступ к СЭБ. При этом целесообразно организовать регистрацию ключа КА таким образом, чтобы на его регистрацию являлось физическое лицо, которое заключило договор и чей образец подписи содержится в досье на клиента. В этом случае появляется возможность регулярно подтверждать идентификацию клиента, заключившего договор на использование СЭБ. Срок замены ключа КА (электронной подписи) устанавливается в договоре на использование СЭБ и может варьироваться в зависимости от степени надежности клиента, но не должен превышать одного года. Если клиент не перерегистрировал открытый ключ КА (электронную подпись) в установленные сроки, то он отключается от доступа к системе ДБО до тех пор, пока не явится для регистрации нового ключа КА.

Предлагаемая система регистрации открытых ключей КА (электронной подписи), на наш взгляд, может являться одной из форм реализации рекомендаций Центрального банка Российской Федерации, изложенных в Письме Банка России от 27 апреля 2007 г. № 60-Т «Об особенностях обслуживания кредитными организациями клиентов с использованием технологии дистанционного доступа к банковскому счету клиента (включая интернет-банкинг)».

Таким образом, правильный выбор ключевой системы шифрования и системы аутентификации позволяет существенно понизить риски мошенничества в системе ДБО, а также репутационный риск кредитной организации в случаях проведения клиентом сомнительных операций через СЭБ.

Наконец, третьим важным аспектом использования средств криптографической защиты в СЭБ является проведение необходимых организационно-технических мероприятий, направленных на обеспечение бесперебойности работы СЭБ. К основным мероприятиям в этом направлении необходимо отнести следующие:

- В кредитной организации, предоставляющей услуги ЭБ, должен быть сформирован пакет внутренних документов, регламентирующих состав и содержание операций, совершаемых

с использованием СЭБ, перечни и характеристики используемых при этом технических и программных средств (включая криптографические средства и другие средства обеспечения информационной безопасности), а также процедуры идентификации клиентов и аутентификации электронных сообщений клиентов.

- Договор с клиентом на подключение к СЭБ должен содержать все необходимые обязательства сторон по соблюдению системы обеспечения информационной безопасности, а также раздел разбора конфликтных ситуаций, которые могут возникнуть в ходе работы в режиме ЭБ, включая разбор конфликтов с использованием средств криптографической защиты (КА, электронной подписи).
- Наличие у сторон необходимой нормативной, технологической и эксплуатационной документации на всю систему обеспечения безопасности СЭБ, включая средства криптозащиты. Наличие необходимых распорядительных документов у клиента по назначению администраторов информационной безопасности, по допуску сотрудников к ключевым носителям, а также по действиям персонала в случаях компрометации ключей.
- Обеспеченность рабочих мест, использующих средства криптозащиты, надежными металлическими хранилищами ключевых носителей с возможностью их опечатывания.
- Специалисты, допущенные к работе с ключевыми элементами и средствами криптозащиты, должны иметь соответствующую подготовку для самостоятельной работы.
- Автоматизированные рабочие места, на которых установлены средства криптографической защиты, должны быть оснащены средствами защиты от несанкционированного доступа, включающими в свой состав средства контроля программного обеспечения автоматизированных рабочих мест (защита от программ-закладок, которые могут нарушить регламентированный ход обработки информации на рабочем месте).
- Доступ к серверам СЭБ должен быть защищен не менее чем двумя устройствами типа межсетевых экранов, один

из которых целесообразно выбирать с реализованной функцией криптозащиты для организации VPN-сегментов сети.

- Кредитной организации, предоставляющей услуги ЭБ, целесообразно открыть в Интернете общедоступный информационный сайт, на котором размещать необходимую нормативно-справочную информацию по СЭБ, правила доступа клиентов к услугам ЭБ с указанием мер информационной безопасности, информацию для клиентов о возможных способах мошенничества в СЭБ, ориентированных на хищение персональных данных клиентов или хищение денежных средств со счетов клиентов, а также рекомендации клиентам по мерам предосторожности, которые необходимо соблюдать для противодействия мошенникам.

8. *Регламент реагирования на нарушения информационной безопасности.*

Документ определяет порядок и процедуры реагирования на нарушения режима информационной безопасности в информационной системе банка. Он содержит:

- описание порядка организации планирования и выделения ресурсов, необходимых для реагирования на нарушения информационной безопасности;
- порядок профилактики и предотвращения нарушений информационной безопасности;
- порядок реагирования на нарушения информационной безопасности;
- описание процесса ликвидации последствий инцидента.

9. *Соглашение о контроле использования служебных сервисов.*

В документе приводится соглашение о контроле использования служебных сервисов информационной системы банка. Данное соглашение заключается со всеми сотрудниками, допущенными к работе с основными служебными сервисами информационной системы банка для выполнения своих должностных обязанностей. Оно устанавливает порядок использования, методы контроля, а также ответственность за несанкционированное использование сотрудниками основных служебных сервисов информационной системы.

Отдельный вопрос информационной безопасности — информирование персонала о вопросах информационной безопасности.

Плотная работа подразделения информационной безопасности с подразделением персонала должна быть направлена на то, чтобы информационная безопасность стала элементом корпоративной культуры. Это достигается обучением и информированием персонала в области информационной безопасности и соблюдением требований информационной безопасности. Положительный эффект дает такая форма работы, как «Памятка по информационной безопасности». В простой форме персонал информируется о том, на что надо обратить внимание в повседневной работе с точки зрения информационной безопасности и кого известить в случае возникновения происшествий или инцидентов информационной безопасности.

Обработка инцидентов информационной безопасности должна строиться на тех же принципах, что и обработка ИТ-инцидентов. Поэтому логично избежать дублирования функций, так как у ИТ-подразделений, как правило, есть отработанная технология управления ИТ-инцидентами. В связи с этим основной идеей, описывающей данную процедуру, является создание единой точки контакта — диспетчерской службы — для обращений пользователей, администраторов ресурсов, где произошел инцидент информационной безопасности, администраторов подсистем информационной безопасности по факту наступления инцидента информационной безопасности, регистрации заявки, классификации заявки, назначения ответственного исполнителя заявки, решения инцидента информационной безопасности ответственными сотрудниками, мониторинга хода работ, закрытия заявки и создания отчетов.

Это решение позволяет учесть интересы подразделений информационной безопасности в обработке инцидентов информационной безопасности и полностью реализовать механизм управления инцидентами информационной безопасности.

В большинстве многофункциональных банковских организаций внедрена Служба поддержки Service Desk, в обязанности которой входит управление инцидентами в области информационных технологий. Процедура управления ИТ-инцидентами регулируется стандартом ISO/IEC20000:2005, пришедшим на смену BS15000:2002, который, в свою очередь, взял за основу библиотеку ITIL. Естественно, что ISO 20000 описывает как систему управления ИТ-сервисами, так и процедуру управления инцидентами, но также рассматривает

ИТ-инциденты. Сама процедура управления ИТ-инцидентами очень близка к процедуре управления инцидентами информационной безопасности с той лишь разницей, что в последнем случае больший упор делается на расследование инцидента, сбор улик, наказание виновных (вплоть до обращения в суд).

Поэтому целесообразно разработать и применить «единую точку контакта» — диспетчерскую службу — для построения процесса управления всеми инцидентами в организации банковской системы, которая обеспечит учет интересов подразделений информационной безопасности и обработку инцидентов информационной безопасности.

Процесс управления инцидентами информационной безопасности в многофункциональном банке должен быть подробно задокументирован.

Основной задачей процесса управления инцидентами информационной безопасности является восстановление нормального предложения услуги настолько быстро, насколько это возможно, с минимальным негативным воздействием на бизнес-процесс и систему безопасности, поддерживая, таким образом, предоставление услуги в соответствии с уровнем, оговоренным в регламенте.

Процесс управления инцидентами информационной безопасности должен наилучшим образом использовать ресурсы информационных технологий для поддержки основной деятельности банка, разработки и поддержки базы данных об инцидентах информационной безопасности, разработки и применения последовательного подхода к обработке и устранению всех зарегистрированных инцидентов информационной безопасности.

Процесс управления инцидентами информационной безопасности обеспечивает единую точку контакта с пользователями бизнес-подразделений банка.

Процесс управления инцидентами информационной безопасности отвечает за обнаружение и запись, классификацию, начальную поддержку, исследование и диагностику, разрешение и восстановление, закрытие инцидентов, их мониторинг, отслеживание и коммуникацию.

Процесс управления инцидентами информационной безопасности строится на следующих принципах:

- Все возникающие инциденты информационной безопасности должны быть зафиксированы.
- Должна существовать известная всем потребителям единая точка контакта с поставщиком услуги.
- Для минимизации и управления влиянием инцидентов информационной безопасности на бизнес должны существовать соответствующие процедуры. Процедуры должны фиксировать порядок регистрации, определения приоритетов, оценки действия на бизнес, классификации, обновления, эскалации, решения и формального закрытия всех инцидентов информационной безопасности.
- Пользователь бизнес-подразделений должен информироваться о ходе работ по инцидентам информационной безопасности или заявкам на услуги. Потребитель должен быть заранее предупрежден, если согласованный для него уровень услуг не может быть предоставлен, а также должен быть в курсе предполагаемых действий по достижению согласованных параметров.
- Весь персонал, привлекаемый к устранению инцидентов в области информационной безопасности, должен иметь доступ к соответствующей информации, такой как известные ошибки, способы решения проблем, а также база данных по управлению конфигурацией.
- Должен существовать механизм привлечения дополнительной компетенции к решению инцидентов информационной безопасности.
- Нештатные ситуации должны быть классифицированы и должны управляться согласно особо определенному процессу.

При организации процесса управления инцидентами информационной безопасности надо помнить, что события информационной безопасности фиксируются не только пользователями, но и техническими средствами обеспечения информационной безопасности. Поэтому диспетчерская служба должна иметь инструкции по порядку реагирования на инциденты, выявляемые и фиксируемые техническими средствами.

Обязательным элементом информационной безопасности является контроль состояния информационной безопасности и оценка соответствия информационной безопасности банковской организации требованиям и рекомендациям нормативных документов на уровне государства и регулятора банковского сектора.

Контрольные мероприятия, как и весь процесс информационной безопасности в целом, должны соответствовать циклическому процессу менеджмента информационной безопасности организации (модель Деминга, рис. 14).

В ходе организации контрольных мероприятий следует учитывать следующие обязательные этапы:

- планирование;
- проведение;
- обобщение, анализ и подготовка выводов;
- доклад вышестоящей инстанции;
- планирование работ по корректировке политики безопасности.

Иерархия контрольных мероприятий представлена на рис. 15.

Контроль со стороны службы безопасности должен включать:

- контроль выполнения регламентов (парольная защита, антивирусная защита, использование Интернета, обновления программного обеспечения и т. д.);
- контроль локальных настроек (операционные системы, прикладное программное обеспечение автоматизированной системы, средства защиты, активное сетевое оборудование и т. д.);

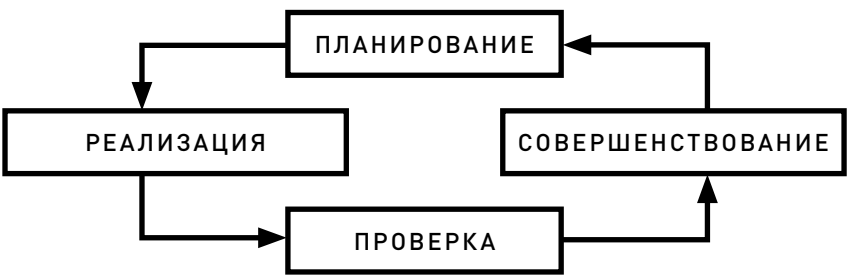

Рис. 14. Модель Деминга

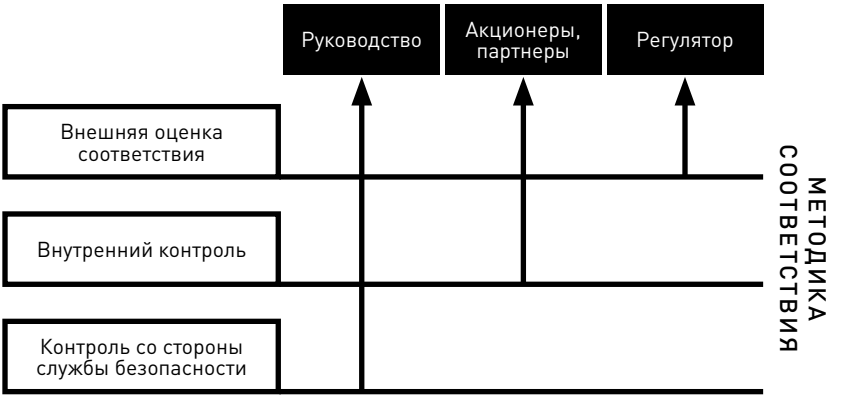

Рис. 15. Иерархия контрольных мероприятий

- контроль действий пользователей и администраторов в автоматизированных системах;
- анализ защищенности с использованием специализированных средств.

Кроме того, хорошей практикой является согласование с СИБ технических заданий на создание, проектирование, тестирование и приемку автоматизированных систем в банковской организации.

7. О СРЕДСТВАХ И СПОСОБАХ ЗАЩИТЫ ИНФОРМАЦИИ

«Быть не надо
ученым
крупным,
Чтоб усвоить
наверняка:
Если данные
общедоступны,
То цена их
невелика».

Экономические основы защиты информации

«Программой программу нельзя защищать:
Бессмысленна эта работа!
Только Мюнхгаузен может поднять
Себя самого из болота!»

Физические и метафизические основы защиты информации

Введение

Исторически получилось так, что современные компьютеры являются реализацией идеи «машины Тьюринга», то есть универсального исполнителя. Это означает, что принципиально они созданы так, чтобы выполнить любую задачу. Любую, а не только те, что мы бы хотели.

Удивительно, что, скорее всего, не обладая в большинстве своем знаниями о машине Тьюринга и ее особенностях, эту довольно специфичную проблему компьютерной безопасности хорошо чувствуют гуманитарно ориентированные люди — писатели, поэты, римские папы — формулируя в тех или иных словах, что компьютеры могут все, и наша задача — заставить их делать только то, что нам нужно, не дать им делать все. Мы, пожалуй, довольно далеки от опасений насчет бунта компьютеров и захвата ими власти над миром, но полностью разделяем убежденность в том, что универсальность

современных компьютеров является основным источником всех связанных с компьютерной сферой угроз. Если компьютер способен выполнить любую задачу, то он выполнит и вредоносную.

Именно в этом состоит цель мероприятий по обеспечению ИБ, если посмотреть на нее с определенной дистанции: нам необходимо добиться того, чтобы все наши (то есть легальные) задачи решались, а задачи злоумышленников (нелегальные) — не решались.

Отсюда распространенное убеждение о том, что все задачи защиты информации сводятся к управлению доступом субъектов к объектам. Это не вполне так, к этому сводятся не все задачи.

Если пытаться уложить деятельность по защите информации в некую максиму, то скорее она будет звучать так: защита информации — это ограничение универсальности средств вычислительной техники.

В этой главе изложим тезисно основные направления этого ограничения.

Пытаясь защититься от вредоносных хакерских программ, человечество уже более 60 лет разрабатывает программы, традиционно относимые к области защиты информации — средства идентификации, аутентификации, авторизации, контроля целостности, антивирусные программы, криптографические средства и т. д. Использование этих средств отчасти приносит положительный эффект, но очень и очень отчасти. Действуя в рамках пусть универсальной, но одной формальной модели, мы неизбежно натолкнемся на ее неполноту — в полном соответствии с теоремой Геделя[103] о неполноте.

Становится очевидным, что искать уязвимости только в программном обеспечении явно недостаточно.

Универсальность компьютера обеспечивается архитектурно, самой «конструкцией» машины Тьюринга, как мыслимой в абстракции, так и реализованной на практике.

Поскольку архитектуру нельзя изменить программным путем, то никакие программные средства не помогут нам защититься

103 Коротко эта теорема Курта Геделя сводится к тому, что если система S непротиворечива, то в ней обязательно есть формула A, которая неопровержима и недоказуема в рамках системы S.

от хакеров надежно. Игра «кто кого» продолжается уже много лет, давая работу сотням тысяч специалистов по ИБ, но не спасая нас от потерь.

Как же быть?

Если уязвимость в архитектуре — то и совершенствовать нужно архитектуру.

И здесь мы подходим к первому, самому радикальному разделению направлений. Мы можем:

1. Усовершенствовать архитектуру уже существующих технических средств.
2. Использовать новые технические средства на базе новой, более совершенной архитектуры.

Следуя первому направлению, эксплуатирующие организации, приобретая новую технику, устанавливают на нее те или иные средства защиты, следуя второму — приобретают технику, спроектированную тем или иным особым образом.

И в том и в другом направлении на рынке представлены как добросовестные и эффективные решения, так и не совсем отвечающие этим свойствам. Ниже о решениях первого класса, так как разоблачения не входят в состав задач данной книги.

7.1. Наложенные средства защиты информации

Для того чтобы действовать в парадигме утверждения «компьютер — это только инструмент», необходимо иметь возможность убедиться, что это именно ваш инструмент, а не того, кто модифицировал его для выполнения собственных задач, возможно, далеко не совпадающих с задачами легального пользователя.

Чтобы убедиться в неизменности аппаратной и программной среды компьютера, необходимо провести контрольные процедуры. Однако очевидно, что если контрольные процедуры производятся измененным в свою очередь компонентом, то в них нет никакого смысла.

Именно поэтому контролировать неизменность среды нельзя программными средствами — так как программа может быть изменена. Для того чтобы убедиться, что она не была изменена, — ее нужно сначала проверить. Если ее мы проверяем другой программой, то сначала нужно проверить ту программу, которой мы проверяем первую… и т. д. Мы попадаем в зону действия известного парадокса «кто будет сторожить сторожей?». В защите информации попытки контролировать целостность среды программными средствами носит название «синдром Мюнхгаузена», поскольку они аналогичны попыткам вытащить себя самого из болота за волосы.

Продолжая эту аналогию, легко прийти к правильным выводам: вытащить себя из болота за волосы — нельзя, потому что нет точки опоры. А вот если тянуть за ветку дерева, растущего на кочке, — то можно, потому что у дерева есть точка опоры.

Что может означать «точка опоры» применительно к компьютерной системе фон-неймановского типа (а абсолютное большинство современных настольных компьютеров имеют именно такую архитектуру), не различающей команды и данные, системе, в которой одним из основных действий является «запись», то есть системе, принципиально модифицируемой?

«Точка опоры» может означать только одно: контролирующие процедуры должны быть вынесены из этой модифицируемой среды в среду немодифицируемую и легко проверяемую, то есть простую, небольшую по объему (тогда легко обеспечить ее верифицируемость). Это означает аппаратное устройство, независимое от компьютера, который оно проверяет.

Независимость контролирующего устройства — обязательное требование: если часть процедур или решений об обработке их результатов вынесены в основной (контролируемый) компьютер, то модифицированной системой могут быть навязаны любые результаты контроля. Эффект от применения аппаратуры сведется к нулю.

И наконец, самое главное — независимое аппаратное контролирующее устройство должно стартовать первым, до старта операционной системы, иначе у модифицированной системы будет возможность отключить контроллер. «Кто первый встал, того и тапки». Стартовать первым должно то, чему мы доверяем.

Такое аппаратное, простое, независимое от компьютера контролирующее устройство, стартующее первым, до загрузки операционной системы (ОС) компьютера, — называется резидентный компонент безопасности (РКБ).

Резидентный компонент безопасности — это встроенный в вычислительную систему объект, способный контролировать целостность среды путем сравнения ее параметров с эталонными.

Задача РКБ — сделать так, чтобы на этапе прохождения контрольных процедур защищаемый компьютер не был универсальным, или «машиной Тьюринга», а потом, после их успешного завершения, пользователю снова становились доступны все плюсы универсальности.

Ключевые характеристики РКБ:

- это устройство памяти с очень высоким уровнем защищенности (его внутреннее программное обеспечение (ПО) должно быть немодифицируемым);
- примитивное (иначе обеспечение его собственной защищенности эквивалентно задаче защиты компьютера, который он защищает);
- встроенное в контролируемую систему и стартующее до старта основной ОС (иначе его функционирование будет необязательным);
- независимое от контролируемой системы (функционирующее автономно);
- перестраиваемое (то есть предполагающее функционирование в режиме управления, когда возможно изменение политик (только специальным привилегированным пользователем) и в пользовательском режиме, когда изменение политик невозможно, и осуществляется только контроль их выполнения).

Концепция РКБ реализована во всех решениях, которые описаны в этом разделе. Каждое из них включает в себя аппаратный компонент (базис) и может включать в себя программную надстройку, неразрывно связанную с этим базисом.

7.1.1. Аппаратный модуль доверенной загрузки

Первым, с чего началась практическая реализация парадигмы аппаратной защиты в нашей стране и в мире, стало средство защиты информации от несанкционированного доступа (СЗИ НСД) «Аккорд-АМДЗ», положившее начало линейке «Аккорд».

«Аккорд-АМДЗ» — это аппаратный модуль доверенной загрузки, РКБ, обеспечивающий тот самый «правильный старт» компьютерной системы, доверенную загрузку ОС.

Доверенная загрузка — это загрузка различных операционных систем только с заранее определенных постоянных носителей (например, только с жесткого диска) после успешного завершения специальных процедур: проверки целостности технических и программных средств компьютера (с использованием механизма пошагового контроля целостности) и идентификации/аутентификации пользователя.

«Аккорд-АМДЗ» может быть реализован на различных контроллерах, но его базовая функциональность всегда остается одинаковой и соответствует заявленной и отраженной в сертификатах соответствия.

Выбор контроллера зависит в первую очередь от того, свободный слот с каким шинным интерфейсом есть у средства вычислительной техники (компьютера, сервера, ноутбука, моноблока), в которое вы планируете установить «Аккорд-АМДЗ».

Это могут быть:

- PCI или PCI–X — контроллеры Аккорд-5MX или Аккорд-5.5;
- PCI-express — контроллеры Аккорд-5.5.e или Аккорд-GX;
- Mini PCI-express — Аккорд-GXM;
- Mini PCI-express half card — контроллер Аккорд-GXMH;
- m.2 — контроллер Аккорд-GXm.2.

Существует также вариант исполнения «Аккорд-АМДЗ» на базе USB-устройства, которое называется «Инаф» (от англ. enough — достаточно). Этот вариант имеет определенные ограничения, которые должны восполняться организационными мерами или применением дополнительных механизмов, однако в ряде случаев его вполне достаточно, отсюда и название.

«Аккорд-АМДЗ» контролирует только старт компьютера и не работает в ОС. Поэтому в тех случаях, когда необходимо не только загрузить доверенную среду, но и разграничить доступ к ресурсам компьютера уже в ходе работы пользователей, особенно при многопользовательском режиме работы или в распределенных инфраструктурах, необходимо применять программно-аппаратные комплексы на базе «Аккорд-АМДЗ» — ПАК «Аккорд-Win32», «Аккорд-Win64» или «Аккорд-X». Они предназначены для разграничения доступа соответственно в 32-х и 64-х разрядных ОС Windows и в ОС Linux.

Функциональность комплексов одинакова — в них реализованы дискреционный (с использованием 13 атрибутов) и мандатный механизмы разграничения доступа, в том числе контроль печати из любых приложений на принтеры любых типов (сетевые, локальные, виртуальные).

Для терминальных систем как на базе Microsoft, так на базе Citrix, предназначены версии TSE (Terminal Server Edition) поддерживающие управление терминальными сессиями. Серверные и клиентские компоненты комплексов взаимодействуют в рамках протоколов ICA или RDP, формируя собственный виртуальный канал.

За счет совокупности своих функций, включающих, в частности, и контроль запуска задач в программной части комплекса, ПАК СЗИ НСД Аккорд позволяет блокировать атаку на «перехват управления», на которой, в свою очередь, базируется большая часть хакерских атак.

Схема атаки обычно выглядит так:

s1) внедряется и размещается в оперативной памяти вредоносное ПО (ВрПО);

s2) внедряется и размещается в оперативной памяти вредоносный обработчик прерываний;

s3) записываются в долговременную память ВрПО и обработчик прерываний;

s4) с помощью любого доступного механизма вызывается прерывание (например, с помощью DDOS-атаки);

s5) внедренный ранее обработчик прерываний срабатывает и передает управление ВрПО;

s6) ВрПО выполняет свою функцию (например, реализует разрушающее программное воздействие).

Здесь s1–s3 — это шаги по подготовке атаки, s4 — инициирование атаки, s5 и s6 — собственно использование архитектурной уязвимости.

Для того чтобы обезвредить шаги s1 и s2, обычно используются антивирусные программы. Иногда это бывает полезным, но только иногда — так как невозможно с помощью антивирусных программ выявить все ВрПО. Более того, специалистам известны конструкции ВрПО, которые точно нельзя обнаружить. Можно даже сказать, что компьютерные вирусы и в целом ВрПО удается обнаружить только в силу их несовершенства. В общем случае всегда можно разработать такое ВрПО, которое не может быть обнаружено с помощью антивирусных программ сигнатурного поиска, эвристических анализаторов и поведенческих блокираторов.

Блокирование последствий выполнения шага s3 выполняется при последующей загрузке с помощью механизмов контроля целостности — по сути, ревизоров, определяющих, есть ли изменения в составе данных; иногда эта проверка выполняется с помощью тех же наборов антивирусных программ, но это слабое решение, так как проверка должна выполняться до загрузки ОС, а программы, в том числе и антивирусные, работают под управлением ОС.

Генерация события на шаге s4 частично блокируется с помощью специальных средств анализа трафика, устанавливаемых как в сети, так и на клиентских компьютерах. Важно то, что пока нет средств, позволяющих гарантированно блокировать эту уязвимость.

Негативные последствия шагов s5 и s6 блокируются с помощью механизмов контроля запуска задач (процессов, потоков). Это очень эффективные механизмы, но реализующие их средства, в том числе и «Аккорд», довольно дорогие и для их настройки нужно быть специалистом в компьютерных технологиях и ИБ.

Поскольку некоторые из перечисленных функций безопасности должны выполняться до загрузки ОС, то реализовать их можно только с помощью сложного устройства, и нельзя реализовать программно.

Эффективность СЗИ НСД «Аккорд» связана с тем, что он блокирует уязвимости, связанные с нарушением целостности, и создает

доверенную среду для работы программных средств, обеспечивающих защиту компьютера на шагах s1–s6.

Несмотря на большую распространенность, цена СЗИ НСД «Аккорд» довольно высока, и его настройка — дело для профессионалов. Конечно, это лучшее решение для корпоративного применения, но ожидать его применения от, например, физических лиц — клиентов ДБО совершенно невозможно.

Сложность его связана именно с тем, что нужно «изменить» фон-неймановскую архитектуру защищаемого компьютера: нужно добавить неизменяемую память, разделить потоки команд и данных, исполнить контрольные процедуры в доверенной среде до запуска ОС и многое другое, чтобы в момент старта компьютер не был «машиной Тьюринга».

Для виртуальных инфраструктур, на которых сейчас все чаще строятся ЦОДы, в линейке «Аккордов» предназначены программно-аппаратные комплексы «Аккорд-В» и «ГиперАккорд». Первый предназначен для виртуализации на базе VMware, второй — для виртуализации на базе Microsoft.

7.1.2. Защита клиентских рабочих мест

Работа конечных пользователей с центром обработки данных (ЦОДом) может строиться несколькими различными способами: работа с виртуальными рабочими станциями, работа на основе терминального доступа, web-доступа или смешанно. Во всех этих случаях пользователь физически работает на каком-то средстве вычислительной техники (СВТ), и оно также является объектом защиты, поскольку именно с него осуществляется доступ к защищаемому ЦОДу. Система защиты должна учитывать все нижеперечисленные требования:

- доступ к системе должен осуществляться из доверенной среды, которая, в свою очередь, должна обеспечиваться на клиентских средствах вычислительной техники;
- внедрение системы защиты не должно вести к замене оборудования, не вышедшего еще из строя, даже если это «зоопарк» разных СВТ с разными ОС;

- защищенный доступ к системе не должен быть разорван с подсистемой разграничения доступа в самой системе.

Системы, работающие с ЦОДами, хороши тем, что позволяют использовать в качестве клиентов практически что угодно. В первую очередь это значит, что можно использовать все, что уже никому не нужно, а выбросить жалко. Это очень важно, однако это далеко не единственный плюс такой неприхотливости терминальных систем.

Кроме возможности использования машин, которые иначе можно только выбросить (и сохранения инвестиций за счет этого), в качестве терминальных клиентов можно использовать и машины, которые обладают прекрасными характеристиками и возможностями. Это позволяет учесть разнородность служебных функций сотрудников организации, а значит, создать терминальную систему, в которой могли бы работать все сотрудники, даже те, кто в силу своих задач не может работать на терминале типа «тонкий клиент».

Можно отказаться от того, чтобы такие сотрудники работали в режиме терминального доступа, однако это заметно снизит эффект от внедрения системы, поскольку использование централизованного ресурса наиболее значимо как раз для тех задач и данных, которые являются общими для сотрудников всех категорий.

Использование в качестве терминального клиента не только специализированных аппаратных терминалов, но и разнообразных средств вычислительной техники (СВТ) — как с высокими, так и с практически отсутствующими характеристиками — позволит избегнуть двух главных проблем, с которыми сталкиваются организации, эксплуатирующие системы терминального доступа, стремящиеся к унификации терминальных клиентов:

1) монопольный поставщик терминалов (с ним может случиться неприятность, или он может начать вести себя не совсем хорошо);
2) постоянные обновления модельного ряда терминалов, чем грешат практически все «бренды» (а в результате либо теряется преимущество унификации, либо внезапно снятую с производства модель необходимо разыскивать чуть ли не «с рук»).

Заметим, что есть производители, грешащие тем, что и терминалы одной модели, абсолютно идентичные по всем параметрам

спецификации, оказываются на поверку не имеющими между собой ничего общего (и даже реализованными на разных чипсетах). Однако это уже, как говорится, другая история.

Итак, возможность строить систему на разнородных СВТ — очень существенный плюс. Однако в тени этого плюса скрывается сложность, связанная с тем, что *среда исполнения* терминального клиента во всех этих случаях (на подлежащих списанию ПЭВМ под Windows XP, мощных машинах проектировщиков под каким-нибудь специфическим Linux, ноутбуке руководителя с Windows 8, ноутбуках или планшетах агентов или инспекторов — вовсе с гарвардской архитектурой) окажется разной.

Это не проблема, если в терминальной системе не нужно обеспечивать ИБ, так как клиенты ICA и RDP есть практически для любой ОС.

Если же система терминального доступа должна быть защищенной, то *контролировать необходимо вычислительную среду всех типов терминальных клиентов*, иначе получается классическая дыра в заборе, сводящая на нет его высоту и острые шипы по периметру. Выгода системы терминального доступа в части организации защиты информации связана ведь именно с унификацией предмета защиты — ОС терминального клиента, узкоспециальной, обычно небольшой по объему, а следовательно, легко контролируемой.

Если мы теряем эту особенность, то фактически задача защиты информации сводится к точно такой же, как если бы в системе применялись обыкновенные ПЭВМ, только к их количеству и разнообразию добавляются еще терминальные серверы. Более того, любая система, в которой одно и то же СВТ применяется в нескольких режимах, требует, помимо защищенности в каждом режиме отдельно, еще и доказанного отсутствия взаимовлияния этих режимов.

Стоит ли тогда вообще игра свеч? Безусловно, защита — это только одна сторона дела, и, возможно, не так критично, что теряется выгода именно в ней, ведь остается масса других плюсов, а защита вообще редко связана с выгодой.

Однако есть решение, позволяющее не терять выгоду унификации терминального клиента, но при этом и не терять возможности использовать в этом качестве практически любые СВТ. Такое решение — загрузка на СВТ необходимой (унифицированной,

контролируемой) среды только на тот период, когда оно должно работать в качестве терминального клиента.

Естественно, для СВТ разных типов и назначений нужно использовать различные (подходящие к каждому конкретному случаю) способы обеспечения загрузки этой контролируемой среды терминального клиента, но всегда она должна быть организована таким образом, чтобы загружаемая для работы в системе терминального доступа среда не влияла на основную среду СВТ, и наоборот.

В настоящее время на отечественном рынке представлены решения всех необходимых типов. Их можно разделить на группы в соответствии с ключевыми особенностями защищаемого СВТ:

1) СВТ разных моделей от разных производителей, основная задача которых — работа в терминальной сессии (классические тонкие клиенты);
2) СВТ — компьютеры различных характеристик, для которых работа в терминальной сессии — эпизодическая задача, а в основном пользователи работают с собственными ресурсами СВТ или с web-системой;
3) компьютер (ноутбук) руководителя.

Последний тип вполне разумно выносить в отдельную категорию, потому что при всей своей немногочисленности в штатном составе организации, руководители — это не та категория сотрудников, которой можно пренебречь.

Рассмотрим, чем будет различаться загрузка эталонной терминальной ОС в этих случаях.

7.1.2.1. Классические тонкие клиенты

Унифицировать среду исполнения ПО терминального клиента и одновременно сделать ее защищенной, но гибкой и администрируемой, можно с использованием комплексов защищенного хранения и сетевой загрузки ОС терминальных станций.

Универсальная часть образа ОС терминального клиента при этом загружается с отчуждаемого персонального устройства пользователя, а затем со специального сервера хранения и сетевой загрузки на клиент скачивается и после успешной проверки целостности и аутентичности полученного образа — загружается та его часть, которая

требует администрирования. Эта часть образа, включающая средства поддержки периферии (она может выходить из строя или просто заменяться), ограничения доступа к устройствам ввода-вывода и съемным носителям (принтерам, флешкам) и тому подобные «индивидуальные» настройки, должна быть доступной для изменений, но в то же время верифицируемой. Это и обеспечивается комплексами защищенного хранения и сетевой загрузки образов терминальных станций.

Таким комплексом средств защищенного хранения и загрузки по сети образов ПО терминальных станций является программно-аппаратный комплекс (ПАК) «Центр-Т».

Конфликт между защищенностью и возможностью автоматического принятия централизованных обновлений является на сегодняшний день болезненным вопросом, который каждая организация решает для себя — либо идя на дополнительные задержки и затраты, либо жертвуя защищенностью. В данном случае из двух зол выбирать не нужно. Коды аутентификации (КА) вырабатываются и проверяются полностью аппаратно внутри устройства, ключи выработки КА никогда не покидают устройства. Все действия, связанные с доступом к ключам в ПАК «Центр-Т», требуют повторного ввода PIN-кода, даже если ранее он уже вводился.

ПАК «Центр-Т» характеризуется двумя основными особенностями:

1) он аппаратно независим, так как полностью реализован на аппаратных персональных устройствах (ПСКЗИ ШИПКА): и клиентские, и серверные компоненты размещаются на дисках, встроенных в эти устройства, и могут исполняться на любом компьютере;
2) он позволяет гарантировать контролируемую целостность и подлинность образов ПО терминальных станций, загружаемых по сети, криптографическими методами, реализованными полностью аппаратно.

В состав комплекса входит специальное автоматизированное рабочее место (АРМ) «Центр», на котором конструируются образы ПО терминальных станций для разных пользователей с разным набором возможностей. Это позволяет достаточно оперативно реагировать на изменение ситуации (например, когда пользователю необходимо работать с терминальным сервером с другой терминальной станции, к которой подключен другой локальный принтер и монитор

с другими параметрами экрана) без снижения уровня ИБ и, что немаловажно, без проведения работ по администрированию непосредственно на рабочем месте пользователя. Поскольку рабочие места пользователей могут быть очень далеко, это важное свойство.

С точки зрения пользователя, работающего с терминальным сервером, старт работы будет выглядеть так:

- пользователь подключает ШИПКУ к терминалу и включает его;
- после запроса PIN-кода ШИПКИ — вводит его;
- после загрузки ОС терминального клиента запускает RDP или ICA клиент и начинает сессию с терминальным сервером;
- после запроса пароля пользователя в ПАК «Аккорд TSE» на терминальном сервере — вводит свой пароль;
- работает с назначенными ему правами в терминальной сессии.

7.1.2.2. Работа с ЦОДом как эпизодическая задача

Если работа в терминальной, виртуальной или web-сессии является эпизодической задачей, то требования к ОС терминального клиента минимальны, а его модификации маловероятны и во всяком случае крайне редки.

Для таких случаев как нельзя лучше подойдет решение с загрузкой эталонного неизменяемого терминального клиента из защищенной памяти отчуждаемого устройства. После окончания работы в терминальной сессии пользователю достаточно отключить устройство и перезагрузиться, чтобы вернуться к работе с ресурсами основного СВТ.

Это вкратце и есть описание доверенного сеанса связи (ДСС), реализуемого, в частности, СОДС (средством обеспечения доверенного сеанса связи) «МАРШ!».

Суть концепции доверенного сеанса связи с точки зрения безопасности заключается в следующем: раз компьютер практически всегда используется в незащищенных сетях и только иногда — в защищенных, значит, нужно добиваться не «тотальной» защиты, что дорого и неудобно, а **защиты, при которой защищенные и «опасные» ресурсы разделяются и не могут использоваться совместно.**

При этом очевидно, что целесообразность применения «постоянной» защиты или средства обеспечения доверенного сеанса связи прямо пропорциональна тому, сколько времени данный конкретный компьютер должен использоваться в режиме доверенной среды. Если постоянно или большую часть времени — то его необходимо полноценно, хоть и дорого, защищать, создавая изолированную программную среду (ИПС), защищая каналы связи, и т. д. и т. п. Если же это короткие сеансы в течение дня — то логично использование СОДС.

Успешность атаки определяется, в числе прочих факторов, временем, в течение которого злоумышленник имеет возможность ее осуществлять.

Это математически доказуемое и доказанное положение давно стало общим местом, в результате чего, к сожалению, дало почву для злоупотреблений, когда несанкционированное использование злоумышленниками ключей, хранящихся в токенах, объяснялось в дальнейшем тем, что пользователи слишком надолго оставляли токены подключенными.

Ошибочность этого объяснения настолько очевидна, что его сложно считать именно ошибочным. Однако предпосылки понятны — любая атака требует подготовки, создания условий для ее успешного проведения.

Подготовить условия для проведения атаки в постоянной среде — удобнее, чем в среде, создающейся на ограниченное время. Поэтому постоянная вычислительная среда должна быть более устойчивой к воздействиям на нее.

Однако, для того чтобы повысить устойчивость *системы*, не обязательно непременно повышать устойчивость *среды*. Альтернатива повышению *устойчивости среды* к воздействию — повышение *устойчивости системы* за счет уменьшения периодов времени существования целевой (для хакера) среды. Вспомним распространенный мотив из детективов и боевиков: для того чтобы «засечь» место, из которого производится телефонный звонок, специалистам необходимо N секунд. Поэтому тот, кому звонят, старается продержать абонента на трубке нужное время, а звонящий — прервать сеанс на N-2-й секунде. После этого можно перезванивать снова — специалистам опять понадобится N секунд, а не только две оставшиеся, так как результат их действий не накапливается, а начинается всякий раз с начала.

Примерна такова и логика ДСС.

Доверенная вычислительная среда создается комплексом средств единожды и на постоянное время и стоит дорого. Доверенный сеанс связи создается многократно по мере необходимости в нем, на непродолжительный промежуток времени (сеанс), и стоят средства его обеспечения ощутимо меньше.

Почему же тогда неверна логика кратковременности подключения токенов? Почему ключи успевают попасть в руки злоумышленников даже в тех случаях, когда токены подключаются только для подписания платежки, и даже в тех случаях, если ключи в них — неизвлекаемые?

Принципиальное требование безопасности к сеансу, детерминирующее безопасность применения данной технологии, — это «обнуление» среды при разрыве сеанса, возвращение ее в исходное состояние. Именно это не дает возможности злоумышленнику накопить результаты воздействий на среду, подготовить условия для проведения атаки. В случае с СОДС это обеспечивается тем, что доверенная среда взаимодействия загружается из раздела памяти ReadOnly (RO) и модифицировать ее можно только во время сеанса связи. В случае же с токенами среда компьютера постоянна, все необходимые манипуляции с ней злоумышленник может произвести в любое удобное время вне зависимости от того, подключен ли токен. И потом даже предельно кратковременного подключения будет достаточно для того, чтобы доступ к ключам был получен.

Атаки, безусловно, возможны и на «МАРШ!» (например, атакой через сеть, так как остальные ресурсы компьютера средой, загружаемой с «МАРШ!», не поддерживаются). Даже если такая атака состоялась, например в доверенную среду попал вирус или была осуществлена попытка «инъекции кода», то после отключения «МАРШ!» от компьютера среда вернется в исходное состояние, так как вирус не сможет записаться в память RO.

С точки зрения пользователя работа с этими комплексами выглядит практически одинаково: пользователь подключает к клиентской машине (например, к аппаратному терминалу) свое персональное USB-устройство (ШИПКУ или «МАРШ!»), происходит (не требуя действий от пользователя, а в соответствии с предварительно заданными управляющим персоналом настройками) загрузка клиентской

ОС, в которой стартует браузер или терминальный клиент и начинается сессия с удаленной системой.

7.1.2.3. Работа с ЦОДом как задача руководителя

На руководителя, как правило, возлагается так много совершенно необходимых обязанностей, что от выполнения «лишних» действий он закономерно хочет быть избавлен. Кроме того, в случае с компьютером или ноутбуком руководителя крайне желательно избегнуть заметных изменений привычного порядка действий при загрузке компьютера и замедления процедуры загрузки ОС, что неизбежно в первых двух описанных случаях.

Поэтому загрузка ОС с терминальным клиентом на СВТ руководителя должна производиться без подключения дополнительных устройств и через интерфейс, который не станет узким местом по скорости чтения. Это значит, что терминальный клиент должен загружаться на такой компьютер прямо из аппаратного модуля доверенной загрузки, требуя от пользователя только указания желаемого в данный момент режима.

Так и реализован «Ноутбук руководителя» — в ноутбук установлен miniPCIe-контроллер Аккорд-GXM (GXMH), firmware которого по факту отсутствия смарт-карты в считывателе загружает ноутбук штатным образом (ОС с жесткого диска), а в случае наличия смарт-карты в считывателе загружает собственную ОС, в которой загружается приложение доступа к защищенному ЦОДу. Таким образом порядок действий руководителя для перехода в режим ДСС сводится к привычной в обычной жизни работе со смарт-картой: установил смарт-карту, ввел PIN-код и получил доступ к защищенным ресурсам.

Поскольку все перечисленные типы терминальных клиентов должны (ну, или могут) работать в одной системе, то логично, чтобы производителем была гарантирована их совместимость.

Среда исполнения терминального клиента — это не единственное, что должно быть контролируемым в системе терминального доступа. В строгом соответствии с теорией, для обеспечения защищенности данных должна быть обеспечена безопасность их хранения, обработки и передачи. Значит, защитить необходимо все задействованные в этих процессах компоненты — терминальные серверы

с ПО и средой его функционирования, каналы передачи данных, терминальные клиенты и отчуждаемые носители информации. А поскольку все это должно представлять собой единую подсистему защиты информации, а не набор разрозненных средств, чреватый дырами на стыках, то при выборе конкретной реализации каждой из перечисленных технологий нужно отдавать предпочтение тем, которые интегрированы со средствами защиты терминальных серверов и как минимум проверены на возможность одновременного использования в одной системе.

Описанный подход призван унифицировать терминальные клиенты без унификации применяемых СВТ. Это позволит построить подсистему защиты информации в системе терминального доступа и экономичнее, и проще с точки зрения администрирования. При этом не будет необходимости разыскивать снятые с производства модели, терять гарантию из-за встраивания сторонних модулей в готовые решения и прочих побочных эффектов унификации, но удастся сохранить разнообразие функциональных возможностей СВТ, работающих вне терминальной сессии. Очевидно, что, когда задача становится слишком сложной, — надо искать ошибку в условии. Ошибка — считать, что защищать необходимо строго ту среду, которая есть на СВТ по умолчанию. Из необходимости работать в защищенной среде этого абсолютно не следует.

Как уже упоминалась, описанные в данном разделе средства защиты — это устройства довольно сложные как по своей архитектуре, так и в настройке (в меньшей степени — в применении). О том, что делать, когда сложность должна быть исключена, а безопасность все же обеспечена, — в следующем разделе.

7.2. Устройства с правильной архитектурой

Каждый день, выходя из дома, мы, даже не задумываясь, запираем дверь. Это действие выполняется привычно, автоматически, так как накопленный за многие годы опыт однозначен — это полезно для сохранения в неприкосновенности принадлежащих нам вещей. Конечно, дверь, замок и ключ не решают проблему воровства

полностью, но ни у кого не возникает сомнения, что дверь все же должна быть, и чтобы вор в нее не влез — необходимо ее не носить с собой, а запирать по месту установки. Заметим еще раз — вещи, находящиеся в квартире, будут *в большей безопасности*, если квартиру защищать.

Аналогия верна и для вашего компьютера. Программы и данные, составляющие принадлежащие вам информационные ресурсы, легче сохранить, если компьютер будет защищен.

Конечно, запертая дверь не гарантирует, что вещи не украдут. Защита компьютера тоже не гарантия от нарушения целостности программ, но это *абсолютно необходимый* рубеж защиты. Вещи из квартиры *точно* украдут, если дверь оставить нараспашку. Без защиты компьютера невозможно обеспечить защиту программ.

Но даже если ваши вещи будут находиться внутри защищенной квартиры, вовсе не обязательно они сохранятся в первозданном виде. Если вы в этом не уверены — попробуйте, *не выходя из квартиры,* вместе с рубашкой постирать паспорт.

Похожая ситуация и в виртуальном мире: казалось бы, в защищенном компьютере ничто не может повлиять на состояние данных и программ — однако же нет! В процессе исполнения одна программа вполне может изменить состояние данных другой программы и даже код другой программы — так, собственно, и ведут себя вирусы, да и не только они.

7.2.1. Компьютеры

Именно поэтому на «рабочих» компьютерах, а особенно на машинах, участвующих в технологических процессах, как правило, обеспечена изолированная программная среда, а то и функционально-замкнутая среда. Очевидно, что избежать влияния потенциально опасных программ на функционирование критически важных, тех, которым следует выполняться исключительно корректно, невозможно, не изолируя их одну от другой. Однако, как изолировать клиент-банк на компьютере клиента от его онлайн-игры?

Потери при ДБО в системах класса «Клиент–Банк», «Банк–онлайн» и других всегда связаны с хакерскими атаками — как

(возможно и такое) клиентов, так и неклиентов банка. Банк обычно неплохо защищен, и слабым звеном системы является компьютер клиента. Если компьютер клиента незащищен, то нельзя ни надежно идентифицировать клиента, ни доверять его подписи, так как она устанавливается в этом случае в недоверенной среде.

Надежная (достаточная) защита компьютера стоит около 15 000–20 000 руб., что неприемлемо для подавляющего числа клиентов. При этом защита ощутимо ограничивает возможности применения компьютера для других целей, что также неприемлемо для клиентов.

Кроме того, существующие системы защиты сложны и требуют специальных знаний для настройки, а этого от клиента требовать вообще невозможно. Более того, если знания такие есть (или еще хуже, пользователю ошибочно кажется, что они есть) — то в своем стремлении улучшить настройки клиент может завести ситуацию очень далеко от предписанного документацией состояния. Клиента в этом сложно обвинять: со своими устройствами, вообще говоря, он имеет право делать все, что сочтет нужным и сможет.

Таким образом, традиционные подходы к защите информации для систем ДБО непригодны.

Выход видится в том, чтобы предоставить клиенту:

- дешевый (7000–8000 руб.),
- защищенный;
- ненастраиваемый (то есть полностью преднастроенный, без внешних функций настройки вообще);
- полнофункциональный (с полноценной ОС и доступом к основным сервисам Интернет) компьютер. Или, точнее, микрокомпьютер, позволяющий, кроме всего прочего, надежно его идентифицировать.

Если базовая уязвимость компьютеров — в их архитектуре, значит, компьютер, удовлетворяющий требованию one-touch-security, должен быть создан на основе принципиально иной архитектуры, не имеющей этой уязвимости. Компьютеры, о которых пойдет речь ниже — это компьютеры, архитектура которых отличается и от архитектуры фон-Неймана (рис. 16), и от гарвардской архитектуры (рис. 17).

Отличительной особенностью архитектуры фон-Неймана является то, что команды и данные не разделяются, они передаются по единому общему каналу.

Гарвардская архитектура предполагает наличие разных каналов для команд и данных.

Такая схема взаимодействия требует более сложной организации процессора, но обеспечивает более высокое быстродействие, так как потоки команд и данных становятся не последовательными, а параллельными, независимыми.

Однако и в случае компьютера фон-Неймановского типа, и компьютера с Гарвардской архитектурой организация потоков команд и данных такова, что архитектурная уязвимость присуща каждому из них. Гибкость, универсальность в обоих случаях обеспечивается возможностью изменения последовательности команд и данных (двунаправленные стрелки от процессора к памяти) — независимо от того, в одной памяти они лежат или разделены. В свою очередь, возможность изменения последовательности команд и данных создает и возможность для несанкционированного вмешательства вредоносного ПО — это и есть основная архитектурная уязвимость, на которой базируются атаки на «перехват управления», описанные в предыдущем разделе.

Однако если в компьютерах, использующих Гарвардскую архитектуру, где потоки команд и данных уже разделены, сделать память неизменяемой, то не будет необходимости использовать сложные механизмы контроля целостности программ и данных до старта ОС, а контрольные процедуры в этом случае можно исполнять под управлением проверенной и неизменяемой ОС.

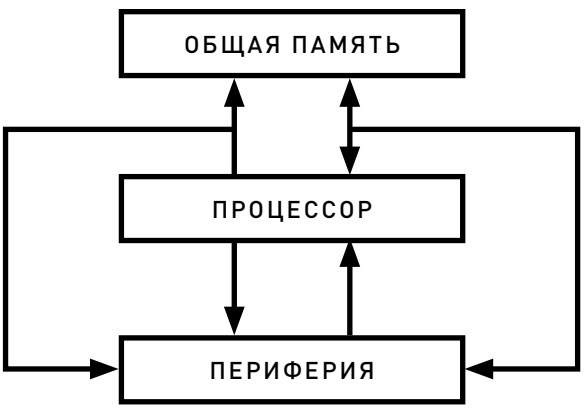

Рис. 16. Архитектура фон-Неймана

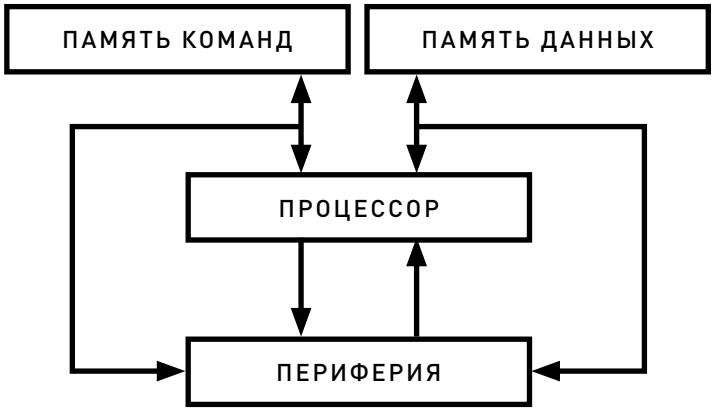

Рис. 17. Гарвардская архитектура

Очевидно, что такая архитектура обеспечит неизменность ОС, программ и данных.

Если вернуться при этом к схеме атаки, описанной выше, то видно, что шаг s3 не может быть выполнен, поэтому и сама атака (шаги s5 и s6) тоже не исполнится. Такой компьютер приобретет значительный «вирусный иммунитет», так как вредоносное ПО не будет фиксироваться на компьютере.

Недостатком в этом случае будет то, что придется дорабатывать практически все ПО, так как разработчики существующего ПО не ограничивают себя в использовании операций записи в память. Для работы практически всех программ необходима возможность записи.

Для того чтобы можно было использовать без доработок все ранее разработанное ПО, необходимо предложенную архитектуру дополнить блоками сеансовой памяти, в которой и будут исполняться программы.

Таким образом, архитектура компьютера будет отличаться на разных этапах — это и есть динамически изменяемая новая гарвардская архитектура.

Она отличается тем, что в ней используется память, для которой установлен режим «только чтение». При загрузке команды и данные размещаются в сеансовой памяти, в которой и исполняются. Начальная загрузка и копирование кодов в сеансовую память могут

выполняться как последовательно, так и параллельно — суть разделения этапов от этого не меняется.

Новая архитектура характеризуется динамической изменяемостью, что обеспечивает защищенность и эффективность, неизменность операционной системы, «вирусный иммунитет» и не мешает возможности применения адаптированных стандартных ОС и всего ПО, написанного для них.

Основных преимуществ два: высокий уровень «вирусного иммунитета»; возможность создания и поддержки доверенной среды, использования всего ранее наработанного ПО.

Важно то, что на основе описанной архитектуры можно создавать компьютеры для всех видов информационного взаимодействия, при которых доверенность и защищенность взаимодействия важна — от ДБО и защищенных «облаков» до Интернета вещей. Сейчас на основе описанной архитектуры разработаны и серийно выпускаются семь типов компьютеров — МКТ, МКТ+, МКТrusT, МКТ-card, МКТ-card long, AQ-МК, TrusTPad. Их особенности описаны в работах д. т. н. В.А. Конявского [28–34], а сами компьютеры — в работе В.В. Кравца [40]. Разработка новых видов компьютеров продолжается.

С учетом того, что цена самого экономичного из этих компьютеров — МКТ — в 10–15 раз ниже традиционного компьютера на базе x86, то понятно, что это и есть современное решение для потенциальных клиентов ДБО.

Таким образом, клиент банка получает ненастраиваемое устройство, которое обеспечивает загрузку неизменяемой проверенной ОС, устанавливает защищенное с использованием криптографических алгоритмов соединение с защищенным центром обработки данных, в котором установлено ПО (клиент ДБО) для доступа к БАС банка. Риски клиентов и банка сведены к минимуму.

Клиент ДБО размещается на ЦОДе, отвечающем всем требованиям по защите информации, и соответственно, доступ к БАС выполняется из одной, достоверно известной точки — ЦОД, по защищенному каналу.

Технология доверенного сеанса связи гарантирует безопасность доступа клиента банка к своему клиенту ДБО (и, соответственно, к банку) из любой точки мира.

Таким образом, клиент банка (человек) с помощью защищенного микрокомпьютера МКТ из любого гостиничного номера, где есть телевизор, защищенно соединяется с клиентом ДБО (программным обеспечением), размещенным на защищенном ЦОДе и по защищенному каналу взаимодействующим с защищенной БАС банка.

Данные клиента обрабатываются в защищенной вычислительной среде, а хранятся на устройстве.

Уровень защищенности позволяет предложить программу страхования от кибермошенничества.

Конечно, нельзя заставить всех клиентов всех банков покупать такое изделие, но целесообразно рекомендовать сделать это, так как при такой защите успешные хакерские атаки на компьютер клиента невозможны при сегодняшнем уровне техники.

Для формирования правильного решения клиенту нужно в клиентском договоре представить обоснованный выбор: управление счетом с использованием защищенного компьютера — и тогда все риски покрывает банк (или ЦОД, или страховая компания) или любые другие механизмы — тогда все риски на клиенте. Так банк и обезопасит себя, и обеспечит высокий уровень защищенности клиента.

Самому же банку целесообразно рассмотреть возможность использования в качестве рабочих мест защищенных компьютеров МКТ-card long. Пример такого использования приведен в следующем параграфе.

7.2.1.1. Пример целесообразного использования микрокомпьютера новой гарвардской архитектуры

Системы все чаще совмещают в себе терминальный доступ, VDI и web, причем рабочие места пользователей соседствуют с участками автоматической обработки данных, к одним и тем же файловым серверам обращаются компоненты разных (в том числе по уровню защищенности) систем, а клиентские СВТ применяются одновременно в двух и более контурах, которые должны, по-хорошему, быть строго изолированными один от другого.

Истоки такой ситуации нам всем хорошо понятны, обобщить их можно так: информационные системы складываются исторически.

Зачастую изначально они проектируются и какое-то время соответствуют современному уровню развития науки и техники. Затем осуществляется модернизация. Часто она вообще проходит незаметно — на уровне локальных улучшений системы управления, например. В той или иной специализированной подсистеме удобно осуществлять функции мониторинга через web-интерфейс — почему не ввести в нее такой модуль?

Потом наступает время более глобальной модернизации — технологии унеслись далеко вперед. Но имеющихся на модернизацию денег не достаточно на коренное **перепроектирование**, а достаточно (опять же, в хорошем случае) только на приобретение новых инфраструктурных элементов и технических средств. Например, на внедрение виртуальной инфраструктуры с целью централизации вычислений за счет виртуализации терминальных серверов и серверов обработки данных. Приобретенное (скорее всего, ПО и серверы, но, возможно, и средства защиты) встраивается в систему настолько успешно, насколько хватает квалификации и энтузиазма у управляющего персонала системы и подрядчика. К счастью, человеческий фактор — это не всегда плохо, и системы продолжают работать и даже иногда начинают работать более эффективно.

И вот однажды необходимо включить в состав технологического процесса новую операцию, предположим, работу с электронной подписью (ЭП) в системе внутреннего электронного документооборота. Выбранное по тем или иным причинам средство электронной подписи (СЭП) принципиально удовлетворяет проектным характеристикам системы (имеет сертификат, поддерживает работу в терминальном режиме и нужную систему управления ключами), для его применения необходимо только добавить в систему какой-то инфраструктурный элемент. Допустим, средство защиты канала. Мелочь. Но это средство, в свою очередь, требует работы с другим протоколом обмена данными. Тоже не беда, протоколы-то стандартные. Вырастает нагрузка на канал — ну, в общем, тоже дело житейское — можно расширить каналы. Хуже, если начинает требоваться изменение версии ОС. Совсем незначительное — не замена на ОС другого семейства, а всего лишь другая версия. И вот с этой версией как раз перестает работать функциональное ПО, выполняющее целевую функцию системы. Не говоря уже о том, что система электронного документооборота

(СЭДО) оказывается готова ко встраиванию СКЗИ, но не готова к выполнению требований к СЭП, и начинается выяснение границ ответственности — на чьей стороне, например, визуализация? СЭП или СЭДО? За счет свойств ключевого носителя или системы управления ключами лучше снижать нагрузку на персонал? И возникает еще очень много аналогичных вопросов.

Как правило, именно в этот момент эксплуатирующая организация задумывается о том, что что-то пошло не так, а подрядчик, выполняющий модернизацию, должен разрешить клубок проблем, возникших из-за исторически сложившейся цепочки логичных решений, часто совершенно не связанных между собой.

Абсолютно очевидно, что не имеет смысла рассказывать, как сделать, чтобы так не получалось — это всем хорошо известно: нужно все время проектировать. Но жизнь складывается тем не менее именно так, а не иначе.

Поэтому просто разберем возможное направление облегчения ситуации на примере условной системы удаленного доступа смешанного типа.

Пускай наша система совмещает в себе следующие инфраструктурные решения и технические средства:

1) физические серверы, часть из которых является ESXi-серверами, часть — терминальными серверами, часть — серверами приложений, часть — файловыми серверами, часть — серверами обработки данных, возможно, еще есть какие-нибудь серверы безопасности и/или обновлений;
2) виртуальные серверы, среди которых те же терминальные серверы, серверы приложений, файловые серверы и серверы обработки данных (как правило, так бывает тогда, когда систему начали «виртуализировать», но процесс растянулся по различным причинам на годы), и еще — серверы управления виртуальной инфраструктурой;
3) инфраструктура виртуализации — VMware;
4) отдельные функции управления системой реализованы в виде web-сервисов;
5) целевое функциональное ПО пользовательского сегмента информационной системы работает в терминальном режиме в среде Windows (на терминальных серверах — Windows).

6) терминальное ПО — Microsoft и Citrix;
7) два контура с разными уровнями защищенности (общедоступно / информация ограниченного доступа);
8) основным способом загрузки ОС терминальных клиентов является сетевой, но отдельные клиенты загружаются локально по причине плохих каналов в территориально удаленных подразделениях;
9) система ЭДО включает в себя механизмы ЭП, реализованные каким-то определенным СКЗИ;
10) в системе используются аппаратные идентификаторы пользователей и ключевые носители на базе USB-устройств и таблеток Touch Memory;
11) в системе контролируется применение флеш-носителей (есть определенные правила и ограничения, однако в целом они применяются);
12) и так далее, каждый интегратор и большинство эксплуатирующих организаций способны продолжить этот список новыми и новыми деталями без ущерба для правдоподобности общей картины.

Очевидно, что причин для тревог за работоспособность и защищенность такой системы — более чем достаточно. Если обобщить до схематичности, то проблема такой «естественной» системы в том, что она развивается из специализированной в универсальную, а это процесс довольно противоестественный.

Изначально корректно спроектированная система «заточена» на оптимальное (то есть с максимальной эффективностью при минимальных затратах и сложностях управления) решение конкретных, ясно описанных в проекте задач.

Для решения ясно описанного круга задач во всех без исключения случаях лучше использовать специальные, а не универсальные, средства.

Затем «жизнь вносит коррективы» **в систему, но не в проект**, и от специальных средств требуются все новые несвойственные им функции. Рассмотрим это на примере средств защищенной сетевой загрузки ПО терминальных станций. Идея применения таких средств состоит в том, что от тонкого клиента не требуется ничего, кроме поддержки периферии, и/а пользователя, контролируемой

целостности и аутентичности, журналирования и управляемости (то есть возможности контролируемой модификации в соответствии с изменениями ситуации со стороны удаленного аутентифицированного администратора). При этом защищенность становится, по сути, основной характеристикой технологии, так как с точки зрения состава, а тем более «удобства» такого загружаемого образа требования минимальны — пользователь с ним практически не имеет никаких дел, он работает с терминальным сервером уже после того, как средство защищенной сетевой загрузки закончило свою работу.

Однако если увеличить постепенно число поддерживаемых чипсетов до нескольких десятков, расширить парк периферии (ведь каждый год выпускается много новых мониторов все лучшего качества), сделать смешанной подсистему печати (ввести и сетевые, и локальные принтеры; любой сотрудник скажет, что ему удобнее иметь принтер на своем столе, а не ходить к сетевому), добавить клиент VPN, поддержку разнообразных идентификаторов и ключевых носителей, а затем еще встроить клиент СЭП, чтобы выработка ЭП производилась корректно на стороне клиента, то загружаемый по сети образ станет полноценной ОС. Это неплохо, но он будет, скажем, довольно объемным, особенно для загрузки по каналам связи низкой пропускной способности.

То же касается всех технологий, нацеленных на специализацию системы, но развиваемых в сторону ее универсализации.

Протокол передачи данных, оптимизирующий передаваемые данные для минимизации нагрузки на канал, теряет все свои преимущества при попытке шифрования трафика. Также в этом случае теряют эффективность и специальные «компрессоры». Шифртекст не сжимается.

Примеры можно умножать.

Очевидно главное — чем более размывается контур круга задач системы, тем менее эффективными становятся специализированные технические средства и решения.

Казалось бы, выход очевиден — необходимо ставить универсальные ПЭВМ, защищать их универсальными ПАК СЗИ НСД, а также антивирусами, средствами межсетевого экранирования, шифрования трафика и всем остальным. Тем самым мы создадим среду

функционирования криптографии (СФК) и решим все задачи, потеряв только в управляемости системы, стоимости владения, удобстве обновления и т. д. В общем, необходимо признать, что это решение плохое.

Видимо, необходимо найти ту грань универсальности и специализированности, которая позволит удовлетворить разросшимся требованиям системы, не вставая на экстенсивный путь бессмысленного наращивания ресурсов (использование техники все большей мощности со все более избыточной функциональностью, требующей обслуживания все большим штатом высококвалифицированного персонала).

Как ни удивительно, но именно подсистема защиты информации, которая, казалось бы, должна вносить в описанный хаос свою существенную лепту, может стать элементом, объединяющим все это в единое целое. И получится это как раз в том случае, если клиентские СВТ будут частью этой подсистемы, делая ее тем самым фузионной, а не агглютинативной[104].

Защищенные терминалы, о которых пойдет речь, — это МКТ-card long.

Для разрешения описанной ситуации мы предлагаем выбрать именно модель МКТ-card long потому, что ее форм-фактор (док-станция с отчуждаемым компьютером) оптимален для использования на стационарно расположенных рабочих местах.

104 Агглютинация и фузия — это два способа построения слов в разных языках. Агглютинация — это механическое присоединение нового члена (форманта) с одним-единственным значением (например, только множественность или только мужской род, или только притяжательность) при каждом наращении смысла. Пример агглютинации в татарском: «в его письмах» хатларында (хат — «письмо»; лар — формант мн. ч.; ын — притяжательный формант 3-го лица; да — формант местного падежа). Фузия же — это способ построения слов и форм, при котором один суффикс, например, может выражать сразу целую совокупность значений, а соединение частей слова происходит так, что не всегда легко провести точную границу. Например, слово «плачет»: корень «плак-» в месте присоединения суффикса (означающего *одновременно* и ед. ч., и 3-е лицо, и наст. вр.) — изменился: претерпел чередование к/ч (из-за влияния гласного переднего ряда на заднеязычный согласный).
Как правило, в языках наблюдаются оба способа, но один из них преобладает. Интересно, что искусственные языки всегда агглютинативные. Среди естественных чисто агглютинативные языки: тюркские, некоторые финно-угорские, монгольские, тунгусо-маньчжурские, корейский, японский, грузинский, баскский, абхазо-адыгские, дравидийские, часть индейских и некоторые африканские.

В отличие от микрокомпьютеров в форм-факторе донглов, к которым необходимо каждый раз подключать всю периферию, в кабинетах на столах сотрудников будут оставаться док-станции с подключенными мониторами, клавиатурами, мышами, считывателями ключевой информации и всем остальным, и на включение такого рабочего места будет уходить не больше времени, чем на запуск обыкновенного компьютера.

В образ ОС МКТ-card long интегрирована клиентская часть ПАК «Аккорд», общая для комплексов защиты физических и виртуальных инфраструктур (ПАК СЗИ НСД Аккорд-Win32 TSE / Аккорд-Win64 TSE, и ПАК СЗИ НСД Аккорд-В), так что один и тот же терминал сможет работать с физическими и виртуальными терминальными серверами без внесения изменений в систему защиту или конфигурацию ОС. Таким образом исключаются сложности по *пунктам 1 и 2*.

Для корректного взаимодействия с виртуальными рабочими столами в образ ОС терминала встроен VMware View Client, тем самым сняты возможные конфликты по *пункту 3*.

Для защищенной работы с web-сервисами в ОС МКТ-card long встраивается браузер и межсетевой экран, который не позволит пользователю отвлечься на посторонние задачи, пользуясь наличием интернет-соединения на рабочем месте. Таким образом, *пункт 4* также не вызовет проблем.

Наличие клиентов ICA и RDP исключает сложности, потенциально связанные с *пунктами 5 и 6*.

Задачу работы в двух контурах защиты (*пункт 7*) с использованием микрокомпьютеров семейства МКТ можно решить несколькими способами. Опишем те из них, которые не требуют использования никаких дополнительных инфраструктурных решений типа «брокеров» или аналогичных.

Очевидно, что основа у этих способов общая — работа в разных контурах будет изолирована в том случае, если соединение с серверной частью производится из разных ОС. Соответственно, мы можем:

1) использовать модификацию TrusT (компьютер в этом случае будет содержать физический переключатель и называться МКTrusT-card long). У этой модификации в разных

физических банках памяти находятся две разные ОС. Запуск одной или второй ОС определяется положением физического переключателя. Этот механизм абсолютно надежен, поскольку перевести переключатель в другое положение может только пользователь, загружающий компьютер, а никак не вирус или хакер. Итак, **при одном положении переключателя запускается ОС, например, с ICA клиентом, который инициирует сессию с терминальным сервером в общедоступном контуре, а при втором положении переключателя — загружается ОС с, допустим, VMware View Client, соединяющимся с защищенным виртуальным рабочим столом**. Или как угодно иначе. Главное, что из одной ОС можно попасть только в один контур, а из второй — только в другой;

2) при использовании стандартной комплектации МКТ-card long обеспечить две различные среды для доступа в разные контуры можно следующим образом. В общем случае, поскольку ОС в компьютерах МКТ неизменяемая (она находится в банке памяти, физически переведенном в режим Read Only), параметры доступа хранятся на внутренней SD-карте. Однако, помимо получения этих параметров с SD-карты, можно получать их (и какое-либо дополнительное ПО в случае необходимости) с сервера по сети.

В модификации «МКТ-card long для двойного применения» реализованы оба эти варианта одновременно, и **в процессе загрузки пользователь может выбрать, откуда получить конфигурационную информацию, и в зависимости от этого выбора попасть в один или другой контур**.

В таком решении совмещены функции комплекса защищенной сетевой загрузки ПО терминальных станций «Центр-Т» и стандартные функции МКТ-card long. Такое совмещение удобно еще и тем, что микрокомпьютеры в этом случае можно использовать внутри уже имеющейся в организации инфраструктуры «Центра-Т», то есть используя серверы хранения и сетевой загрузки этого комплекса без разворачивания новых.

Наиболее логичным видится доступ в контур ограниченного доступа с помощью загружаемых по сети конфигураций, и доступ

в общедоступный контур с конфигурациями на SD-карточке (потому что это позволит более гибко и оперативно управлять настройками доступа именно в более тщательно защищаемый контур). Хотя можно поступить и наоборот — зависит скорее от желательного порядка администрирования этих конфигураций, чем от соображений безопасности.

Таким образом, помимо потенциально проблемного *пункта 7*, выполняется и условие *пункта 8*.

Ну и, конечно, неверно было бы списывать со счетов естественный способ, порождаемый самой архитектурой решения — док-станция и отчуждаемый ПК. Док-станции и ПК в общем случае инвариантны один к другому, то есть любой ПК можно подключить к любой док-станции той же модели. А значит, доступ в разные контуры можно получать, просто подключая к своей док-станции разные компьютеры.

Пункт 9 — включение в технологию обработки электронных документов выработки и проверки ЭП — имеет огромное количество нюансов, связанных с особенностями деятельности организации, особенностями документов, которые должны таким образом обрабатываться, и пр. Если нарисовать предельно обезличенную схему, то она, с учетом обрисованных условий, может выглядеть, например, примерно так: документы формируются на терминальных серверах и должны быть подписаны операторами терминалов, при этом работа должна производиться с учетом требований Федерального закона Российской Федерации от 06.04.2011 № 63-ФЗ «Об электронной подписи» (далее — 63-ФЗ) и Требований к средствам электронной подписи (Приложение № 1 к приказу ФСБ России от 27 декабря 2011 г. № 796) (далее — Требования).

С применением защищенного терминала МКТ-card long это может быть реализовано, например, так:

1. Документ формируется на терминальном сервере.
2. Когда его должен подписать оператор терминала, документ передается с терминального сервера на терминальный клиент.
3. В целях контроля целостности документа при передаче по каналу, перед отправкой на терминал он подписывается

СКЗИ на ключе сервера в автоматическом режиме (статья 4 63-ФЗ[105]).

4. На терминале подпись проверяется резидентным СКЗИ терминала.
5. В случае подтверждения целостности документ визуализируется (часть 2 статьи 12 63-ФЗ[106]).
6. Оператор должен сознательным действием подтвердить корректность отображенного документа (часть 2 статьи 12 63-ФЗ).
7. Подтверждение оператора является сигналом для вычисления хеш-функции от документа резидентным СКЗИ терминала. Далее тем же резидентным СКЗИ или отчуждаемым персональным СКЗИ (токеном) вычисляется ЭП (п. 15 Требований[107]).
8. После подписания документ снова визуализируется на терминале (часть 2 статьи 12 63-ФЗ).

Подтверждение оператора является сигналом для отправки подписанного документа на сервер.

Идентификаторам и ключевым носителям в нашем описании условной системы посвящен отдельный пункт, однако именно в контексте ЭП имеет смысл заметить, что в случае актуальности угрозы использования подложного СВТ в качестве терминального клиента необходимо, чтобы применяемый токен имел механизмы

105 Статья 4 ФЗ-63 «Принципами использования электронной подписи являются: недопустимость признания электронной подписи и (или) подписанного ею электронного документа не имеющими юридической силы только на основании того, что такая электронная подпись создана не собственноручно, а с использованием средств электронной подписи для автоматического создания и (или) автоматической проверки электронных подписей в информационной системе».

106 Часть 2 статьи 12 ФЗ-63: «При создании электронной подписи средства электронной подписи должны:
1) показывать лицу, подписывающему электронный документ, содержание информации, которую он подписывает;
2) создавать электронную подпись только после подтверждения лицом, подписывающим электронный документ, операции по созданию электронной подписи;
3) однозначно показывать, что электронная подпись создана».

107 П. 15 Требований: «Средства ЭП класса КС3 противостоят атакам, при создании способов, подготовке и проведении которых используются возможности...: ...доступ к СВТ, на которых реализованы средство ЭП и СФ».

различения СВТ, разрешенных и не разрешенных для работы с ключами (пункт 31 Требований[108]). Такое устройство — «Идеальный токен»[109] — поддерживается МКТ-card long.

Очевидно, что факторами, определяющими реализуемость данной схемы (как и любой другой разумной схемы встраивания в технологию ЭДО механизмов ЭП) на микрокомпьютерах семейства МКТ, являются, с одной стороны, доверенная среда, обеспечиваемая технологически, и с другой — их вычислительные характеристики, достаточные для вычисления и проверки ЭП резидентным СКЗИ и корректной визуализации документа[110].

На данный момент есть опыт встраивания всех наиболее распространенных отечественных СКЗИ.

В части идентификаторов и ключевых носителей (*пункт 10*) первоочередное значение имеет сложившаяся в системе практика применения, поскольку это как раз та «мелочь», которая в системе настолько многочисленна и замена которой настолько трудоемка, что необходимость такой замены, особенно единовременной, может стать решающим противопоказанием для приобретения новых СВТ или системы защиты. Если использование даже очень удачного во всех отношениях пользовательского терминала потребует перерегистрации всех пользователей во всех подсистемах, требующих предъявления идентификатора, или даже просто дополнительной регистрации еще N идентификаторов (особенно если N — трехзначное и выше число), то любой владелец системы взвесит трудозатраты на эту процедуру. Что уж говорить о ключевых носителях — во многих организациях выпуск ключей является абсолютно сакральной процедурой.

108 П. 31 Требований: «В состав средств ЭП классов КС3 должны входить компоненты, обеспечивающие: ...управление доступом субъектов к различным компонентам и (или) целевым функциям средства ЭП и СФ на основе параметров, заданных администратором или производителем средства ЭП...»

109 Речь об этом устройстве пойдет в следующем разделе.

110 *Параметры компьютера:* Процессор 4-ядерный, 1,6 ГГц, Cortex A9; Графический процессор Mali400, 2D/ 3D OpenGL ES2.0/ OpenVG1.1; ОЗУ 2GB DRR3; WiFi IEEE802.11 b/g/n; Bluetooth V4.2; Считыватель карт MICRO SD (TF card) до 32GB; Размер защищенного диска 8 ГБ.
Параметры док-станции: Порт HDMI: 2, Порт USB: 8 (host) + 1 (slave), Порт Ethernet, Порт питания: 1 DC4.0mm, Питание: DC5V, 2A.

Имея в виду эту особенность, разработчики предусмотрели в МКТ-card long целый ряд возможностей.

Во-первых, сам отчуждаемый компьютер из состава МКТ-card long удовлетворяет всем признакам персонального аппаратного идентификатора и ключевого носителя. Он отчуждаемый, персональный, безусловно аппаратный и защищенный. Он может выполнять функции идентификатора пользователя в СЗИ НСД семейства «Аккорд» и защищенного ключевого носителя.

Такое хранение и аутентифицирующей, и ключевой информации является заметно более правильным с точки зрения защиты информации по следующим причинам. При идентификации с помощью компьютера пользователь подтверждает не только то, что подключается к системе именно он, но и то, что он это делает именно со своего законного рабочего места, а не со специально подготовленного надлежащим образом ноутбука, например, просто используя свой легальный идентификатор. Это позволит блокировать значительное число уязвимостей, связанных с так называемым BYOD (Bring Your Own Device — концепция использования личных устройств на рабочем месте), что на самом деле зачастую является неконтролируемым размыванием защищенного контура.

В плане работы с ключами все еще более очевидно, ведь даже храня ключи на так называемом токене, можно скомпрометировать их, подключив токен не к защищенному рабочему месту, а к незащищенному компьютеру, на котором уже есть какой-нибудь ворующий ключи троян. Так же как и в предыдущем случае, пользователь может действовать из лучших побуждений, например, желая поработать сверхурочно на домашнем компьютере, но при этом он сведет на нет усилия по защите информации в целой системе.

Заметим, что для укрепления метафорического смысла термина «ключ» — пропорции отчуждаемого компьютера таковы, что он помещается в стандартный пенал для ключей и может сдаваться под охрану в конце рабочего дня.

Если такое применение для эксплуатирующей организации привлекательно, перерегистрация идентификаторов и перезапись ключей можно производить постепенно, в плановом порядке, а в переходном периоде продолжать использовать уже введенные в эксплуатацию устройства — за эту возможность отвечает пункт «во-вторых» (ниже).

Во-вторых, в МКТ-card long реализована поддержка наиболее распространенных типов идентификаторов (список расширяемый, поскольку образ ОС формируется для каждой конкретной системы отдельно) и ключевых носителей, работающих по стандартному протоколу CCID.

Особенностью политики работы с идентификаторами и ключевыми носителями в отдельных организациях бывает запрет на использование одного и того же устройства одновременно в обоих качествах. Даже если и в качестве носителя ключа, и в качестве идентификаторов используются, допустим, ТМ-идентификаторы или USB-ключи, или смарт-карты — использовать *одно и то же* устройство, чтобы хранить данные для и/а и ключи с сертификатами, — нельзя. В таких случаях, конечно, как бы ни было удобно идентифицироваться с помощью своего же рабочего устройства и на нем же носить свои ключи, придется использовать отдельный ключевой носитель как минимум.

Учитывая описанные выше опасности, связанные с применениями ключевых носителей на несанкционированных компьютерах, мы рекомендуем «идеальный токен», который подключается только к заранее разрешенным администратором рабочим местам.

Наконец, остался последний из выделенных в начале пунктов — *11-й пункт*: флешки.

До сих пор все средства защиты информации, нацеленные на контроль использования подключаемых устройств, представляли собой некоторое ПО, устанавливаемое на сервер (или в ОС автономного ПК). Это были или модули в составе монитора разграничения доступа (такой модуль есть и в СПО «Аккорд»), или специальное ПО, предназначенное для контроля подключаемых устройств, типа Device Lock. Такие средства вполне могут функционировать и в серверной части описанной нами системы. Однако все, кто пытался решить задачу контролируемого использования флешек в организации, знают, что этого недостаточно и что необходимо не только применять флешки внутри защищенного контура по определенным правилам, но и исключить их применение за пределами контура, иначе все предпринятые усилия никак не помешают ни вынести информацию наружу, ни привнести вредоносное ПО извне.

Для комплексного решения этой задачи необходимо использовать флешки на базе защищенных служебных носителей. Работа

с такими флешками — линейки «Секрет»[111] (а именно — «Секрет Особого Назначения») — в режиме терминальной сессии поддержана в МКТ-card long.

Есть еще одна особенность нашей условной системы, которая не была вынесена в отдельный пункт, поскольку не является архитектурной, но явно заметна по сюжету. Это подверженность системы частым модернизациям по различным причинам.

Эта особенность важна для нас потому, что, казалось бы, находится в некотором противоречии с идеей зафиксированности и неизменности вычислительной среды, лежащей в основе линейки компьютеров МКТ. Противоречие это разрешено: для микрокомпьютеров реализована возможность обновления защищенной ОС. Если систему планируется модернизировать часто и радикально — лучше заказывать МКТ-card long с поддержкой системы защищенных обновлений. В противном случае вносить изменения в его защищенную от перезаписи ОС будет все равно возможно, но только в сервисном центре.

7.2.2. Служебные носители (флешки, ключевые носители, средства хранения журналов)

Другой пример технического средства, в отношении которого тоже постоянно ведутся разговоры о непреодолимости «человеческого фактора», — это разного рода носители информации. В первую очередь, конечно, флешки.

Однако недалеко отстоят и, например, токены — ключевые носители, на небрежном отношении пользователей к которым основывается большинство попыток вендоров оправдать утечки и потери, произошедшие «под защитой» их устройств.

Как и все остальные, мы считаем, что бесполезно бороться с человеческим фактором. Здесь, так же как и в предыдущем случае, не надо пытаться изменить человека, надо изменить то, что в наших силах — архитектуру «железки».

111 Речь о служебных носителях пойдет в следующем разделе, здесь ограничимся лишь информацией о совместимости решений.

Изменение в отношении архитектуры носителя требуется принципиально того же плана, как и в отношении компьютера: универсальное устройство нужно сделать менее универсальным.

Таким, чтобы оно выполняло те функции, которые нужно, на тех компьютерах, на которых можно, и совершенно ничего не выполняло в любых других условиях.

Если предельно обобщить (охватывая все возможные носители сразу), то их стандартная архитектура будет характеризоваться двумя важными для безопасности параметрами — памятью RW (универсальной, для любых задач) и возможностью работы на любом ПК (универсальный инструмент).

Ограничивать универсальность этих параметров можно и нужно.

Эта задача уже решена, и решения запатентованы [40, 50].

Рассмотрим основные типы носителей, наиболее часто применяемые в реальных системах.

7.2.2.1. Флешки

В информационных системах — государственных, частных или личных — данные *хранятся, передаются* и *обрабатываются*. Средства хранения данных принято называть носителями.

Носители данных в информационной системе (как, впрочем, и средства их обработки) могут быть стационарными и мобильными. Помимо этого носители информации могут быть составной частью оборудования, выполняющего также и *обработку* данных, а могут быть носителями в собственном смысле слова — устройствами, с помощью которых информацию *носят*, и во время того, как ее носят, она там *хранится*. А потом, когда информацию *перенесли*, она обрабатывается с помощью какого-либо другого оборудования. И вновь сохраняется на носитель, чтобы быть *перенесенной* куда-то еще.

Являясь частью защищенной информационной системы, носители информации тоже должны быть защищенными.

Защищенность — характеристика объекта, определяющая его способность противостоять атакам. Поэтому тезис о том, что защищенность различных элементов информационных систем обеспечивается разными способами, очевиден: защищенность объекта повышает способность противостоять *именно тем атакам*, осуществление

которых *наиболее вероятно* по отношению к данному элементу системы. Спасательный круг существенно повысит защищенность на воде, но совершенно не повысит ее при пожаре или, скажем, морозе.

Что это означает применительно к вопросу защищенности мобильных носителей информации?

Носители информации являются частью информационной системы, и, значит, существенно бóльшая их защищенность по отношению к остальным ресурсам системы не имеет смысла («общий уровень защищенности определяется уровнем защищенности самого слабого звена», или «дыра в заборе»[112]), она никак не усилит общую защищенность данных, и переплачивать за нее нецелесообразно. Нет практического смысла использовать сверхзащищенную флешку в незащищенной системе.

Однако, даже для того чтобы защищенность флешки соответствовала уровню защищенности самого обыкновенного домашнего компьютера, не защищенного ничем, кроме антивируса, эта флешка должна:

а) находиться в квартире и нигде кроме;
б) быть каким-то мистическим образом защищена от возможного воздействия вирусов.

Теоретически это достижимо с помощью организационных мер. Владелец флешки, которая используется только внутри защищенного помещения для переноса информации между несколькими защищенными от вирусов компьютерами, может быть спокоен — флешка не снижает общей защищенности его системы.

К сожалению, такая идеальная с точки зрения безопасности ситуация даже если и возникает, то обычно длится недолго: флешку понадобится куда-то вынести.

Самая главная особенность мобильных носителей состоит в том, что они подвержены дополнительным угрозам (по отношению к угрозам, актуальным для основной («стационарной») системы), связанным с тем, что контур системы для них проницаем: они могут не только *выноситься* (и выносятся!) за пределы системы,

112 «Ситуация напоминает строительство забора на даче: его делают все выше, а клубнику как воровали, так и воруют. Видимо, где-то есть дыра. В этом случае важнее не наращивать высоту забора, а дыру забить».

но и *использоваться* там. А, как следствие, это приводит к утечкам информации *из* системы и к притоку вредоносного ПО *в* систему.

Именно поэтому проекты защищенных информационных систем зачастую предусматривают полный запрет на использование USB-носителей. Флешки признаются абсолютным злом потому, что они *могут* использоваться *вне* системы. Значит, защищенный носитель — это такой носитель, который может использоваться *только внутри* системы (государственной, корпоративной, личной) и не может использоваться вне ее.

Назовем такой носитель служебным.

Служебный носитель — это такой носитель, который позволяет оперативно и просто переносить информацию *внутри системы* согласно ее внутренним правилам, но не позволяет ни выносить хранимую на нем информацию *из системы*, ни приносить *в систему* информацию, записанную на него *вне системы*. Никому, в том числе и легальному пользователю. Только в этом случае носитель не будет снижать общего уровня защищенности системы даже при его физическом выносе за ее периметр.

Если посмотреть с этой точки зрения на продукты информационной безопасности, позиционируемые поставщиками как средства защиты информации на флешках, то выяснится, что при всех своих возможных плюсах необходимую задачу они не решают.

Критерии оценки, которые адекватны понятию «защищенный служебный носитель», следующие:

- является ли продукт средством хранения и переноса информации (носителем);
- удобно ли его использование (аппаратные требования, требовательность к навыкам эксплуататора, мобильность, дружественность);
- снижает ли применение продукта степень негативных последствий кражи или утери носителя с данными для системы;
- защищает ли продукт данные от доступа посторонних лиц;
- при использовании вне защищенной системы способен ли продукт предотвратить «заражение» вредоносным ПО, которое в дальнейшем может попасть в систему;
- можно ли при помощи продукта защитить данные от хищения мотивированным инсайдером;

- имеет ли применение продукта нормативные ограничения в Российской Федерации;
- сколько стоит продукт.

Ни одно из представленных до сих пор на рынке средств или решений по защите информации не давало возможности создать систему, включающую в себя защищенные служебные носители, поскольку не было предложено решения главной задачи: **привязки носителя к системе**.

В программно-аппаратных комплексах (ПАК) линейки «СЕКРЕТ» именно эта функция является основной.

Что может предпринять злоумышленник в отношении флешки как носителя информации, включенного в интересующую его систему?

1. Кража или находка.
2. Отъем.
3. Завладение оставленным без присмотра устройством.
4. Завладение путем мошенничества и социальной инженерии.
5. Покупка у мотивированного инсайдера.

Как правило, пп. 1, 2 и 5 имеют своей целью завладение данными с флешки, а п. 3 или 4 может также иметь целью внедрение подложных данных или вредоносного кода (реже, но тоже возможно, — уничтожение данных на флешке).

В отличие от угроз данным в сетях или на локальных компьютерах, которые реализуются разнообразными атаками, угрозы, связанные с флешками, характеризуют мощные общие признаки возможных атак: *физическое завладение* устройством и получение доступа к его памяти *на каком-то ПК*.

Атаки на флешки через сеть, например, весьма маловероятны и будут скорее атаками на *данные на дисках компьютера* (подключаемых), а не на *данные на флешке*. И в любом случае вряд ли возможность реализации такого рода угрозы может быть классифицирована как уязвимость *флешки*.

Очевидно, что защитить маленькое устройство от физической кражи (или находки в результате целенаправленного поиска в местах возможных потерь, провокации потери) — крайне сложно и практически невозможно сделать это техническими методами.

Более того, и применение организационных мер крайне затруднительно, поскольку на физическое владение таким маленьким

предметом очень сильно влияет характер пользователя — рассеянный он или любит похвалиться, или нечист на руку, или доверчивый…

Значит, задача защиты флешки сводится к тому, чтобы сделать нелегальное физическое обладание ею бессмысленным. То есть, даже имея флешку, получить доступ к данным на ней на не разрешенном явно для этой флешки компьютере не разрешенному явно пользователю должно быть невозможно. Тогда одинаково бесполезно (или, если смотреть с другой стороны баррикад, — не опасно) ее красть (терять), отнимать (отдавать), покупать (продавать) и т.д.

Для того чтобы флешка работала на одних компьютерах и не работала на других, флешка должна уметь *различать* компьютеры.

Это первая задача, только после решения которой можно обсуждать, по каким параметрам различать компьютеры правильно, а по каким нет, или каким образом добиваться изменения списка разрешенных (или запрещенных) компьютеров.

Очевидно, что все эти вопросы важны, но только в том случае, если флешка *в принципе* различает компьютеры.

Обыкновенная флешка делать этого не может. Это связано с тем, что у флешки нет для этого никаких ресурсов. Если говорить упрощенно, флешка состоит из памяти и контроллера USB (рис. 18).

Рис. 18. Архитектура USB-накопителя

Ни то ни другое не является ресурсом, способным осуществлять произвольные операции.

Компьютер может различать флешки по их уникальным идентификаторам — VID, PID и серийному номеру, если на нем установлены средства для этого (например, USB-фильтры), потому что у него, в отличие от флешки, есть необходимые вычислительные ресурсы. Стоит иметь в виду, что эти уникальные идентификаторы не всегда и не совсем уникальны (все флешки некоторых производителей имеют один и тот же серийный номер, а с помощью специального технологического ПО эти «уникальные параметры» можно менять). Однако в любом случае, для того чтобы проанализировать тот или иной признак объекта (флешки ли, компьютера ли), тот, кто анализирует, должен иметь ресурсы, предназначенные для такого анализа.

Вывод очевиден: чтобы различать компьютеры, флешка должна сама быть компьютером. Именно в этом и состоит отличие служебных носителей (СН) «Секрет». Архитектура флешек изменена в устройствах «Секрет» следующим образом (рис. 19).

Управляющий элемент в СН «Секрет» различных модификаций реализован по-разному, однако общая логика остается единой: управляющий элемент «коммутирует» компьютер с диском «Секрета» (собственно флешкой) только после успешного завершения

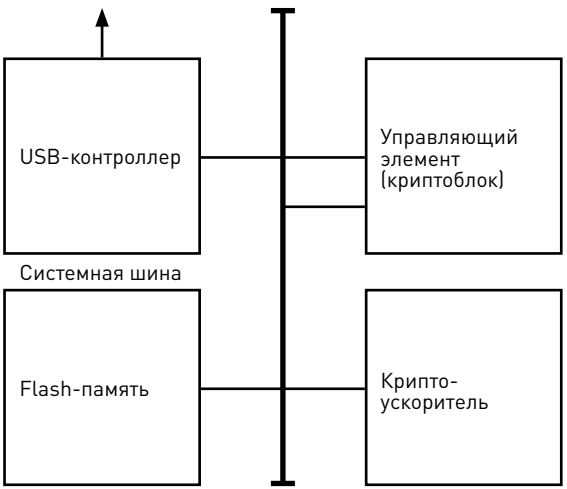

Рис. 19. Архитектура служебного носителя

контрольных процедур: взаимной аутентификации СН, компьютера и пользователя. До того как сценарий аутентификации будет успешно разыгран до конца, диск «Секрета» не будет примонтирован, не появится в списке дисков и не окажется доступен не только для пользователя, но и для системы (с ее потенциальными закладками или вирусами).

Дополнительно защитные свойства «Секрета» могут быть усилены шифрованием данных при записи на диск. Выбирать такой носитель целесообразно тогда, когда разумно предположение, что злоумышленник может попытаться считать данные с флеш-памяти напрямую, например, выпаяв ее с устройства. Однако надо иметь в виду, что за счет аппаратного шифрования заметно снижается скорость чтения/записи, это неизбежные издержки. В СН «Секрет» без шифрования скорости чтения/записи не отличаются от скоростей обычных флешек.

Такова принципиальная структура и логика защитных свойств *служебного носителя* «Секрет», а *продукты* линейки «СЕКРЕТ» различаются тем, как организовано управление процессом взаимной аутентификации компьютера, «Секрета» и его пользователя.

7.2.2.2. Ключевые носители

Ключи, так же как и любые данные, существуют в трех процессах: хранятся, обрабатываются (в том числе создаются и уничтожаются) и передаются.

Никаких других состояний у данных — и ключей как явлений этой сущности — не бывает.

Ключи отличаются от других данных только одним: компрометация ключей заметно более критична. Это значит, что принципиально никаких специфичных приемов для защиты именно ключей не требуется, просто обеспечиваться меры защиты должны несколько более тщательно, чем в отношении любых других данных.

Почему более тщательно — очевидно на уровне здравого смысла. Сравним случай компрометации документа и компрометации ключа. Если скомпрометирован документ, то наступают некие негативные последствия. Безусловно, они могут быть весьма существенными, поэтому защищать необходимо отнюдь не только ключи. Но все-таки,

если происходит компрометация ключа (например, ключа ЭП), злоумышленник может создавать неограниченное количество документов от имени пользователя, чей ключ скомпрометирован.

К сожалению, здравый смысл не всегда детерминирует безопасное поведение, потому более жесткие требования по защите ключей (хотя вернее было бы сказать — систем с ключом) предъявляются и регуляторами.

В свете требований к СЭП, в которых взаимоувязаны все три состояния ключа, это становится особенно наглядно: мы можем руководствоваться самыми разными соображениями, выбирая тип желательной для нас в тех или иных обстоятельствах ЭП, выбирая подходящий для нас СЭП, но как только мы выбрали усиленную ЭП (то есть «ЭП с ключом»), мы попадаем в зону действия существенно более высоких требований.

Таким образом, с точки зрения безопасного существования криптографических ключей в автоматизированной системе (АС) принципиальное значение имеют два фактора:

1) защищенное хранение ключа (и, соответственно, носителя ключа);
2) условия доступа к ключу и работы с ним (то есть СФК).

Очевидно и не нуждается в детализации, что второй фактор (условия доступа к ключу) касается и обработки, и передачи ключей — как части технологии, реализуемой СКЗИ (СЭП) при выполнении своих функций.

В то же время очевидно, что криптография, как правило, является вспомогательным механизмом, а не основной целевой функцией системы, поэтому условно выделяемым третьим фактором можно считать степень влияния на информационную инфраструктуру. Естественно, что удорожание и усложнение системы обычно желательно минимизировать, поэтому средство хранения ключей, например, требующее изменения применяемых в системе протоколов взаимодействия, замены операционных систем и/или внедрения не требующихся ни для чего более средств защиты каналов связи, — может считаться удачным решением только для подрядчика, который будет нанят на все эти работы.

Этот параграф посвящен средству хранения ключей (токену), которое позволяет решить несколько большее число задач, чем обычно

применяемые в этом качестве устройства, не требуя серьезных инфраструктурных изменений АС. Поэтому оно называется «Идеальный токен».

Сложившаяся практика

Сложившаяся практика применения ключей такова, что в качестве их носителей используются универсальные накопители (дискеты, флешки), идентификаторы пользователей, если они представляют собой устройства с доступной для записи/чтения памятью (ТМ-идентификаторы) или специализированные устройства (смарт-карты, USB-токены).

Обзор этих видов «хранилищ ключей» (невозможно использовать данную формулировку без кавычек, так как далеко не все эти объекты хотя бы минимально приспособлены к хранению именно ключей) приведен ниже. Из обзора исключены дискеты, так как побочным эффектом развития вычислительной техники, все реже имеющей дисководы для дискет, явилось и постепенное отмирание применения этого носителя и в этой конкретной функции.

Здесь невозможно не вспомнить снова аксиому о том, что для специальных целей логично применять специализированные средства.

Однако и специализированные средства — токены[113] — не идеальны.

Токены предоставляют возможность использования хранимых на них ключей и сертификатов после предъявления PIN-кода (авторизации пользователя). Казалось бы, таким образом блокируются все уязвимости, связанные как с хранением, так и с доступом к ключу.

Однако очевидно, что ограничение доступа к ключу только использованием PIN-кода недостаточно. Токен должен использоваться только в той системе, в которой обеспечена защита от несанкционированного доступа (а именно — обеспечена доверенная СФК), а PIN-код можно правильно ввести в любой среде. Токен не может определить, в какой системе производится попытка работы с ним, у него нет для этого никаких механизмов. Невозможность расширения

113 Это слово используется в разных значениях, но в рамках этого текста условимся понимать «токен» только в одном из них: как защищенное тем или иным способом хранилище ключей в виде объектов PKCS.

функций токена проистекает не из лени программистов, а из ограниченности его архитектуры (рис. 20).

Чем же опасна невозможность контролировать внешнюю среду? Например, в ней могут быть предустановлены программные закладки, предназначенные для перехвата криптографической информации или перехвата управления компьютером. При правильно введенном PIN-коде (а в некоторых случаях и до введения PIN-кода) все это вредоносное ПО получит доступ к ключам.

В части доступа к ключу очевидна необходимость учитывать как условия доступа пользователя (человека), так и условия доступа СКЗИ и другого системного и функционального ПО.

При этом следует учитывать особенности сред и систем, в которых пользователи выполняют задачи, связанные с криптографическими преобразованиями: работа в различных ОС, загруженных на СВТ различных архитектур из различных источников различными способами, — может иметь целый ряд особенностей, существенно влияющих на безопасность ключа.

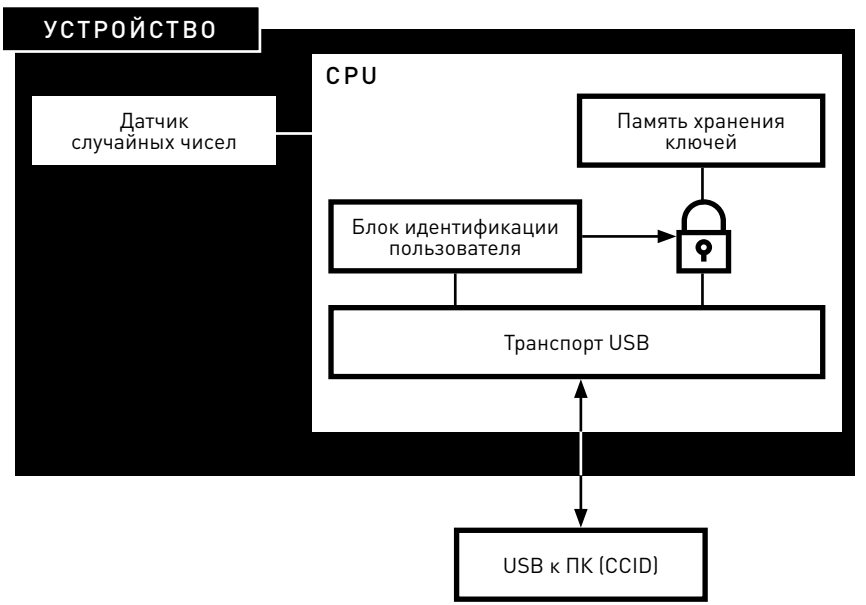

Рис. 20. Архитектура токена

Отсюда вытекают требования к защищенному ключевому носителю. Защищенный носитель ключа в идеальном случае должен быть способен контролировать:

- доступ к ключу через любые интерфейсы, в том числе и путем применения разрушающего программного воздействия (РПВ);
- среду, в которой производится попытка доступа к ключу.

Естественно, защищенный ключевой носитель не должен контролировать корректность работы СКЗИ или собственно обеспечивать среду его функционирования (это функция средства доверенной загрузки). То есть задача «контроля» среды, из которой осуществляется доступ к ключу, сводится к тому, чтобы доступ к ключу предоставлялся не только исключительно легальному пользователю, но и исключительно на заданных рабочих местах (наличие «правильной» среды на которых обеспечивается в установленном в организации порядке). Принципиально это та же задача, что и для флешек: ограничение числа компьютеров, на которых технически возможна работа с токеном.

В случае реализации такой защитной меры при случайном или преднамеренном подключении токена к неразрешенному (а значит, недоверенному) компьютеру, устройство не будет примонтировано, значит, ключи не будут доступны ни пользователю (даже легальному), ни системе (с потенциально функционирующими в ней вирусами и закладками).

Кроме того, при этом будет исключено несанкционированное использование ключей легальным пользователем токена вне рамок его служебных задач. Это важно, так как само по себе СКЗИ не может определить правомерность формирования данного документа на данном компьютере и подписания его с помощью того или иного ключа.

Вероятность подмены рабочего места звучит не очень страшно только по одной причине: кажется, что в этом никто особенно не заинтересован (например, трудно представить, что бухгалтер соберется сделать с домашнего ноутбука нелегальный перевод, подписав платежку своей ЭП).

Однако на самом деле представить себе сценарий как случайной, так и злонамеренной компрометации ключа и документа — несложно.

Предположим несколько самых явных.

Начнем с добросовестного бухгалтера (таких, мы уверены, большинство). Из лучших побуждений — выполнять часть работы сверхурочно — он может организовать себе дополнительное рабочее место дома. При этом он может разделить работы по критичности и для «домашнего» выполнения выделить не платежи, а только подготовку и отправку в налоговую инспекцию отчетов в электронном виде. Это делается с помощью одной из специальных программ, например «Фельдъегерь», и бухгалтеру на его домашнем компьютере даже не потребуется «Клиент-банк».

Скорее всего, из средств защиты от НСД на этом «дополнительном рабочем месте» будет в лучшем случае только антивирус. Эта ситуация создаст предпосылки для компрометации ключа с помощью широко распространенных вредоносных программ. В случае направленной атаки это позволит злоумышленнику в дальнейшем использовать украденный ключ в своих целях. Если же компьютер используется и для проведения платежей, а не только для подготовки и отправки отчетов, то задача злоумышленника и вовсе упрощается.

Все еще хуже, если злоумышленником является сам бухгалтер (надеемся, что не доведем никого до греха).

Итак, если бухгалтер задумал провести нелегальный платеж, что его может остановить? Теоретически, его должна сдержать неотказуемость от ЭП на его ключе.

Однако в действительности при наличии технической возможности передачи ключевого носителя другому лицу и одновременно возможности применения ключа на произвольном СВТ, неотказуемость от ЭП — это уже вопрос алиби, а не криптографии.

Нарисуем такой «детектив»: злоумышленник организует рабочее место с необходимым для проведения платежа ПО. На собственном рабочем месте он подготавливает накануне несколько платежных поручений, подписанных его ЭП, но не отправляет их.

Вечером токен с ключом ЭП бухгалтер передает сообщнику и договаривается о времени проведения незаконного платежа таким образом, чтобы сам владелец ключа в это время был на рабочем месте на глазах у свидетелей.

В результате, в условленное время злоумышленник находится на виду у будущих свидетелей и отправляет заранее подготовленные платежки со своей легальной ЭП (токен ему для этого не нужен, ведь

документы подписаны заранее). В это же время в другом месте с другого компьютера другое физическое лицо (сообщник) подписывает ключом нашего героя другое платежное поручение, используя токен.

При разборе инцидента злоумышленный владелец ключа имеет все шансы отказаться от своей ЭП, так как находился в это время на собственном рабочем месте и даже отправлял другой документ с подписью на том же ключе, а никаких следов отправки нелегального платежа на его рабочем СВТ нет. Очевидно, что он совершенно ни при чем.

Чтобы избежать обвинений в предвзятости к бухгалтерам, приведем пример, никак не связанный с платежами.

Предположим, что злоумышленником движет желание осуществить атаку на корпоративную информационную систему, обрабатывающую информацию ограниченного доступа.

Предположим, что система — распределенная централизованная (допустим, система терминального доступа, или web-система). Предположим, что документы обрабатываются на сервере, сервер надлежащим образом защищен, клиентские СВТ не содержат средств обработки информации (тонкие клиенты), загружаются с обеспечением доверенности клиентской ОС и каналы между клиентами и сервером тоже защищены.

Ключи СКЗИ, защищающего канал, хранятся в токене.

Наиболее очевидная атака — это подключение в качестве терминального клиента произвольного СВТ злоумышленника, оснащенного программами для осуществления какой-либо атаки на систему.

Если атаку осуществляет легальный пользователь системы — он обладает идентификатором к СЗИ НСД на сервере и токеном с ключами СКЗИ, защищающего канал (зачастую это одно и то же устройство).

Предотвратить эту атаку может только применение комплексной системы защиты, включающей взаимную аутентификацию клиентского СВТ и сервера. Это не рядовая функция, зачастую относительно сервера аутентифицируется только пользователь.

Все эти леденящие кровь сценарии невозможны, если токен просто различает СВТ, к которым его подключают.

Итак, защищенный ключевой носитель должен:

1) быть персональным отчуждаемым устройством;
2) быть специализированным именно для хранения ключей устройством (то есть обеспечивать возможность защищенного

хранения криптографических ключей с применением интерфейсов работы со смарт-картой (CCID или PKCS#11));

3) предоставлять доступ к ключам только легальному пользователю после успешной аутентификации в устройстве;
4) предоставлять легальному пользователю доступ к ключам только на тех СВТ, на которых данному пользователю разрешено работать с данным ключевым носителем;
5) удовлетворять требованию патентной чистоты.

Функции токена с функцией ограничения числа разрешенных компьютеров объединяет в себе «Идеальный токен» — токен с несколько измененной архитектурой: она включает в себя блок идентификации компьютера, до прохождения проверки которым недоступен в том числе и блок идентификации/аутентификации пользователя (рис. 21).

В «Идеальном токене» есть две роли пользователей — «Администратор» и собственно «Пользователь». Список компьютеров, на которых разрешена работа с «Идеальным токеном», определяется

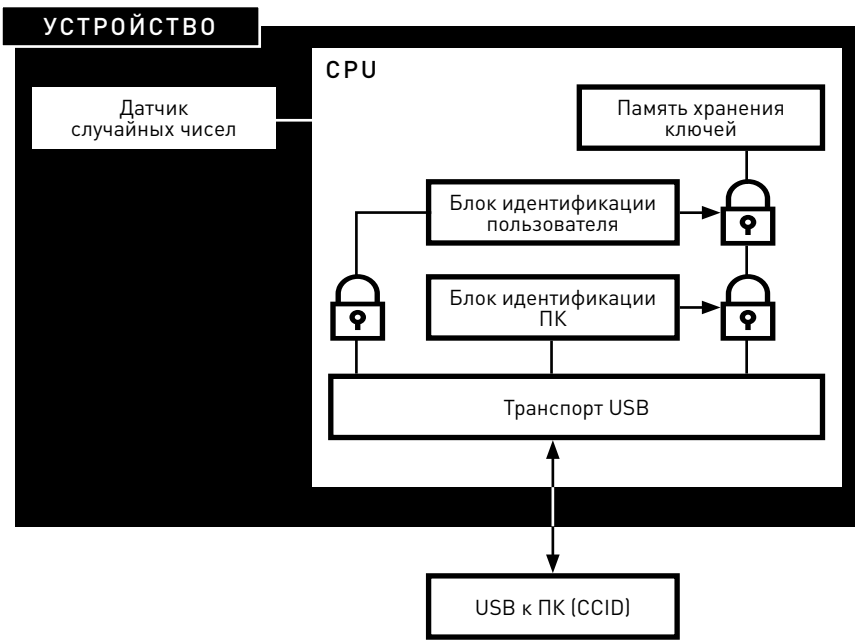

Рис. 21. Архитектура «Идеального токена»

пользователем с ролью «Администратор», который с точки зрения информационной системы должен быть администратором ИБ или лицом, которому делегированы соответствующие функции.

Для того чтобы добавить компьютер в список разрешенных, Администратор подключает к нему «Идеальный токен», его СПО определяет, а ВсПО запоминает внутри устройства ряд параметров этого рабочего места. При каждом последующем подключении «Идеальный токен» определяет параметры текущего компьютера и сравнивает с теми данными, которые соответствуют разрешенным рабочим местам. Если они совпадают, разрешается доступ к токену со стороны внешнего ПО — то есть, собственно, со стороны СКЗИ (СКЗИ — это внешнее по отношению к «Идеальному токену» ПО), иначе в доступе отказывается.

Очевидно, что ни одно другое устройство, применяемое для защищенного хранения ключей, не выполняет более трех требований к защищенным ключевым носителям одновременно (см. таблицу 1). При этом важнейшее требование, касающееся СФК, не выполняется ни одним из них.

«Идеальный токен» является специализированным устройством, предназначенным именно для хранения ключей СКЗИ и поддерживающим все необходимые для этого интерфейсы.

Таблица 1

Требование	Смарт-карта	Токен	Флеш-накопитель	ТМ-идентификатор
Персональное отчуждаемое устройство	+	+	+	+
Поддержка интерфейсов CCID и/или PKCS#11	+	+	—	—
Контроль легальности пользователя*	+	+	—	—
Контроль легальности СВТ	—	—	—	—

* «+» или «—» в строке «Контроль легальности пользователя» оценивает наличие в ключевом носителе собственных механизмов, независимых от механизмов СКЗИ. То же справедливо и для остальных параметров, однако именно в отношении указанного возможна неоднозначная интерпретация.

Использование «Идеального токена» возможно только после успешного завершения взаимной аутентификации токена и компьютера, к которому его подключили, а затем — успешной аутентификации пользователя в токене и СКЗИ.

Таким образом, при корректной настройке системы управляющим персоналом, исключена возможность сознательной или случайной компрометации ключей из-за подключения к незащищенному компьютеру, на котором могут быть предустановлены программные закладки, предназначенные для перехвата ключей или перехвата управления компьютером. А также, что не менее важно, исключено несанкционированное использование ключей легальным пользователем токена — вне рамок его служебных задач, что невозможно предотвратить при использовании обычных токенов, не различающих служебные и любые другие ПК.

В то же время «Идеальный токен» лишен каких бы то ни было избыточных функций, негативно влияющих на цену изделия.

Технология «Идеального токена» запатентована [50].

Обзор ключевых хранилищ

Смарт-карты

Смарт-карты обычно обладают весьма скромным объемом памяти данных, десятки килобайт, однако этого достаточно для хранения ключей или сертификатов. Для доступа к данным необходим ввод PIN-кода. Устройство может быть заблокировано после некоторого количества неверных вводов PIN подряд, что делает затруднительным подбор PIN. Смарт-карты обладают хорошей совместимостью, так как используют стандартный протокол, но для их использования требуется кардридер. Одна из основных проблем смарт-карт — их возможный отказ, так как тонкий пластиковый корпус чипа не может обеспечить надежную защиту при физических воздействиях.

Если злоумышленник завладел и смарт-картой, и ее PIN-кодом, он сможет получить доступ к данным. Владелец смарт-карты технически может (хотя и не должен бы) использовать ее вне доверенной среды, при этом PIN-код может быть перехвачен с устройства ввода, ключи могут быть списаны из оперативной памяти или из памяти смарт-карты после разблокировки хозяином.

Разумеется, хранение ключей — это не единственная функция смарт-карты, но одна из основных.

Токены

Токены могут иметь более широкие возможности по сравнению со смарт-картами. Например, устройство может содержать свою собственную клавиатуру для ввода PIN-кода, что значительно усложняет перехват. Обычно для работы с токеном необходима установка драйверов.

Если злоумышленник завладел и токеном, и необходимым кодом доступа, он сможет получить доступ к данным. Владелец токена технически может (хотя и не должен) использовать его вне доверенной среды, при этом ключи могут быть списаны из оперативной памяти или прямо из устройства после его разблокировки хозяином.

Хранение ключей — это не единственная и не основная функция токенов, их основное назначение — двухфакторная аутентификация.

Флеш-накопители

Обычные флеш-накопители не обладают никакой защитой. Могут быть украдены или утеряны, в этом случае любой человек сможет получить доступ к данным. Зато флеш-накопители обладают значительным объемом памяти, совместимы практически со всеми устройствами, имеющими USB-порты. Флеш-накопитель может быть использован на любом АРМ в любых условиях.

Было бы нелепо даже рассматривать вопрос о том, является ли хранение ключей сколь-нибудь специальной функцией флеш-накопителей.

TM-идентификаторы

В основном, так же как и флешки, не обладают никакими защитными механизмами, кроме необходимости наличия специального считывающего устройства, впрочем, свободно продаваемого.

Содержимое TM-идентификаторов можно копировать, поэтому данные, хранящиеся в устройстве в открытом виде (в том числе и ключи), могут быть легко скомпрометированы.

Основное предназначение ТМ-идентификаторов, как и токенов, — двухфакторная аутентификация. Если аутентифицирующей информацией являются не непосредственно хранящиеся в ТМ-идентификаторе данные, а результат преобразования, которое производится резидентным компонентом безопасности с данными, полученными по разным каналам, то копируемость памяти ТМ-идентификатора не является критичным фактором. В отличие от считывания хранящихся в «таблетке» в открытом виде ключей.

7.2.2.3. Другие служебные носители

По принципу, впервые реализованному в служебных носителях «Секрет», кроме «Идеального токена», построены и другие служебные носители для различных более узких целей. Например, это программно-аппаратный неперезаписываемый журнал ПАЖ — где свойства «Секрета» дополнены тем, что память, в которой сохраняются журналы событий различных устройств и приложений — Add only, то есть в нее можно только добавлять, а что-либо удалять или изменять в ней нельзя. Также ПАЖ характеризуют некоторые особенности реализации ролей пользователей, связанные работой именно с журналами, но они не касаются архитектуры и являются, в общем-то, частными деталями.

Еще один пример — мобильный генератор лицензий: устройство, позволяющее распространять лицензии на программное обеспечение, избегнув основных типов проблем, с которыми сталкиваются при этом вендоры ПО.

Более того, решений такого рода может быть очень много, потому что базовый принцип — изменение архитектуры как способ решения проблем с нею — является научным, а значит, экспериментально подтверждаемым и воспроизводимым.

Завершая главу, вынуждены признать, что она не претендует на полноту материала даже на уровне перечня типов средств и способов защиты информации. Представленное — скорее очерки. Однако, думается, они позволят сделать самостоятельные выводы и обобщения, достаточные для розыска необходимого читателю решения, если оно не описано в этой главе в явном виде.

8. ВЛИЯНИЕ «ТЕНЕВОГО ИНТЕРНЕТА» НА БЕЗОПАСНОСТЬ ЭЛЕКТРОННОГО БАНКИНГА

Введение

Конец XX и начало XXI вв. олицетворяют собой быстрое развитие информационных технологий, которые существенно упрощают жизнь людей и позволяют им вести более динамичный образ жизни, сосредоточив свои усилия на организации решения той или иной задачи, а не на ее реализации. Жизнь человека уже не представляется возможным без мобильных устройств, компьютеров, технологий «умного дома», корпоративных систем, систем электронного правительства, электронных денег, ЭБ и, конечно же, локальных и глобальных сетей. Специфика сети Интернет размывает такие привычные для реального мира понятия, как государственные границы, начало и конец совершения преступления, традиционная идентификация индивидуума и т. д. Однако специфичность виртуальной среды не отменяет законы и привычные правила реального мира, а потому вопросы свободы слова, неприкосновенности жизни человека, интеллектуальной собственности, денежной эмиссии, обеспечения защищенного перевода денежных средств, защиты прав физических и юридических лиц также остаются актуальными, в связи с чем повышается актуальность вопросов информационной безопасности. Работа ведется на всех уровнях: начиная с защиты пароля персонального компьютера владельцем этого компьютера и заканчивая вопросами противодействия кибертерроризму и кибершпионажу органами государственной безопасности той или иной страны. И чем активнее повседневные процессы человека переносятся в виртуальное пространство, тем острее становятся вопросы безопасности по причине неизменности человеческой сущности, которая иной раз может породить действия как хулиганского характера (пример — молодой человек, который пишет в домашних условиях вредоносное программное обеспечение и распространяет

его посредством электронной почты), так и идеологического характера (пример — практика подготовки собственных хакеров Китая (КНР), которые в дальнейшем осуществляют атаки на сервера государственных служб других стран)[114].

Технологии обхода защитных средств и технологии защиты развиваются в совместном противоборстве, и бывает так, что одни технологии переходят в другие. Хорошим примером являются технологии так называемого теневого Интернета (примером могут служить системы — TOR и I2P), которые, предположительно, были созданы спецслужбами Соединенных Штатов Америки с целью обеспечения конфиденциальности работы своих агентов[115]. Но в итоге «теневой Интернет» стал решать задачи совершенно иного характера, в том числе осуществления незаконных сделок по продаже наркотиков, вооружения, организации заказных убийств, а так же взаимодействия террористических и радикальных ячеек по всему миру с целью организации акций устрашения. «Теневым Интернетом» пользуются и различные хакерские группы, такие как Anonymous, целью которых является отстаивание свобод человека и неприкосновенности его жизни. Данный феномен вызывает общественный резонанс, потому что, с одной стороны, действия этой группы не направлены на извлечение прибыли, а с другой стороны, являются незаконными, так как обычно влекут за собой порчу чужого имущества (визуального представления официального сайта, оборудования и т. д.).

В условиях размытости границ в сети Интернет, а так же плотного взаимодействия индивидуумов, зачастую одна и та же группа лиц может по заказу выполнять действия как мошеннического характера, так и террористического, что обостряет необходимость поиска и нейтрализации злоумышленника, какие бы цели он ни преследовал.

Банковский сектор как основной поставщик услуг ЭБ является одной из приоритетных целей злоумышленников. Это связано с намерениями злоумышленников незаметно украсть электронные денежные средства клиентов банка или самого банка.

114 Официальное воровство: как Китай крадет технологии у всего мира. URL: http://inosmi.ru/fareast/20150911/230231504.html

115 https://wikileaks.org/wiki/WikiLeaks: Tor

Несмотря на повышенную угрозу хищений электронных средств, а также возможные санкции со стороны контрольно-надзорных органов, руководство кредитных организаций не всегда в должной мере осознает необходимость увеличения расходов на обеспечение информационной безопасности, а иногда и вообще идет по пути максимального сокращения сотрудников информационной безопасности в целях уменьшения расходов. Сотрудникам профильных подразделений бывает трудно убеждать руководство, «на пальцах» объясняя модель угроз и рисков, доводя до сведения статистику инцидентов. Сказывается инерция высшего образования: вузы, в которых ведется подготовка по специализации «информационная безопасность банков», можно буквально перечесть по пальцам.

Эта и ряд других проблем обеспечения информационной безопасности в гражданских, публичных сферах в значительной мере связаны с относительно недавним появлением данной проблематики в России.

8.1. Проблемы политического характера

Рассматриваемые проблемы можно условно разделить на два типа:

1. Возможные зарубежные санкции и их последствия.
2. Агрессивные действие (военные) в киберпространстве со стороны враждебно настроенного государства или банд-формирования (экстремистской ячейки).

В первом случае необходимо обратиться к опыту 2014 г., когда по решению США платежные системы перестали обслуживать держателей карт некоторых российских банков. Под санкции попали крупные государственные банки (с государственным участием) ОАО «Сбербанк России», ОАО «Банк ВТБ» и сравнительно небольшие ОАО «СМП-Банк» и ОАО «АБ “Россия”».

Потенциальной угрозой для российских банков и платежных систем являются новые зарубежные санкции, которые могут быть поддержаны иностранными производителями программного обеспечения. Возможна приостановка не только поставок новых продуктов, но и обновления уже работающих версий.

Следует помнить, что программное обеспечение банковских автоматизированных систем и систем ДБО во многом базируется на продукции Oracle, Microsoft, Symantec, Cisco и других иностранных компаний, даже если они работают в России через дочерние организации. Эти компании в один «прекрасный» момент могут, ссылаясь на санкции, прекратить поддержку своих продуктов компаниям, попавшим под санкции.

Из-за этого критически возрастут уязвимости, которыми способны воспользоваться злоумышленники. Налицо будет и угроза блокировки извне операционной деятельности банка, которая сделает невозможными расчеты между контрагентами, в частности, торговыми предприятиями. Например, сети продуктовых магазинов со складом.

В результате торговым предприятиям придется платить штрафы по договорным обязательствам, прекратится поступление продукции на прилавки, начнется отток покупателей и уменьшение товарооборота. Банк же потеряет реальную прибыль, так как день простоя банка выражается в многомиллионных суммах, а в худшем случае банк может и лишиться клиента.

В первом случае речь шла о санкциях, которые обычно носят временный характер, что хорошо видно на примере страны Иран, которая с 2006 г. находилась под разными санкциями. Однако в период с 2015 по 2016 г. большая часть из них была снята, в том числе снято блокирование доступа к международной системе SWIFT, которая используется для международных переводов между банками. Во втором же случае речь идет о военных действиях (кибервойнах), направленных на дестабилизацию работы банковских сервисов, включая ЭБ. Конечно, в большой степени это касается банков, обслуживающих крупные предприятия Россия — заводы, фабрики, сектор добычи полезных ископаемых, атомную отрасль и т. д.

Ни для кого уже не секрет, что разработчики информационных систем и оборудования США закладывают в них уязвимости по требованию спецслужб этой страны. По этому же пути идут и разработчики КНР и Израиля. Эти страны преследуют различные цели: начиная от разведывательных, то есть сбора информации, заканчивая в случаях необходимости удаленным выведением из строя систем или оборудования, удаления данных и т. д.

Кроме того, во многих странах идет подготовка войсковых киберподразделений, которые решают задачи нанесения ущерба противнику в киберпространстве.

Хорошим примером может послужить атака, предположительно со стороны ВМС США и Израиля, на ядерный центр Ирана в 2010 г., когда с помощью вируса было выведено из строя 100 ядерных центрифуг. Результатом стало двухгодичное восстановление исследований в ядерной области[116].

В случае атаки на крупный или средний российский банк, включая его резервные центры (резервные ЦОДы), можно получить ситуацию экономического коллапса, так как географически распределенные организации не смогут осуществлять переводы ни с помощью интернет-банкинга, ни при личном визите в соответствующий банк, прекратится товарооборот, начнется повсеместный голод, волнения. То есть страна будет оккупирована в считаные дни без ввода войск.

Вывод. Для решения подобных проблем необходимо государственное участие и системный подход. В том числе необходима поддержка научных исследований и разработчиков решений по информационной безопасности, а также государственное субсидирование предприятий — производителей отечественного ИТ-оборудования и программного обеспечения.

8.2. Проблема «теневого Интернета» на примере системы TOR и идентификации злоумышленников

Для кражи денежных средств клиента или банка злоумышленники все чаще прибегают к системам «теневого Интернета».

Существуют две схожие версии создания «теневого Интернета» (той части Интернета, которая скрыта от людей непосвященных и не имеющих идентификатора для работы со скрытыми сервисами).

116 http://www.nytimes.com/2011/01/16/world/middleeast/16stuxnet.html?_r=0

Первая версия — это следствие желания людей вести деятельность, неподконтрольную силовым ведомствам. Примером может быть осуществление переписки о политических взглядах и т. д.

Вторая версия — это создание инструмента для анонимного взаимодействия силовых ведомств со своими агентами, а также их финансирование с помощью виртуальной валюты, которая неподконтрольна традиционной банковской системе, что по факту делает более успешным проведение какой-либо операции этих агентств.

Авторы склоняются ко второй версии, так как исходный код был разработан Военно-морскими силами Соединенных Штатов Америки, а в дальнейшем выложен в общий доступ (предположительно в целях масштабного развертывания за счет обычных обывателей). Но в целом идея создания «теневого Интернета», независимо от деталей, сводилась к осуществлению скрытой, неподконтрольной кому-либо деятельности. Технологии «теневого Интернета» развивались стремительно. Вначале это были ресурсы (файловые серверы, сайты и т. д.), которые невозможно было найти через поисковые системы типа Google или Yandex. Сейчас же это широко развитые, гибкие, защищенные системы вроде I2P и TOR.

Следует заметить, что в основе работы большинства систем «Теневого Интернета» находится технология NAT, позволяющая маскироваться пользователям.

«Теневой Интернет» дал надежное прибежище криминальному контингенту.

Яркие примеры «луковичных сайтов» из системы TOR, используемых в криминальных целях:

1. http://runionv62ul3roit.onion — анонимный форум. Обсуждаются различные темы, включая изготовление оружия и наркотиков в бытовых (домашних условиях), уход от правосудия.
2. http://clsvtzwzdgzkjda7.onion/ — форум хакеров. Активное обсуждение по взлому сети, элементов банковской инфраструктуры, кражи денег с пластиковых карт.
3. http://silkroadvb5piz3r.onion — сайт по продаже наркотиков, оружия, детской порнографии (рис. 22). Вход только по приглашению (технология приглашения на сайт неизвестна, при входе требуется аутентификация).

4. http://665lw5dt6g32twwo.onion — сайт российских националистов. Централизованная координация действий участников, в том числе силовых акций и действий по подрыву доверия к ветвям власти.

Список не ограничивается перечисленными сайтами, а является выдержкой из множества сайтов «теневого Интернета» в составе TOR. Очевидно, что более 90% опубликованных сайтов в «теневом Интернете» используются в целях, далеких от законных, и посему цели, заявленные при широком развертывании сетей типа TOR, — такие как сохранение свободы человека на частную жизнь, — не соответствуют действительности, а в реальности сети используются для совершения противоправных действий и ухода от правосудия.

В соответствии с технической документацией, размещенной на официальном сайте разработчиков, сеть TOR представляет собой набор созданных на добровольной основе серверов, которые позволяют пользователям этой сети работать с ресурсами сети Интернет, сохраняя свою анонимность и обеспечивая безопасность своих действий. Основной особенностью является создание набора туннелей при соединении пользователя с каким-либо ресурсом. В отличие

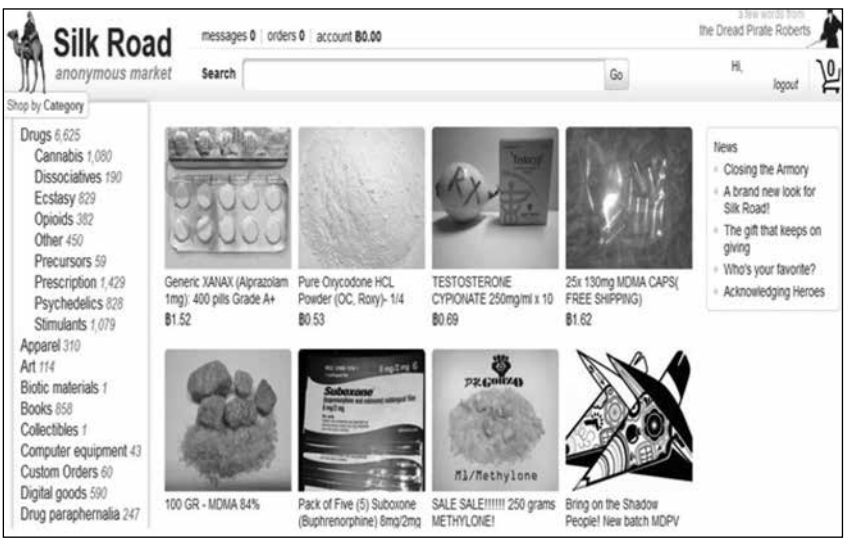

Рис. 22. Сайт по продаже наркотиков в сети TOR

от прямых соединений пользователей при стандартной работе в сети Интернет, это дает возможность публиковать любую информацию, не боясь быть идентифицированным кем-либо.

Заявленные разработчиками цели использования сети TOR:

- обычные граждане имеют возможность без отслеживания их действий посещать любые ресурсы сети Интернет;
- журналисты могут взаимодействовать по защищенным каналам с диссидентами и осведомителями;
- некоммерческие организации могут работать за рубежом со своими домашними сайтами, не уведомляя об этом никого;
- всевозможные группы активистов могут использовать данную систему для реализации прав и свобод граждан всего мира;
- ВМС США используют данную систему для сбора оперативной информации из открытых источников, чтобы скрывать IP-адреса, принадлежащие ВМС США, тем самым не привлекая внимания к своей активности.

Яркими представителями спонсоров развития сети TOR являлись и являются:

1. ВМС США (2001–2006).
2. Национальный научный фонд (2007).
3. Google (2008–2009).
4. Национальная исследовательская лаборатория США (2006–2010).
5. Национальная христианская организация (2010–2012).
6. Фонд Форда (2012–2014).
7. Департамент США по защите прав человека (2013–2016).
8. Министерство иностранных дел Германии (2015).

Работа сети TOR представляет из себя взаимодействие большого количества серверов сети TOR, каждый из которых отдает часть пропускной способности своего интернет-подключения для нужд сети. Этот принцип работы схож с принципом работы пиринговых сетей. Любой пользователь сети TOR может через настройки программы предоставлять свой компьютер как сервер, отдавая часть пропускной способности, тем самым развивая анонимную сеть и улучшая этим собственную анонимность.

Браузер TOR, который предварительно устанавливается пользователем и работает в том числе как прокси-сервер, случайным

образом выбирает несколько серверов из доступных (список серверов браузер TOR периодически скачивает с центрального сервера) и создает тоннель, проходящий через эти сервера. Трафик пользователя будет пропускаться через данный тоннель. У тоннеля есть вход — это браузер TOR на компьютере пользователя и выход — последний из этого тоннеля сервер.

TOR шифрует передаваемые пользователем данные открытыми ключами серверов, входящих в цепочку тоннеля (рис. 23). При этом компьютер пользователя отсылает данные на первый сервер в этой цепи, который снимает с данных свой слой шифра и передает их далее, а с реальной точкой назначения непосредственно общается сервер, служащий точкой выхода из тоннеля.

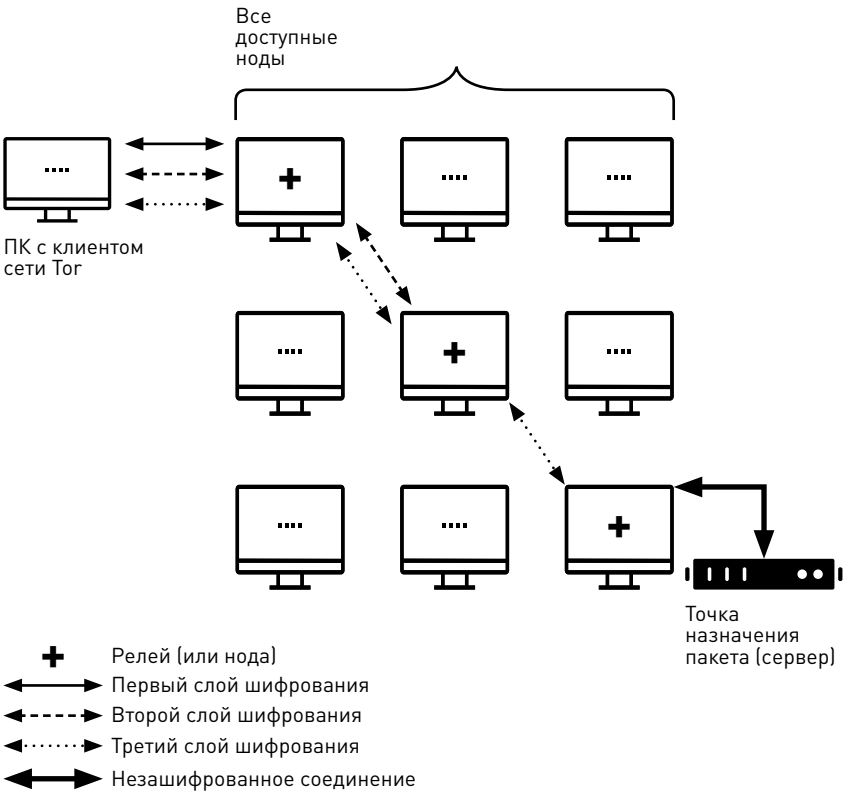

Рис. 23. Принцип работы сети TOR

Данная технология позволяет защитить пользователя от слежки и возможных негативных последствий после посещения специфических сайтов в сети. В точке назначения невозможно определить IP-адрес и местонахождение пользователя, так как пользователь не связывается с ней напрямую, кроме того серверы-посредники получают ограниченные, только необходимые сведения. К примеру, первый сервер в цепочке сети TOR, выбранный для тоннеля, не может точно определить, назначены ли данные для пользователя или он тоже является посредником в цепочке для другого пользователя. Ни один узел в цепочке тоннеля, кроме выходного сервера, не имеет доступа к передаваемым данным (в незашифрованном виде), так как это не нужно для их работы. Серверам из цепочки в тоннеле необходима лишь информация о том, какой следующий сервер в цепи посредников будет получать зашифрованное содержимое.

Для того чтобы каждый сервер в цепи имел только часть необходимой именно для него информации, используется шифрование с открытыми ключами. Данный метод шифрования хорошо себя зарекомендовал и очень надежен, и даже если отдельный сервер в цепочке находится под контролем противника, он не сможет получить информацию, предназначенную для других серверов в цепочке тоннеля.

Только последний сервер R3 в цепочке тоннеля (рис. 23) может расшифровать передаваемые данные, которые он отсылает на конечный пункт назначения (интернет-ресурс). Обратный ответ он может доставить на компьютер пользователя таким же образом, с сохранением анонимности.

Другими словами, есть: входной узел для первичного шифрования; посреднический узел, который осуществляет только обмен между узлами сети TOR; выходной узел, который является передаточным звеном между сетью TOR и ресурсом сети Интернет.

В последней версии TOR используются также сторожевые узлы, которые защищают от компрометации. Фактически они снижают вероятность компрометации, но не обеспечивают полную защищенность. В сети TOR также используются мостовые узлы, которые применяются для построения цепочек и которые являются анонимными. Их основной целью является противодействие блокированию узлов системы TOR по списку.

В качестве еще одной особенности можно отметить построение новой цепочки в системе TOR каждые 10 минут и наличие встроенных механизмов имитации работы некоторых протоколов, с целью обеспечения защищенного обмена между мостами и узлами.

Однако следует заметить, что построение подобных географически распределенных цепей узлов сети снижает скорость работы в Интернете.

Основные уязвимости, дестабилизирующие работу сети TOR, можно разбить на три вида:

1. Уязвимости браузера TOR, работающем на базе браузера Mozilla.
2. Уязвимости архитектуры сети TOR.
3. Уязвимости, связанные с работой других сервисов.

В первом случае идет речь об уязвимостях самого браузера и различных уязвимостях сопутствующих элементов — плагинов. Действительно, уязвимости самого браузера позволяют произвести атаки заинтересованных лиц на самого клиента. Однако даже с ресурсами Агентства национальной безопасности США уследить за всеми пользователями не видится возможным, учитывая тот факт, что устраняются уязвимости довольно быстро. Это подтверждается опубликованными документами в WikiLeaks, ранее украденными Эдвардом Сноуденом. К уязвимостям плагинов можно отнести внутренние ошибки Flash и HTML5, с помощью которых можно вынудить пользователя сети TOR отправить реальный адрес. В настоящий момент эти уязвимости стали менее актуальными в связи с отсутствием поддержки данных плагинов в последних версиях браузера TOR.

Во втором случае используются еще менее эффективные способы, которые требуют использования высокопроизводительных компьютеров:

- Атака по времени. Это расшифровка данных в результате анализа параметров времени шифрования. Эффективность низка, так как происходит шифрование на всех трех узлах цепи серверов TOR. То есть для анализа параметров времени шифрования необходимо слушать траффик на первом узле, однако использование сторожевых узлов сводит эту возможность к минимуму.

- Глобальное пассивное наблюдение. Это позволяет наблюдать отклонения по назначению трафика, тем самым выявляя нужный трафик. Однако данный способ неэффективен, так как выявление отклонений невозможно в случае малых скоростей. А работа пользователей TOR связана преимущественно с малым скоростями, в связи с географической распределенностью узлов, которые участвуют в построении цепи.
- Взлом и заражение мостов TOR с дальнейшей слежкой за пользователями, в том числе подменой ключей шифрования. Поиск мостов, как и их взлом, также считаются задачами малореализуемыми.
- Вывод из строя сторожевых узлов с помощью DoS-атак. В настоящее время уязвимость неактуальна в связи с максимальным сокрытием адресов сторожевых узлов со стороны разработчиков проекта TOR.

В третьем случае уязвимость связана с работой пользователей через TOR с системой Bitcoin. Методика использует уязвимость протокола криптовалюты, которая позволяет клиентам осуществлять свободный сбор статистики и выбор произвольных узлов. Поэтому атакующий, используя даже незначительное в общей массе количество случайных соединений, может собрать достаточно информации для последующего ее анализа. После накопления определенного массива данных, применяя DoS-атаку на сеть Bitcoin, можно деанонимизировать не менее половины ее пользователей. Так как в системе Bitcoin по умолчанию применяется бан IP-адресов, причастных к DoS-атакам, ее применение через выходные узлы TOR позволяет последовательно выводить из строя клиентов, работающих через эту анонимную сеть. И как следствие, становится возможным выделение тех из них, которые не работают с клиентом, выходящим в сеть через TOR. Опасность этой атаки заключается в том, что она работает, даже если соединения с Bitcoin зашифрованы. Однако атака неэффективна в случае краткосрочных действий пользователей в сервисе Bitcoin, не говоря о том, что работа с виртуальной валютой не является нарушением закона.

Регулярно публикуются новые исследования об уязвимостях TOR, однако в большинстве своем уязвимости носят либо кратко-

срочный характер, то есть легко устраняются, либо могут быть использованы только при каких-то ограничениях и/или в малых сегментах сети.

На данном этапе TOR остается одной из самых защищенных систем. В настоящий момент в разных странах мира (в том числе силовыми ведомствами) ведутся разработки по модификации TOR или по использованию дополнительных программ вкупе с TOR с целью создания более защищенной системы.

Вывод: система TOR является неотъемлемой частью Теневого Интернета и преимущественно используется для ведения незаконной деятельности, а также ухода от правосудия, в том числе при атаках на СЭБ. Несмотря на это, различные коммерческие и государственные организации (преимущественно из США) продолжают спонсировать данный проект под предлогом защиты прав человека. Технология работы данной сети, а также ее постоянное развитие не позволяют в полной мере противоборствовать противозаконным действиям, совершаемым в рамках данной сети. А топология самой системы исключает возможности для предотвращения ее использования и деанонимизации большей части пользователей данной сети, а также ее взлома или вывода из строя. Перечисленные факты подталкивают к необходимости инновационного подхода к противодействию подобным сетям.

8.3. Проблемы законодательного характера

В нынешних реалиях российские банки максимально стараются переложить риски информационной безопасности при предоставлении услуг ЭБ, включая риски кражи электронной подписи, несанкционированного доступа к личному кабинету, мошенничества и т. д., на плечи самого клиента. Очень малое количество операторов по переводу денежных средств и платежных систем в полной мере отдают отчет в том, что качество обеспечения безопасности того или иного сервиса — залог плодотворного взаимодействия с клиентом. Лишь в редких случаях суды общей юрисдикции Российской Федерации идут по пути того, чтобы обязать тот или иной банк вернуть деньги

клиенту, если клиент после кражи денег выдвигает исковое требование к банку о возврате денег, руководствуясь позицией, что безопасность сервиса — это обязанность стороны, предоставляющей услугу интернет-банкинга.

Основной закон, регламентирующий переводы денежных средств в электронном виде, — Федеральный закон от 27.06.2011 № 161-ФЗ «О национальной платежной системе». В статье 9 этого закона не указано, каким образом клиент должен быть уведомлен о проведенном платеже, хотя именно своевременное уведомление клиента позволяет избежать мошенничества. В статье 27 этого закона не установлена ответственность участников за невыполнение требований по информационной безопасности, установленных Правительством Российской Федерации и Банком России, а также не выстроена концепция, которая ориентирует банки максимально обеспечивать защищенность своих сервисов, включая СЭБ. Это уже не говоря о таких сложностях, как нахождение клиента за рубежом и невозможность сообщить банку о проблемах: например, у клиента может быть утерян носитель электронной подписи, нет возможности позвонить, а банк не принимает сообщения по электронной почте.

На настоящий момент большинство договоров банков с клиентом выстраиваются с максимальной защитой интересов самих банков, а не их клиентов. В подобных условиях банк обходится минимальным набором защитных механизмов.

Необходимо отметить, что ЭБ не ограничивается только переводом электронных денежных средств, он также подразумевает возможность для клиента давать поручение на приобретение ценных бумаг или валюты на Московской бирже в рамках брокерского договора. А риски по этому направлению иной раз куда выше, чем при операциях перевода электронных денежных средств в системах «Банк–Клиент».

Еще один важный момент заключается в том, что большинство банков пытаются перекладывать на клиента расходы на дополнительные средства безопасности, как то токены, средства подтверждения транзакций и т. д. Индивидуальные предприниматели и малый бизнес максимально стараются снизить свои расходы на обслуживание, а в итоге оказываются в зоне риска, не имея достаточных знаний по пользованию техническими средствами, не устанавливая

банального антивирусного средства на рабочем персональном компьютере, на котором осуществляется соединение с банком, не говоря о более сложных ситуациях, например, использовании бесплатного Wi-Fi в общественных местах.

Усложняет ситуацию то, что в соответствии с Федеральным законом от 06.04.2011 № 63-ФЗ «Об электронной подписи» отсутствует унифицированный подход (обязательство любой организацией принять документ, подписанный усиленной квалифицированной электронной подписью) к электронной подписи: гражданин или юридическое лицо не могут сгенерировать ключи электронной подписи и выпустить в сертифицированном удостоверяющем центре по доступной цене квалифицированный сертификат, а далее использовать усиленную квалифицированную подпись в любой системе интернет-банкинга банка, микрофинансовой организации, ломбарда, платежного агента и т. д.

Данная проблема сказывается на сложности управления своими услугами со стороны клиента, повышаются риски физической кражи носителей криптографических ключей и сложности управления верификации транзакций.

Федеральный закон от 27.07.2006 № 152-ФЗ (ред. от 21.07.2014) «О персональных данных», с учетом невысоких штрафных санкций, предусмотренных КоАП, не обязывает со всей серьезностью относиться к обеспечению безопасности персональных данных, особенно когда вопросы касаются взыскания денежных средств с должников или навязывания дополнительных услуг своим клиентам.

По причине отсутствия судебной практики и реальной ответственности со стороны банков, банки нарушают статью 26 Федерального закона от 02.12.1990 № 395–1 (ред. от 05.04.2016) «О банках и банковской деятельности» и передают сведения, относящиеся к банковской тайне, третьим лицам — акционерам, материнским банкам, в том числе зарубежным.

Законодательная база России в области информационной безопасности не в полной мере соответствует реальным нуждам в данной сфере. Процесс законотворчества, создание новых законов и редактирование действующих, требуют вовлечения тех людей, которые непосредственно обеспечивают информационную безопасность на местах.

8.4. Проблемы обеспечения информационной безопасности на местах в банковском секторе

Системы ЭБ, кроме случаев аутсорсинга, являются неотъемлемой частью инфраструктуры банка, и качество обеспечения безопасности на местах напрямую сказывается на возможностях злоумышленника произвести атаку на банк. Зачастую сам банк является пользователем систем интернет-банкинга. К ним можно отнести системы управления депозитарными счетами в уполномоченных банках Московской биржи, системы перевода денежных средств через Банк России, отправку отчетности в Банк России, взаимодействие с платежными системами, как то «Город» или QIWI, для ускоренного перевода платежей, связанных с оплатой мобильной связи и т. д., систему SWIFT, системы перевода моментальных платежей типа Western Union и т. д.

Положение Банка России от 9 июня 2012 г. «О требованиях к обеспечению защиты информации при осуществлении переводов денежных средств и о порядке осуществления Банком России контроля за соблюдением требований к обеспечению защиты информации при осуществлении переводов денежных средств» № 382-П, а также отраслевые стандарты Банка России по информационной безопасности[117] призваны максимально обезопасить банки от возможных попыток злоумышленников украсть деньги или нанести вред банку, например сорвать сделку крупного клиента банка, который должен внести до какого-то времени авансовый платеж, чтобы начать сотрудничество с определенным покупателем.

Основные ошибки и проблемы при обеспечении информационной безопасности на местах:

1. Некачественно сформированный процесс управления криптографическими ключами. Обычно это проявляется в том, что ключи передаются неуполномоченным лицам, конечная отправка платежей осуществляется не с выделенного

117 С содержанием Стандартов Банка России по информационной безопасности можно ознакомиться на официальном сайте Банка России http://www.cbr.ru/psystem/

рабочего места как физически, так и отделенного от сети банка.

2. В небольших банках можно встретить ситуацию, когда ключи нескольких пользователей записаны на один накопитель, а также на постоянной основе размещен компьютер, с которого администраторы удаленно осуществляют отправку. Данная ситуация дает хорошую возможность для злоумышленников, которые каким-то образом проникли в банк — через подкупленного сотрудника, занесенного вируса или нелояльного сотрудника самого банка, в том числе сотрудника ИТ-подразделения.
3. Неподготовленность персонала к воздействиям извне. Социальная инженерия остается одной из самых актуальных проблем. Нередко злоумышленники собирают информацию об определенных сотрудниках из социальных сетей, форумов и т. д. Далее, представляясь сотрудниками регуляторов, различных ведомств, сотрудниками технической поддержки, преступники просят произвести перевод денежных средств. Также нередки случаи, когда злоумышленники направляют письма сотрудникам от имени каких-то проверяющих органов с вложением (якобы отчетом), открыв которое сотрудник банка заражает рабочую станцию.
4. Низкая организованность в предоставлении доступа. Нередко в банках можно встретить ситуацию, когда на площадке (в помещении), где работают дилеры, используется вход в системы под одной учетной записью, что усложняет возможность контроля действий дилеров, а также расследования инцидентов.
5. Экономия на средствах безопасности. В первую очередь нарушаются требования об эшелонировании антивирусной безопасности, которая хотя бы разделяет серверный и пользовательский сегмент в банке. Данные нарушения облегчают задачу злоумышленнику произвести заражение станций.
6. Плохое сегментирование сети на сетевом уровне, отсутствие шифрования.
7. Нерегулярное сканирование инфраструктуры на наличие уязвимостей.

8. Сокращение штатов в подразделении, ответственном за информационную безопасность (неудивительно, что большая часть злоумышленных действий проводится бывшими сотрудниками ИТ/ИБ банков), или наличие непрофессиональных сотрудников. Нередки ситуации, когда менеджерский состав по информационной безопасности выстраивается по принципу «свой–чужой», и предпочтение отдается «проверенным людям», а не талантливым и профессиональным.
9. Несвоевременное обеспечение информационной безопасности систем интернет-банкинга. Очень показательный инцидент был в марте 2014 г., когда, используя уязвимости Heartbleed, злоумышленники вмешались в работу системы продажи билетов РЖД и могли перехватывать платежи процессинга ВТБ118.
10. И, пожалуй, самой распространенной ошибкой, даже для крупных банков, является отсутствие риск-ориентированного подхода к информационной безопасности. Это выражается в поиске баланса между потребностями бизнеса, проблемами безопасности, а также разницей в возможностях современных технологий безопасности с тем, что есть инновационного в мире информационных технологий. К сожалению, в большинстве случаев преобладает или узкотехнический подход, или нормативно-регламентирующий.

Данный список неполон, однако даже такие типовые проблемы и ошибки дают хорошие возможности для злоумышленников, заразив сеть банка или используя уязвимости самих систем интернет-банкинга, получить доступ к управлению средствами с целью их кражи. Только вовлеченность руководства кредитных организаций и риск-ориентированный подход в состоянии изменить проблему и улучшить состояние безопасности ЭБ.

8.5. Проблемы обеспечения информационной безопасности на стороне клиента

Концептуальная схема, выработанная российским банковским сообществом, такова: большую часть рисков при использовании систем интернет-банкинга несет сам клиент.

Нередки случаи, когда банки навязывают средства безопасности, которые фактически не выполняют свою функцию, в том числе это касается различных токенов, которые не в состоянии защитить от подмены платежа в момент подписания.

Системы в банках по противодействию мошенничеству также могут быть обойдены злоумышленниками с помощью имитации повседневного платежа, постепенного вывода денег, использования всех данных самого клиента и т. д.

Сами клиенты нередко пренебрегают правилами безопасности:

1) легко сообщают сведения о пароле, данных карточки незнакомым лицам, в том числе по телефону;
2) переходят на поддельные сайты, не обращая внимания на оформление и адрес самого сайта;
3) размещают в свободном доступе паспортные данные, что позволяет злоумышленникам подделать доверенность и выпустить новую сим-карту для подтверждения платежей;
4) не заботятся об антивирусной защите, поэтому злоумышленникам не составляет труда получить доступ к СЭБ.

Данный список также неполон, однако демонстрирует слабую осведомленность клиентов о мерах безопасности. Отсутствие жесткой обязанности участия банков в предоставлении безопасного сервиса клиентам ведет к тому, что мошенники и по сей день имеют возможность наращивания капитала, полученного преступным путем.

Обеспечение информационной безопасности СЭБ в России требует системного подхода. Проблемы отсутствия ИТ-систем собственного производства, доверенной банковской зоны, широкое распространение «теневого Интернета», нежелание банков обеспечивать информационную безопасность на местах, низкая осведомленность обычных пользователей, в первую очередь граждан и представителей малого бизнеса, создают плодотворное поле для процветания мошеннического контингента.

Предстоит большая работа для того чтобы изменить ситуацию, однако в России присутствуют люди, которые болеют за дело и которым небезразлично состояние информационной безопасности как на местах, так и в стране в целом. При поддержке Банка России и силовых ведомств, а также правильного законодательного фона, возможно создание защищенного ЭБ и качественно нового интернет-продукта для клиентов кредитных организаций и не только.

ЗАКЛЮЧЕНИЕ

В заключение хотелось бы еще раз обратить внимание на то, что прогресс в области информационных и телекоммуникационных технологий и последующее за ним развитие технологий ДБО внесли принципиальные изменения в работу кредитных организаций. Это обусловлено наблюдающимися изменениями в информационном контуре банковской деятельности и появлением в нем новых участников: провайдеров услуг и различных каналов связи, а также появлением совершенно нового типа клиента, который уже не приходит в банк для того, чтобы осуществить те или иные банковские операции, а сам становится «операционистом».

Тем, кто сомневается в том, что технологии ДБО (включая системы ЭБ) будут активно использоваться в банковском бизнесе, авторы предлагают ответить на несколько вопросов:

1. Согласны ли Вы, что количество пользователей Интернета в ближайшие несколько лет будет только расти?
2. Согласны ли Вы, что количество банковских услуг, предоставляемых через Интернет, будет расти ввиду их явной дешевизны по отношению к обслуживанию «в офисе»?
3. Согласны ли Вы, что большинство клиентов желает, чтобы их банковские операции выполнялись как можно быстрее?
4. Согласны ли Вы, что клиентам удобно иметь возможность контролировать состояние своего банковского счета в режиме «24 × 7»?
5. Согласны ли Вы, что клиентам удобнее совершать свои операции, не имея привязки к определенному месту?
6. Согласны ли Вы, что отсутствие прямого контакта банка с клиентом (при использовании технологий ДБО и ЭБ, в частности) приводит к росту количества преступлений с использованием компьютерных технологий и глобальной сети Интернет?

Очевидно, что большинство опрашиваемых дадут положительные ответы на все вопросы. Исходя из этого можно сделать только

один вывод: в ближайшее время технологии ДБО (и системы ЭБ, в частности) будут активно внедряться в банковский бизнес, а способы совершения преступлений, связанных с хищением денежных средств с использованием компьютерных технологий и удаленного доступа, будут только совершенствоваться.

Лишь целенаправленная работа по обеспечению безопасности ЭБ может свести к минимуму возможности киберпреступников и обеспечить доверие к данному виду ДБО.

СПИСОК ИСПОЛЬЗОВАННЫХ ИСТОЧНИКОВ И ЛИТЕРАТУРЫ

Нормативные правовые акты

1. Федеральный закон от 02.12.1990 г. № 395-1 «О банках и банковской деятельности».
2. Федеральный закон от 7 августа 2001 г. № 115-ФЗ «О противодействии легализации (отмыванию) доходов, полученных преступным путем, и финансированию терроризма».
3. Федеральный закон от 10 июля 2002 г. № 86-ФЗ «О Центральном банке Российской Федерации (Банке России)».
4. Федеральный закон от 27 июля 2006 г. № 149-ФЗ «Об информации, информационных технологиях и о защите информации».
5. Федеральный закон от 27 июня 2011 г. № 161-ФЗ «О национальной платежной системе».
6. Федеральный закон от 6 апреля 2011 г. № 63-ФЗ «Об электронной подписи».
7. Приказ ФСБ России от 27 декабря 2011 г. № 796. Приложение 1.
8. Письмо Банка России от 24 мая 2005 г. № 76-Т «Об организации управления операционным риском в кредитных организациях».
9. Письмо Банка России от 27 апреля 2007 г. № 60-Т «Об особенностях обслуживания кредитными организациями клиентов с использованием технологии дистанционного доступа к банковскому счету клиента (включая интернет-банкинг)».
10. Письмо Банка России от 7 декабря 2007 г. № 197-Т «О рисках при дистанционном банковском обслуживании».
11. Письмо Банка России от 31 марта 2008 г. № 36-Т «О Рекомендациях по организации управления рисками, возникающими при осуществлении кредитными организациями операций с применением систем интернет-банкинга».

12. Письмо 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».
13. Письмо Банка России от 14 декабря 2012 г. № 172-Т «О Рекомендациях по вопросам применения статьи 9 Федерального закона «О национальной платежной системе».
14. Письмо Банка России от 10 июня 2013 г. № 104-Т «О повышении внимания кредитных организаций к отдельным операциям клиентов».
15. Письмо Банка России от 19 июня 2013 г. № 110-Т «О повышении внимания кредитных организаций к отдельным операциям клиентов».
16. Письмо Банка России от 24 марта 2014 г. № 49-Т «О рекомендациях по организации применения средств защиты от вредоносного кода при осуществлении банковской деятельности».
17. Стандарт Банка России «Обеспечение информационной безопасности организаций банковской системы Российской Федерации. Общие положения» СТО БР ИББС-1.0-2014.

Книги и статьи

18. *Акаткин Ю.М., Конявский В.А.* Безопасный доступ к корпоративным облачным приложениям. Information Security / Информационная безопасность. 2014. № 1.
19. *Бирюков К.А.* Средства безопасного хранения ключей // Безопасность информационных технологий. М., 2013. № 3. — С. 50–53.
20. *Грень И.В.* Компьютерная преступность. — Минск: Новое знание, 2007. — 413 с.
21. Дистанционное банковское обслуживание / Центр исследований платежных систем и расчетов. — М.: КноРус, 2010. — 328 с.
22. *Конявская С.В.* Информатизация без нагрузки // Национальный банковский журнал. 2016. № 2 (февраль). — С. 58–59.
23. *Конявский В.А.* Управление защитой информации на базе СЗИ НСД «Аккорд». — М.: Радио и связь, 1999. — 325 с.

24. *Конявский В.А., Гадасин В.А.* Основы понимания феномена электронного обмена информацией. — Мн.: Серия «Библиотека журнала “УЗИ”», 2004. — 327 с.
25. *Конявский В.А., Лопаткин С.В*. Компьютерная преступность. Т. I, II. — М., 2006, 2008. — 560 с., 840 с.
26. *Конявский В.А.* Защищенный микрокомпьютер МК-TRUST — новое решение для ДБО. Национальный банковский журнал, 2014. № 3 (март).
27. *Конявский В.А., Акаткин Ю.М.* Мы не доверяем облаку или облако нам? Information Security / Информационная безопасность, 2014. № 1.
28. *Конявский В.А., Степанов В.Б*. Компьютер типа «тонкий клиент» с аппаратной защитой данных: Патент на полезную модель № 118773. 27.07.2012, бюл. № 21.
29. *Конявский В.А.* Компьютер с аппаратной защитой данных от несанкционированного изменения: Патент на полезную модель № 137626. 20.02.2014, бюл. № 5.
30. *Конявский В.А.* Мобильный компьютер с аппаратной защитой доверенной операционной системы: Патент на полезную модель № 138562. 20.03.2014, бюл. № 8.
31. *Конявский В.А.* Мобильный компьютер с аппаратной защитой доверенной операционной системы от несанкционированных изменений: Патент на полезную модель № 139532. 20.04.2014, бюл. № 11.
32. *Конявский В.А.* Мобильный компьютер с аппаратной защитой доверенной операционной системы: Патент на полезную модель № 147527. 10.11.2014, бюл. № 31.
33. *Конявский В.А., Акаткин Ю.М*. Мобильный компьютер с аппаратной защитой доверенной операционной системы от несанкционированных изменений: Патент на полезную модель № 151264. 27.03.2015, бюл. № 9.
34. *Конявский В.А.* Рабочая станция с аппаратной защитой данных для компьютерных сетей с клиент-серверной или терминальной архитектурой: Патент на полезную модель № 153044. 27.06.2015, бюл. № 18.
35. *Конявский В. А.* Не надо оплачивать уязвимости // Аналитический банковский журнал. 2014. № 10 (222). — С. 62–64.

36. *Конявский В.А.* Компьютер с вирусным иммунитетом // Информационные ресурсы России. 2015. № 6. — С. 31–34.
37. *Конявский В.А.* Эпохе бурного развития — компьютер с динамической архитектурой // Национальный банковский журнал. 2016. № 3(март). — С. 102–103.
38. *Конявский В.А.* Научно-методические проблемы создания защищенных информационных технологий // ВКСС Connect! 2006. № 1 (34). — С. 41–43.
39. *Конявский В.А., Лопаткин С.В.* Компьютерная преступность. В 2-х т. Т. 1. — М.: РФК-Имидж Лаб, 2006. — 560 с.
40. *Кравец В.В.* Идеальный токен // Комплексная защита информации: материалы XX науч.-практ. конф. — Минск, 19–21 мая 2015 г. — Мн.: РИВШ, 2015. — С. 114–115.
41. *Ладынская Ю.П., Батраков А.Ю.* Хранение данных СКЗИ: выбор носителя // Информационная безопасность: материалы XIII Международной конференции. — Таганрог, 2013. Часть 1. — С. 129–134.
42. *Логинов Е.Л.* Отмывание денег через интернет-технологии. — М.: ЮНИТИ-ДАНА, 2005. — 208 с.
43. *Лямин Л.В.* Применение технологий электронного банкинга: риск-ориентированный подход. — М.: КноРус: ЦИПСиР, 2011. — 336 с.
44. *Ревенков П.В., Бердюгин А.А.* Дистанционное банковское обслуживание: Интернет создает нового клиента и расширяет профили рисков // Банковское дело, 2013. № 12 (240). — С. 64–67.
45. *Ревенков П.В., Дудка А.Б., Сычев А.М., Пеленицын А.М.* Электронный банкинг: сопутствующие риски и особенности безопасного функционирования: Практ. пособие. — М.: ИД «Регламент», 2009. — 248 с.
46. *Ревенков П.В.* Управление рисками в условиях электронного банкинга: Монография. — М.: ИД «Экономическая газета», 2011. — 168 с.
47. *Ревенков П.В.* Финансовый мониторинг в условиях интернет-платежей. — М.: КноРус: ЦИПСиР, 2016. — 64 с.
48. *Реформатский А.А.* Лингвистика и поэтика. — М., 1987. — С. 52–76.
49. *Роговский Е.А.* Кибер-Вашингтон: глобальные амбиции. — М.: Международные отношения, 2014. — 848 с.

50. Специальный съемный носитель информации. Патент на полезную модель № 94751. 27.05.2010, бюл. № 15.
51. Съемный носитель ключевой и конфиденциальной информации. Патент на полезную модель № 147529. 10.11.2014, бюл. 31.
52. *Сычев М.Ю.* Основы информационной безопасности. — М.: ЕАОИ, 2007. — 300 с.
53. Форензика — компьютерная криминалистика / Н.Н. Федотов. — М.: «Onebook.ru», 2012. — 420 с.: ил.
54. *Фролов Д.В., Поспелов А.Л., Ревенков П.В.* Обеспечение информационной безопасности в условиях ДБО // Аналитический банковский журнал. 2014. № 6 (219). — С. 76–81.
55. *Фролов Д.Б., Персанов Д.Ю.* Практические аспекты аутсорсинга процессов обеспечения безопасности // БИТ МИФИ, 2012 — С. 128–132.
56. *Фролов Д.Б.* FinCERT: основные задачи и направления развития // Банковское дело, 2016, № 2.
57. Цифровой банк: как создать цифровой банк или стать им / Крис Скиннер; пер. с англ. Сергея Смирнова. — М.: Манн, Иванов и Фербер, 2015. — 320 с.
58. *Кинг Б.* Банк 3.0. Почему сегодня банк — это не то, куда вы ходите, а то, что вы делаете. — М.: ЗАО «Олимп-Бизнес», 2014. — 520 с.

Электронные ресурсы

59. *Крылов Г.О.* «Международные проблемы информационного права» // http://search.rsl.ru/: Электронная библиотека Российской Государственной Библиотеки, 2013. URL: http://search.rsl.ru/ru/record/01006682336
60. *Лунтовский Г.И.* Внимание к безопасности — критерий зрелости / BIS – Journal № 2 (21), 2016.
61. *Неваленный А.В.* «Переоценка приоритетов» // http://www.journal.ib-bank.ru: электронная версия журнала «Информационная безопасность банков», 2015. URL: http://www.journal.ib-bank.ru/post/335

62. *Фролов Д.Б., Неваленный А.В.* Противодействовать кризису // http://www.journal.ib-bank.ru: электронная версия журнала «Информационная безопасность банков», 2015. URL: http://www.journal.ib-bank.ru/post/359
63. Trusted Cloud Computers [Электронный ресурс]: http://www.trustedcloudcomputers.ru

Документы, размещенные на официальном сайте Базельского комитета по банковскому надзору (bis.org)

64. Risk Management Principles for Electronic Banking July 2003. URL: http://www.bis.org/publ/bcbs98.htm
65. Risk Management Principles for Electronic Banking May 2001. URL: http://www.bis.org/publ/bcbs82.htm
66. Management and Supervision of Cross-Border Electronic Banking Activities October 2002. URL: http://www.bis.org/publ/bcbs93.htm
67. Risk Management for Electronic Banking and Electronic Money Activities March 1998. URL: http://www.bis.org/publ/bcbs35.pdf
68. Electronic Banking Group Initiatives and White Papers October 2000. URL: http://www.bis.org/publ/bcbs76.htm

Сычев А.М., Ревенков П.В., Дудка А.Б.

БЕЗОПАСНОСТЬ ЭЛЕКТРОННОГО БАНКИНГА

Руководитель проекта *М. Султанова*
Корректор *И. Астапкина*
Компьютерная верстка *Б. Руссо*

Подписано в печать 20.04.2017. Формат 60×90/16.
Бумага офсетная № 1. Печать офсетная.
Объем 20,0 п. л. Тираж 2000 экз. Заказ № .

ООО «Интеллектуальная Литература»
109380, г. Москва, ул. Степана Шутова, д. 4, стр.1
Тел. +7 (495) 363-13-48
e-mail: info@intlit.ru

Знак информационной продукции
(Федеральный закон № 436-ФЗ от 29.12.2010 г.)

18+

О КОМПАНИИ БЭСТ

БЭСТ — быстроразвивающаяся молодая российская платежная система. Платежная система «БЭСТ» была зарегистрирована Центральным Банком РФ в июле 2014 года. Головной офис организации расположен в Москве. Контролируется организация полностью российскими владельцами. Технологии, используемые компанией, также имеют российское происхождение, что позволило БЭСТ получить статус национально значимой платежной системой.

В июле 2015 года Платежная система «БЭСТ» зарегистрирована, как Оператор по обработке персональных данных. В сентябре 2015 года ею был получен сертификат безопасности ФСБ, став первой некредитной организацией получившей необходимые лицензии ФСБ.

В настоящее время имеется два расчетных центра: НКО «Объединенная расчетная система» (АО) и АО «Банк Воронеж».

Уникальность технологий системы позволило наладить получение переводов не только в пунктах выдачи, но и в банкоматах некоторых партнеров. При этом нет необходимости в пластиковой карте. Первым стратегическим партнером по реализации данной услуги компании стал ПАО «БИНБАНК».

Система БЭСТ обладает готовыми техническими решениями и легким интеграциным процессом, подключения ориентированные на Банки, микрофинансовые организации, компании использующие терминальный процессинг или Интернет эквайринга (по России и за рубежом) и пр.

Преимуществами Платежной системы «БЭСТ» является интеграционные взаимоотношения с различными платежными системами денежных переводов России и Зарубежья, высокая доля комиссионного вознаграждения Партнеров, возможность маршрутизировать отправку переводов, принудительно или автоматически, а также безопасность работы системы.

Будем рады видеть Вас в числе наших Партнеров!

О КОМПАНИИ PAYPAL

Компания PayPal была основана в 1998 году группой энтузиастов, которые увидели необходимость в новой форме денег для цифрового будущего. Уже 18 лет PayPal предлагает своим клиентам простой, удобный и более безопасный способ оплачивать товары или отправлять личные платежи.

В 2016 году PayPal обработала 6,1 млрд транзакций, 2 млрд из которых были совершены через мобильные устройства. Обслуживая 200 млн активных счетов своих клиентов, PayPal удалось построить платформу электронных платежей поистине глобального масштаба. Она представлена более чем на 200 рынках, поддерживает платежи с использованием более 100 мировых валют, позволяет выводить деньги на банковские счета в 56 валютах и хранить средства на счетах PayPal в 25 валютах.

PayPal позволяет своим пользователям оплачивать покупки и отправлять деньги, не раскрывая данные банковской карты или другую финансовую информацию.

Платежи через PayPal покрываются Программой защиты покупателей и Программой защиты продавцов[1], в рамках которых PayPal помогает решать спорные ситуации. Если товар не подошел и требуется вернуть покупку продавцу, PayPal также предоставляет услугу бесплатного возврата товаров, возмещая стоимость обратной доставки[2].

Предпринимателям PayPal предлагает ряд решений по приему онлайн-платежей. Продавцы могут установить PayPal на своем веб-сайте, либо выставлять счета на оплату по электронной почте. Это более быстрый и безопасный способ получения средств через интернет — деньги поступают на счет PayPal в считанные минуты, и затем могут быть выведены на банковский счет.

Полномасштабную деятельность на российском рынке компания PayPal начала в 2013 году. С этого момента российские клиенты получили возможность осуществлять электронные платежи, а также отправлять/принимать денежные переводы и выводить средства на банковские счета в российских рублях. Это также позволило клиентам PayPal принимать платежи на своих сайтах, в том числе и от зарубежных покупателей, привлекая еще больше клиентов со всего мира. Кроме того, жители России получили уникальную для других рынков возможность быстро и просто пополнять свои счета PayPal наличными в офисах Евросети и Связного.

За годы работы на российском рынке компания PayPal установила партнёрские отношения с тысячами отечественных компаний самого различного масштаба, от небольших магазинов до таких лидеров рынка как: Аэроэкспресс, Афиша, Детский мир, e96, Groupon, LaModa, ЛитРес, Mail.ru, OZON.ru, Туту.ру, ВКонтакте, Emex, Exist.ru и многие другие.

1 https://www.paypal.com/ru/webapps/mpp/paypal-safety-and-security
2 https://www.paypal.com/ru/webapps/mpp/refunded-returns