Банковский бизнес

БАНКОВСКИЙ БИЗНЕС

ЕЖЕКВАРТАЛЬНЫЙ НАУЧНО-ПРАКТИЧЕСКИЙ ЖУРНАЛ

№ 4`2016

РЕДАКЦИЯ

119034 Москва,
ул. Пречистенка,
д. 10, офис 7
Тел.: +7 499 766-92-77,
766-97-92, 766-93-04

E-mail: study@v-consult.ru
Сайт: www.v-consult.ru

Отпечатано и разработано
в ООО «Издательство
«Граница»
123007 Москва,
Хорошевское шоссе, 38

Тел.:
+7 495 941-26-66, 36-46
E-mail:
granica_publish@mail.ru

СОДЕРЖАНИЕ

ГОСУДАРСТВЕННАЯ ДУМА ФЕДЕРАЛЬНОГО СОБРАНИЯ
РОССИЙСКОЙ ФЕДЕРАЦИИ СЕДЬМОГО СОЗЫВА

2 декабря 2016 года № 350-7 ГД

г. Москва

ПОСТАНОВЛЕНИЕ

Об Основных направлениях единой государственной денежно-кредитной политики на 2017 год и период 2018 и 2019 годов

Рассмотрев представленные Центральным банком Российской Федерации Основные направления единой государственной денежно-кредитной политики на 2017 год и период 2018 и 2019 годов, в соответствии со статьей 45 Федерального закона от 10 июля 2002 года № 86-ФЗ «О Центральном банке Российской Федерации (Банке России)» Государственная Дума Федерального Собрания Российской Федерации постановляет:

1. Принять к сведению Основные направления единой государственной денежно-кредитной политики на 2017 год и период 2018 и 2019 годов.

2. Настоящее Постановление вступает в силу со дня его принятия.

Председатель Государственной Думы
Федерального Собрания Российской Федерации **В. В. Володин**

Из Основных направлениий единой государственной денежно-кредитной политики на 2017 год и период 2018 и 2019 годов*

ВВЕДЕНИЕ

События последних лет показывают, что назрела необходимость смены модели экономического развития России. Для того чтобы обеспечить устойчивый экономический рост и повышение благосостояния общества, важно снизить уязвимость экономики к изменению внешних условий, решить глубокие внутренние структурные проблемы. Они проявились не только в экономическом спаде, последовавшем за снижением цен на сырьевые товары российского экспорта в 2014 г., но и в предшествовавшей ему затухающей экономической динамике (даже при благоприятной конъюнктуре мировых товарных рынков). Вектор развития России будет зависеть от готовности как органов государственного управления, так и всех членов общества перейти к инвестиционно-инновационной модели экономического роста, приложить усилия к формированию его внутреннего потенциала и созданию благоприятной среды для экономической деятельности. Для этого в первую очередь требуются повышение эффективности управления, обновление основных фондов и развитие инфраструктуры, внедрение новых технологий, а также формирование качественных институтов, что будет способствовать повышению производительности труда. По сути, это вызов для органов государственного управления, регуляторов и всех участников экономических отношений на всех уровнях, в том числе для Банка России.

Банк России нацелен на обеспечение ценовой и финансовой стабильности как важных условий для устойчивого экономического роста и социального благополучия. Комплексность и многоплановость решаемых задач, а также широкий спектр воздействия на экономическую систему принимаемых Банком России решений требуют от него взвешенного и сбалансированного подхода, особенно в условиях накопившихся структурных ограничений в экономике и при сохраняющемся негативном влиянии внешних факторов. Неотъемлемым элементом такого подхода является согласованность решений по всем направлениям деятельности Банка России, а также его тесное взаимодействие с органами законодательной и исполнительной власти.

Проводимая в рамках стратегии таргетирования инфляции денежно-кредитная политика, наряду с другими мерами государственной политики, в исключительно сложных внешних условиях сыграла роль амортизатора, сгладив влияние внешних шоков на функционирование экономики и жизнь людей. Действия Банка России и в дальнейшем будут направлены на поддержание внутренней экономической стабильности, в первую очередь — на замедление инфляции и сохранение ее на уровне около 4%, а также на стимулирование сбережений домашних хозяйств, их защиту от инфляционного обесценения и создание условий для трансформации сбережений в инвестиции, что является важной составляющей новой модели роста экономики. Для решения этих задач необходимо сохранить умеренно жесткую денежно-кредитную политику, обеспечивающую положительный уровень реальных процентных ставок.

Политика Центрального банка обеспечивает ряд важных условий для сбалансированного экономического развития. В то же время с учетом характера решаемых Центральным банком задач его политика по объективным причинам не может стать основной движущей силой экономического роста. Успешность принимаемых Банком России мер будет во многом зависеть от контекста общей стратегии макроэкономической политики, перспектив преодоления структурных ограничений в экономике. Для устойчивого роста благосостояния, повышения уровня и качества жизни людей необходимо, чтобы структурная политика, создающая стимулы для интенсивного развития, стала основным пунктом общественной, политической и экономической повестки.

* Одобрено Советом директоров Банка России 11 ноября 2016 года.

1. ЦЕЛИ И ПРИНЦИПЫ ДЕНЕЖНО-КРЕДИТНОЙ ПОЛИТИКИ НА СРЕДНЕСРОЧНУЮ ПЕРСПЕКТИВУ

В настоящее время, когда в целом удалось обеспечить стабилизацию ситуации в российской экономике после второй волны нефтяных шоков середины 2015 — начала 2016 года и наметились признаки ее адаптации к изменившимся внешним условиям, первостепенной задачей государственной макроэкономической политики становится создание условий и стимулов для поступательного и устойчивого экономического развития России. Сохранение модели экономического роста, основанной на экспорте сырьевых товаров и стимулировании потребления, даст лишь краткосрочный эффект, поскольку ее потенциал во многом исчерпан в предшествующие годы. В настоящее время востребованной является стратегия, направленная на преодоление структурных проблем российской экономики, улучшение качества функционирования социально-экономических институтов, обеспечение макроэкономической, в том числе финансовой и ценовой, стабильности. При этом важно сформировать у всех членов общества, в первую очередь участников экономических отношений, понимание того, что источники экстенсивного роста во многом исчерпаны. Для того чтобы за фазой восстановления экономической активности последовал переход к устойчивому росту экономики и благосостояния населения, необходимы создание внутренних источников развития, стимулов для повышения производительности и эффективности экономической деятельности, улучшение качества управления на всех уровнях как в государственном, так и в частном секторе. На формирование такой долгосрочной стратегии и на создание у всех хозяйствующих субъектов стимулов к интенсивному развитию должны быть направлены скоординированные действия всех ветвей власти, контрольно-регулирующих органов и системы государственного управления в целом.

При выполнении своих законодательно определенных функций и задач Банк России исходит из того, что цели его политики и подходы к ее реализации должны способствовать обеспечению устойчивого экономического развития. В части своей компетенции Банк России формирует ряд необходимых для этого условий, обеспечивая ценовую и финансовую стабильность, предупреждая накопление финансовых дисбалансов и амортизируя воздействие на экономику негативных внешних шоков и процессов. Банк России также принимает меры по развитию национальной платежной системы, конкурентоспособного, устойчивого и заслуживающего доверия финансового рынка, использующего передовые технологии, предоставляющего широкий спектр финансовых услуг населению и бизнесу и в наибольшей степени отвечающего потребностям развития экономики. Комплексность и многофакторность стоящих перед Банком России задач требуют четкости и согласованности действий по всем направлениям его деятельности, тесного взаимодействия с органами законодательной и исполнительной власти. Именно координация мер Правительства Российской Федерации и Банка России сыграли важную роль в преодолении острой фазы кризиса конца 2014 — начала 2015 года и последующей стабилизации ситуации.

При этом успешное выполнение Банком России своих функций формирует далеко не все, а лишь некоторые условия экономического благополучия и само по себе не может стать основным драйвером экономического роста. Будущее экономики в решающей степени будет зависеть от перспектив преодоления структурных ограничений. Структурная, налоговая и бюджетная политика государства должна определять степень, формы и условия его влияния на движение материальных и финансовых ресурсов в экономике, содействовать появлению новых отраслей и отраслевой диверсификации, оптимизации территориального размещения факторов производства, технологическому перевооружению, развитию всех видов экономической и социальной инфраструктуры, повышению конкурентоспособности российских товаров до мирового уровня. От выбора вектора общей макроэкономической политики будут во многом зависеть эффективность принимаемых Банком России мер и их влияние на благосостояние российских граждан.

Денежно-кредитная политика Банка России играет основную роль в формировании таких важных условий экономического развития и социальной стабильности, как низкие темпы инфляции, предсказуемый уровень процентных ставок, защищающий сбережения от инфляционного обесценения и необходимый для планирования инвестиций. Эти условия обеспечиваются прежде всего через сдерживание инфляционных процессов. Денежно-кредитная политика нацелена на постепенное снижение годовой инфляции до 4% и поддержание ее вблизи этого уровня в дальнейшем. При стабильно низкой инфляции предприятия и домашние хозяйства могут более уверенно строить производственные и семейные планы, принимать решения о расходах, сбережениях и инвестициях. Напротив, высокая инфляция, как правило, подвержена сильным колебаниям, увеличивает неопределенность и хозяйственные риски, осложняет расчеты на будущее, сокращает горизонт планиро-

вания, снижая стимулы к сбережениям и инвестициям, усиливает социальную дифференциацию. Высокая и волатильная инфляция, как правило, закладывается в процентные ставки, становясь дополнительным бременем для домашних хозяйств и предприятий. При прочих равных условиях высокая инфляция способствует усилению социального неравенства, росту дифференциации доходов, отражаясь наиболее негативно на благополучии людей со средним и низким уровнем достатка, номинальные доходы которых относительно стабильны. В ходе социологических опросов российские граждане не случайно называют высокую инфляцию одной из самых острых для себя проблем (см. приложение 2). Ценовая стабильность является неотъемлемым элементом благоприятной среды для жизни людей и ведения бизнеса, для устойчивого экономического роста.

Экономика может расти и на фоне относительно высокой инфляции. Но такая инфляция, как правило, нестабильна и таит в себе угрозу дальнейшего ускорения и перехода к быстрому росту цен даже под влиянием временных факторов. В этих условиях возникают риски накопления диспропорций в финансовой сфере, реальном секторе, обострения социальной напряженности, при которых невозможно устойчивое экономическое развитие.

Целевой уровень инфляции 4% выбран с учетом особенностей ценообразования и структуры экономики в нашей стране. Это несколько выше, чем в странах с развитыми рыночными механизмами, многолетним опытом сохранения ценовой стабильности, укрепившимся доверием к денежным властям и низкими инфляционными ожиданиями. В таких странах цель по инфляции обычно устанавливается на уровне от 1 до 3%. Постоянное поддержание инфляции в России вблизи этих значений мерами денежно-кредитной политики сильно затруднено из-за структурных экономических проблем: повышенного уровня монополизации и относительной неразвитости рыночных механизмов, низкой эффективности и недостаточной отраслевой диверсификации экономики. Кроме того, устойчивой стабилизации инфляции на исторически нехарактерном, низком для России уровне на начальном этапе будет также мешать инертность инфляционных ожиданий – укоренившаяся за многие годы привычка населения и бизнеса вести хозяйство в условиях высокой инфляции.

Наряду с указанными факторами выбор в пользу 4% продиктован необходимостью минимизации рисков возникновения дефляционных тенденций на рынках отдельных товаров. В условиях существующей структуры российской экономики изменение цен на различные группы товаров происходит неравномерно, в потребительской корзине довольно высока доля товаров и услуг, цены на которые могут сильно колебаться. Поэтому при общем уровне инфляции существенно ниже 4% возникает риск продолжительного снижения цен, то есть дефляции, на рынках различных групп товаров. Дефляция, охватывающая широкий круг товаров, может повлечь за собой не менее негативные последствия, чем высокая инфляция. Для того чтобы процесс выравнивания относительных цен не приводил к дефляционным явлениям, целевой показатель прироста общего индекса потребительских цен в нашей стране должен устанавливаться с некоторым "запасом". В то же время этот "запас" не должен быть слишком большим, поскольку при более высокой инфляции (например, около 10%), как правило, возрастает амплитуда ее колебаний и становится сложнее обеспечить ее стабильность и предсказуемость в случае реализации различных шоков, чем при инфляции около 4%. Это особенно проявляется, когда значительная доля потребительской корзины приходится на товары, цены которых могут существенно изменяться. В России такой группой товаров является продовольствие, составляющее более трети потребительской корзины. Динамика цен продовольственных товаров сильно зависит от итогов сбора урожая, конъюнктуры мировых товарных рынков. При невысоком целевом уровне инфляции снижается и потенциал роста цен на эту социально значимую группу товаров в случае действия неблагоприятных факторов. Устойчивость, предсказуемость темпов роста потребительских цен имеют не менее важное значение для экономического развития и благополучной жизни людей, чем их абсолютный низкий уровень.

Банк России проводит денежно-кредитную политику в рамках режима таргетирования инфляции, основанного на управлении внутренним спросом. Поэтапный переход к нему начался после кризиса 2008–2009 годов и был завершен в конце 2014 года. При данном подходе основным каналом влияния Центрального банка на денежно-кредитные условия в экономике и в конечном счете на инфляцию становятся процентные ставки. Изменяя ключевую ставку, Банк России воздействует на краткосрочные ставки денежного рынка, а через них – на весь спектр процентных ставок в финансовом секторе экономики по всей длине кривой доходности (от процентных ставок по рыночным облигациям до ставок по депозитам и кредитам банков). Повышение процентных ставок при прочих равных условиях стимулирует сбережения, ослабляет кредитную активность, ограничивая спрос на товары и услуги и сдерживая инфляционное давление. Снижение процентных ставок действует в обратном направлении: оказывает стимулирующее влияние на внутренний спрос, создавая мотивацию к сокращению сбережений и повышая доступность кредита. Таким образом, воздействуя

через процентные ставки на спрос на товары и услуги, Центральный банк оказывает влияние на темпы роста цен в экономике. Повышение или снижение процентных ставок также отражается на динамике курса национальной валюты, который может изменяться и под воздействием других факторов, оказывая влияние в первую очередь на цены импортных товаров и через них на инфляцию в целом. Косвенный эффект динамики валютного курса связан с изменением ценовой привлекательности отечественной продукции относительно импортной, которое приводит к изменению спроса и цен на эти группы товаров. Чувствительность инфляции к изменениям валютного курса зависит не только от доли импорта в потребительской корзине, но и от характера инфляционных ожиданий, а также доверия общества к проводимой денежно-кредитной политике. Если Центральный банк последовательно обеспечивает ценовую стабильность, то укрепляется уверенность домашних хозяйств и бизнеса в сохранении низкой инфляции. Участники экономических отношений становятся менее чувствительными к действию проинфляционных факторов, а также курсовой динамике. В обществе формируется уверенность, что Центральный банк не допустит существенных колебаний потребительских цен или их продолжительного и устойчивого роста. В такой ситуации инфляционные ожидания остаются стабильно низкими и при этом чутко реагируют не только на действия, но и заявления Центрального банка. В этих условиях большое значение приобретают информационная открытость Центрального банка, разъяснение им широкой общественности целей и ожидаемых результатов денежно-кредитной политики, публикация оценок текущей ситуации и прогноза. Это позволяет повысить прозрачность и предсказуемость проводимой политики, тем самым снижая степень экономической неопределенности, и вносит вклад в укрепление доверия к Центральному банку.

Стратегия таргетирования инфляции в наибольшей степени подходит для России на современном этапе, особенно в условиях неблагоприятной и изменчивой конъюнктуры мировых рынков, ограниченного доступа российской экономики к внешнему финансированию. В рамках данного подхода Центральный банк нацелен на обеспечение внутренней экономической стабильности, в первую очередь стабильности цен и предсказуемости изменения процентных ставок. Такая модель денежно-кредитной политики в наибольшей степени соответствует задаче создания благоприятных внутренних условий для развития экономики. Применяемый с конца 2014 года режим плавающего валютного курса не только позволяет сохранить валютные резервы, но и формирует стимулы к правильной реакции всех участников экономических отношений на изменение внешних условий, обеспечивая оптимальную подстройку к ним экономики. Таким образом, плавающий валютный курс защищает экономическую систему от накопления дисбалансов, в том числе избыточного наращивания внешнего долга, и делает ее более устойчивой в долгосрочном плане к колебаниям внешнеэкономической конъюнктуры. Попытки регулирования валютного курса в условиях внешних шоков, напротив, заканчивались финансовыми и экономическими кризисами, что подтверждает опыт России и других стран. Значительные изменения валютного курса в ответ на динамику мировых товарных рынков связаны с сильной сырьевой ориентацией экономики и, безусловно, негативно влияют как на реальный сектор, так и на инфляцию. Однако эти курсовые колебания не связаны непосредственно с использованием режима таргетирования инфляции, а вызваны резким ухудшением внешних условий для российской экономики при ее сохраняющихся структурных проблемах. Вследствие колебаний цен на мировых товарных рынках резкие и болезненные перепады испытывают не только валютный курс и цены, но и темпы экономического роста, уровень жизни населения в сырьевой, слабо диверсифицированной экономике. Долговременная стабилизация валютного курса, снижение его реакции на изменения внешних условий, при которых он будет подвержен лишь небольшим колебаниям, а также уменьшение влияния валютного курса на инфляцию, настроения и ожидания населения и бизнеса, состояние экономики в целом станут по-настоящему возможны только после преодоления ее сырьевой зависимости.

Воздействуя через процентные ставки на спрос и инфляцию, Центральный банк неизбежно влияет и на экономическую активность. Эффективность влияния денежно-кредитной политики на инфляцию, а также степень, в которой меры по снижению инфляции будут отражаться на деловой активности, зависят от того, насколько чувствительна реакция экономической системы на изменение ключевой ставки Центрального банка, то есть от того, насколько хорошо работает трансмиссионный механизм денежно-кредитной политики. Это определяется множеством разнообразных факторов на уровне как финансового, так и реального сектора, а также особенностями макроэкономической политики в целом.

Четкость передачи сигнала от ключевой ставки к финансовой сфере и его влияние на деятельность предприятий и домашних хозяйств во многом зависят от роли финансового сектора в движении денежных ресурсов в экономике, в формировании сбережений и кредита. При этом важным условием является доверие населения и бизнеса к финансовым посредникам. Большое значение имеют также

технологии и сложившиеся практики осуществления платежей и расчетов в экономике. В России сохраняется большой потенциал для качественного изменения и усиления роли финансовых институтов в обслуживании экономической деятельности. Последовательная политика Банка России в сфере надзора, регулирования и развития всех сегментов финансовой системы, нацеленная на укрепление финансовых институтов, будет создавать условия для сбалансированного развития финансовой системы. Это также улучшает условия реализации денежно-кредитной политики, увеличивая эффективность трансмиссионного механизма. Повышение качества финансового посредничества окажет позитивное влияние на доступность услуг организациям, которые способны выступать надежными заемщиками и эмитентами ценных бумаг в целях осуществления инвестиционной деятельности. Развитие широкого спектра инструментов с различным соотношением риска и доходности будет повышать инвестиционную привлекательность российского финансового рынка и его институтов.

Эффективность влияния Центрального банка на динамику потребительских цен, как отмечено выше, в значительной мере зависит и от характера инфляционных ожиданий, уровень которых в России пока довольно высок (при заметной тенденции к их снижению). Более чем за два десятилетия, в которые Россия пережила не один экономический кризис, домашние хозяйства и бизнес привыкли к тому, что цены могут заметно и непредсказуемо расти, и закладывают это на будущее. Но такая ситуация, сложившаяся в России, не уникальна: многие страны, имевшие высокую и нестабильную инфляцию, столкнулись с этой проблемой и постепенно решили ее. Последовательная политика Банка России, направленная на замедление инфляции, со временем стабилизирует инфляционные ожидания на низком уровне, существенно облегчая задачу поддержания ее около целевого уровня в дальнейшем.

Действенность мер денежно-кредитной политики Банка России определяется и структурными особенностями российской экономики. Динамика цен зависит не только от изменений платежеспособного спроса, на регулирование которого в основном ориентирована денежно-кредитная политика, но и факторами на стороне товарного предложения. Можно выделить целый ряд причин структурного характера, которые тормозят расширение и снижают гибкость товарного предложения, а также уменьшают чувствительность производства и потребления к изменению уровня цен. Это существенно усложняет задачу регулирования инфляции мерами денежно-кредитной политики, а также препятствует экономическому росту. В числе таких факторов – высокая степень монополизации во многих отраслях экономики. При низкой конкуренции естественные монополии, другие крупные предприятия и торговые посредники не имеют достаточных стимулов к повышению операционной эффективности и снижению издержек производства, перекладывая их в значительной мере на плечи потребителя. В таких условиях отсутствует гибкая реакция со стороны производителей на изменение спроса, в том числе и под влиянием мер денежно-кредитной политики. Кроме того, возможности компаний наращивать производство в ответ на увеличение платежеспособного спроса ограничены накопившимися диспропорциями, которые затрудняют увеличение экономического потенциала. Эти диспропорции в том числе связаны с сильным физическим и моральным износом парка машин и оборудования, низким уровнем внедрения передовых технологий, недостаточной развитостью транспортной и логистической инфраструктуры.

Другим фактором, который может привести к ограничению возможностей Центрального банка влиять на цены через платежеспособный спрос, является высокий уровень социального неравенства, который выражается в неравномерном распределении доходов и богатства в обществе. Резкая дифференциация доходов и сбережений может быть причиной слабой ценовой эластичности спроса. С одной стороны, семьи с низкими доходами, в основном покупающие товары первой необходимости, не могут в ответ на рост цен сокращать потребление большинства товаров ниже минимально необходимого для жизни уровня. Как правило, такие семьи не имеют сбережений, а их возможности получения кредита сильно ограниченны. Расходы этих домашних хозяйств на потребление почти не реагируют на изменения процентных ставок в экономике. С другой стороны, состоятельные домашние хозяйства тратят небольшую долю своих высоких доходов на покупку основных товаров потребительской корзины, поэтому изменения цен большинства товаров существенно не влияют на объемы их потребления. Семьи со средним уровнем дохода наиболее чутко реагируют на изменение процентных ставок и потребительских цен, что, в свою очередь, стимулирует производителей подстраиваться под изменения их спроса. Неравномерность распределения сбережений при прочих равных условиях препятствует их трансформации в инвестиции и негативно влияет на экономический рост. Значительная часть российского населения имеет небольшие сбережения, а наиболее состоятельные семьи в современных реалиях склонны к формам накопления, не способствующим экономическому развитию страны (в основном в виде вкладов в зарубежных банках, приобретения дорогой недвижимости за границей и импортных предметов роскоши). Экономическая политика, способствующая более равномерному

распределению доходов в обществе, будет формировать условия не только для сбалансированного развития и социальной стабильности, но и для усиления действенности сигналов денежно-кредитной политики, которые в зависимости от обстоятельств направлены на повышение склонности людей к потреблению или сбережению.

Структурные проблемы и особенности российской экономики не делают замедление инфляции в России невозможным, но они снижают действенность мер денежно-кредитной политики, увеличивая риски недостижения целевого показателя по инфляции или его достижения неприемлемой ценой «переохлаждения» экономики, снижения потенциала ее роста. Процесс замедления инфляции становится более болезненным и сложным, а Центральный банк для достижения цели по инфляции при прочих равных условиях вынужден проводить более жесткую денежно-кредитную политику, чем это было бы необходимо в отсутствие структурных ограничений. С учетом указанных факторов Банк России следует стратегии постепенного замедления инфляции до 4% в течение нескольких лет, выбирая скорость ее снижения с учетом экономических условий. В частности, при резком изменении внешнеэкономической ситуации в 2014 году, которое негативно отразилось на российской экономике, горизонт достижения целевого уровня инфляции был расширен с 2016 года до конца 2017 года.

Учитывая, что решения по ключевой ставке оказывают влияние на экономическую систему в целом, Банк России наряду с инфляционными рисками в равной степени оценивает и учитывает возможные последствия принятых решений для реального и финансового секторов экономики, чтобы своими действиями не создавать угроз для финансовой стабильности и не спровоцировать ухудшение экономической ситуации. Принимая меры и просчитывая их ожидаемые последствия, Банк России придерживается взвешенного подхода, придавая большое значение сбалансированности своих решений. Это обеспечивается в том числе через разработку макроэкономического прогноза на три года вперед, в рамках которого проводится всесторонний анализ факторов и перспектив экономического развития с учетом последних тенденций, заявленных мер макроэкономической политики и потенциальных источников рисков. Банк России принимает решения, опираясь в первую очередь на долговременные устойчивые экономические тенденции, в меньшей степени реагируя на проявления краткосрочных факторов, которые могут оказать лишь временное влияние на инфляцию и экономическую динамику. Это позволяет избежать неоправданно частых изменений ключевой ставки, обеспечивая стабильность процентных ставок в экономике, и достичь с помощью проводимой политики более сбалансированного в среднесрочном плане результата.

В то же время эффективность денежно-кредитной политики, как и макроэкономической политики в целом, в решающей степени зависит от согласованности действий всех органов государственного управления. Банк России учитывает особенности проведения денежно-кредитной политики в условиях существующих структурных проблем и координирует свои действия с усилиями Правительства Российской Федерации по преодолению структурных ограничений в экономике. Координация денежно-кредитной и бюджетной политики важна и в вопросах формирования суверенных фондов, которые позволяют сгладить воздействие изменений конъюнктуры мировых товарных рынков на экономику, в том числе на реальный валютный курс и конкурентоспособность российских товаров и услуг. Пополнение и расходование суверенных фондов в рамках бюджетного правила, возможность применения которого рассматривается уже с 2017 года[1], обеспечит устойчивость государственных финансов и предсказуемость макроэкономической политики в целом.

Учитывая многоплановость решаемых Банком России задач, большое значение приобретают выверенность и взаимная согласованность мер, принимаемых по различным направлениям его деятельности, а также учет их влияния на условия реализации денежно-кредитной политики и макроэкономической политики в целом. При этом важно комплексное применение инструментов, имеющихся в распоряжении Центрального банка. В частности, ключевая ставка имеет широкий спектр влияния и не может быть инструментом точечного воздействия. Банк России имеет в своем арсенале инструменты макропруденциального регулирования для предупреждения возникновения финансовых дисбалансов, перегрева отдельных сегментов финансового рынка, которые могут угрожать ценовой стабильности и негативно повлиять на экономическую ситуацию.

В текущих условиях, при накопившихся структурных дисбалансах и негативном воздействии внешних факторов денежно-кредитная политика, по сути, выполняет функцию стабилизатора экономики. При объективной невозможности в силу характера решаемых задач стать основным двигателем экономического развития Банк России наряду с замедлением инфляции сосредоточивает свои усилия на поддержании стабильности внутренних

[1] Подход к применению бюджетного правила представлен в проекте «Основных направлений бюджетной политики на 2017 год и на плановый период 2018–2019 годов». Применение бюджетного правила планируется начать с 2020 года. В 2017–2019 годах предполагается использование переходных положений бюджетного правила.

финансовых условий, создании стимулов к формированию сбережений и снижению долговой нагрузки, уровень которой в отдельных секторах экономики весьма высок (с точки зрения отношения платежей по обслуживанию долга к получаемым доходам). Решение этих задач вместе со снижением инфляции требует от Центрального банка проведения умеренно жесткой денежно-кредитной политики для формирования номинальных процентных ставок на уровне, обеспечивающем положительные реальные ставки процента. На среднесрочном горизонте такой подход сохранится, делая возможным постепенное снижение инфляции, а также номинальных ставок процента при сохранении в положительной области реальных ставок процента. Это делает банковские депозиты и иные рублевые сберегательные продукты привлекательными для населения, защищая их от инфляционного обесценения и поддерживая склонность к сбережениям. В этих условиях кредитные ставки также формируются на уровнях, превышающих инфляцию, стимулируя производителей и торговых посредников повышать операционную эффективность и предупреждая избыточное накопление долговой нагрузки, что способствует повышению устойчивости балансов реального и финансового секторов. Стабильность процентных ставок, защищающих сбережения от инфляции, и их предсказуемое постепенное снижение по мере замедления темпов роста потребительских цен представляются существенным фактором стабилизации экономики, одним из условий ее перехода к фазе устойчивого роста.

Альтернативные подходы к проведению денежно-кредитной политики, в основном предполагающие ее резкое смягчение через ускоренное снижение процентных ставок и увеличение объемов банковского кредитования, в текущих условиях могут создать системные риски для экономической стабильности и социального благополучия. Безусловно, в настоящее время важным вектором государственной экономической политики должно стать создание условий и стимулов для инвестиций, технологического перевооружения промышленности для направления имеющихся в экономике ресурсов в приоритетные отрасли и проекты, которые могут стать катализатором экономического роста. Однако за попыткой решения данной задачи посредством масштабного расширения денежной эмиссии последует существенное ускорение инфляции при одновременном снижении реальных процентных ставок с их переходом в отрицательную область. Это приведет к инфляционному обесценению сбережений и доходов основной массы населения. По существу, предлагается метод стимулирования промышленности за счет инфляционного налога, снижающего благополучие большинства домашних хозяйств, особенно социально незащищенных слоев населения. Такой подход создает очевидные угрозы для социальной и экономической стабильности, но при этом не решает поставленную задачу как минимум по двум причинам. Во-первых, усиление роли государства в выборе направлений кредитования потребовало бы подготовительных мер по перестройке государственных институтов как на уровне национальной экономики, так и на уровне отдельных отраслей. Произвольное, вне системы эффективного государственного управления, удовлетворение заявок на получение дешевых кредитов не обеспечит поступательного экономического развития. Во-вторых, банковский кредит не является основным источником инвестиций для большинства организаций. В предыдущие годы многие российские предприятия накопили высокий уровень задолженности, и в текущих условиях, напротив, необходимо снижение долговой нагрузки, которая для некоторых отраслей корпоративного сектора уже находится на уровне, близком к максимальным значениям для стран с формирующимися рынками. Дальнейшее ее повышение даже под низкий процент приведет к накоплению системных рисков, что идет вразрез с задачей повышения устойчивости экономики.

Необходимы иные решения, позволяющие активизировать роль государства в стимулировании экономического развития, но не приводящие к ускорению инфляции и накоплению дисбалансов, а также не создающие угроз для социальной стабильности. Финансирование приоритетных для экономического развития проектов и программ может осуществляться прежде всего через привлечение капитала на принципах государственно-частного партнерства, а также через использование иных рыночных, налоговых, бюджетных и регуляторных механизмов и мотиваций в целях перераспределения уже созданных денежных накоплений между предприятиями, отраслями и сегментами экономики без существенного увеличения банковского кредитования и долговой нагрузки. Динамика банковского кредитования и соответствующее увеличение денежной массы представляют собой производную от потребностей экономики, формируемых наличием материальных, людских, управленческих ресурсов для увеличения производства товаров и услуг. Применение любых методов льготного снижения процентной ставки по банковским кредитам ниже рыночного уровня (помимо бюджетных субсидий) для создания более мягких условий кредитования отдельных проектов и программ должно быть ограниченным. При прочих равных условиях это приводит к удорожанию стоимости кредитов для экономики в целом за счет ухудшения условий кредитования отраслей, не получающих государственных льгот. Это основная причина, по которой Банк России ограничивает объемы предо-

ставления средств в рамках своих специализированных инструментов рефинансирования.

Как показывает мировой опыт, существуют различные примеры распределения ролей между государственными институтами при проведении политики стимулирования экономического развития. Наиболее успешным зарекомендовал себя подход, при котором Центральный банк и Министерство финансов отвечают за ценовую и финансовую стабильность на макроуровне, а другие государственные институты создают условия и стимулы к перераспределению финансовых потоков между отраслями, секторами и сегментами экономики (при соблюдении общего ограничения по ресурсам) в рамках согласованной системы государственного стратегического и оперативного управления. Основные цели и принципы денежно-кредитной политики, которая является неотъемлемым элементом общей государственной экономической политики, достаточно универсальны для любой модели экономики. Ценовая и финансовая стабильность при любых формах взаимодействия государства с бизнесом способствует экономическому и социальному благополучию. Последовательная денежно-кредитная политика, нацеленная на сохранение внутренней экономической стабильности, снижает неопределенность, создает для всех участников экономических отношений четкие ориентиры, понятные «правила игры», что важно как для ведения текущей деятельности, так и для составления планов на будущее всеми участниками экономических отношений.

4. СЦЕНАРИИ МАКРОЭКОНОМИЧЕСКОГО РАЗВИТИЯ И ДЕНЕЖНО-КРЕДИТНАЯ ПОЛИТИКА В 2017–2019 ГОДАХ

Банк России принимает решения в области денежно-кредитной политики на основе оценки текущей экономической ситуации и среднесрочного макроэкономического прогноза. Прогноз охватывает трехлетний период, что одновременно позволяет учитывать лаги влияния денежно-кредитной политики на экономику и дает субъектам экономики ориентиры для принятия решений на среднесрочном горизонте планирования. При этом Банк России рассматривает наиболее вероятный (базовый) сценарий развития экономики, а также анализирует альтернативные варианты изменения ситуации, внешние и внутренние риски, реализация которых может оказать влияние на финансовую систему и экономику в целом и, соответственно, на условия проведения денежно-кредитной политики. Рассмотрение совокупности вариантов позволяет Банку России принимать решения сбалансированно и проводить политику таким образом, чтобы быть готовым обеспечить сохранение ценовой и финансовой стабильности при реализации рисковых сценариев.

В целом, как ожидается, в рамках трехлетнего прогнозного периода условия развития российской экономики останутся непростыми. С учетом этого крайне важное значение будет иметь сохранение последовательной и согласованной макроэкономической политики, направленной на обеспечение экономической стабильности и формирование условий для устойчивого роста. Политика Банка России, со своей стороны, будет способствовать этому за счет достижения ценовой стабильности (подразумевающей снижение инфляции до целевого уровня 4%) и финансовой стабильности, а также обеспечения устойчивости банковского сектора и развития финансовой системы в целом.

Макроэкономические прогнозы Банка России формируются с учетом того, что на развитие ситуации в российской экономике может воздействовать ряд факторов, находящихся вне прямого влияния денежно-кредитной политики. К их числу относятся внешние (такие, как темпы роста глобальной экономики, конъюнктура международных финансовых и товарных рынков) и внутренние условия (параметры государственной политики, структурные характеристики экономики). Данные факторы Банк России прогнозирует на сценарной основе и при формировании прогноза учитывает в качестве предпосылок.

Внутренние факторы, существенно влияющие на экономическую ситуацию, но находящиеся вне воздействия денежно-кредитной политики, в сценариях Банка России предполагаются достаточно однородными. Предпосылки о таких внутренних условиях Банк России формирует исходя из принятых на текущий момент решений и анонсированных планов в области государственной политики. Для сохранения разумной консервативности прогноза Банк России не вносит дополнительных предположений о еще не зафиксированных в официальных документах мерах, последствия реализации которых в отсутствие четко определенных параметров трудно оценить.

Во-первых, важным фактором формирования внутренних экономических условий будет являться реализация бюджетной политики. Банк России предполагает, что на прогнозном горизонте сохранится сформированный к настоящему времени Пра-

вительством Российской Федерации и Минфином России консервативный подход к планированию бюджета[2]. С одной стороны, в условиях превышения расходов бюджета над доходами на трехлетнем горизонте сохранится потребность в расходовании значительной доли средств Резервного фонда, а также, возможно, части средств Фонда национального благосостояния. С другой стороны, за счет планируемых ограничений на рост бюджетных расходов будет достигаться последовательное сокращение дефицита бюджета для достижения его сбалансированности к 2020 году, когда планируется в полной мере начать применение модифицированного бюджетного правила[3]. В 2017–2019 годах предполагается использование его переходных положений. Такой подход обеспечит сохранение безопасного с точки зрения финансовой стабильности уровня государственного долга и поддержание устойчивости государственных финансов в средне- и долгосрочной перспективе. Применение бюджетного правила также снизит уязвимость российской экономики к изменениям внешнеэкономической конъюнктуры, ограничивая колебания реального валютного курса и, следовательно, его влияние на конкурентоспособность российских производителей.

С учетом сдержанной динамики бюджетных расходов, необходимой для сокращения дефицита, стимулирующее влияние бюджетной политики на экономику в этот период будет ограниченным. Вклад потребления государственного сектора в динамику ВВП будет близким к нулю или слабо отрицательным. В этих условиях важную роль сыграют меры по оптимизации структуры бюджетных расходов, а также дополнительные меры государственной политики, направленные на повышение долгосрочного потенциала устойчивого экономического роста.

На трехлетнем горизонте потоки средств, связанные с финансированием бюджета из средств суверенных фондов, будут оказывать воздействие на формирование ликвидности банковского сектора. Вместе с тем их итоговое влияние на кредитные условия в экономике, по оценкам Банка России, будет весьма ограниченным, в первую очередь в силу эффективного использования системы инструментов Банка России для достижения операционной цели денежно-кредитной политики – поддержания краткосрочных ставок денежного рынка вблизи ключевой ставки (см. раздел 3).

Во-вторых, значимой предпосылкой для среднесрочного прогноза инфляции также является предположение об умеренных темпах повышения административно регулируемых цен и тарифов в соответствии с планами, сформированными к настоящему времени Правительством Российской Федерации. Сохранение подхода к индексации тарифов, подразумевающего их увеличение темпами не выше уровня инфляции, будет важным условием отсутствия дополнительного инфляционного давления со стороны этого фактора на прогнозном горизонте.

В-третьих, Банк России исходит из предположения о сохранении в прогнозный период действия структурных ограничений для роста экономики, связанных с демографической ситуацией, а также инфраструктурными и институциональными характеристиками экономики. Действие указанных ограничений проявляется в сохранении несбалансированной структуры российской экономики, ее недостаточной диверсификации и преобладающей сырьевой направленности. Структура экспорта России остается смещенной в пользу товаров нефтегазовой отрасли и других продуктов добывающего сектора, тогда как доля отечественной продукции с более высокой степенью переработки, поставляемой на внешние рынки, остается небольшой. Это увеличивает чувствительность экономики к изменению внешних условий, в частности к изменению цен на нефть, а также влияет на формирование доходов и цен. Недостаточная развитость отдельных сегментов производства инвестиционных и потребительских товаров определяет низкий уровень конкуренции как на внутреннем уровне, так и с импортными аналогами. В свою очередь, это может увеличивать волатильность цен, затруднять снижение инфляции в целом и при прочих равных условиях требовать усиления реакции со стороны денежно-кредитной политики для уменьшения инфляционных рисков.

Другой особенностью экономической системы, которая также может осложнить замедление инфляции мерами денежно-кредитной политики, является степень неравенства доходов. По-прежнему высока доля домохозяйств с низкими доходами, структура потребления которых смещена в пользу товаров первой необходимости. Чувствительность спроса на такие товары к изменению цен может быть более низкой, чем по другим товарам, что может сокращать стимулы к ценовой конкуренции среди производителей и поставщиков отдельных товаров этой категории. Кроме того, при относительно низком уровне доходов в составе потребительской корзины остается повышенной доля продовольствия, цены на которое отличаются высокой волатильностью и чувствительностью к действию разовых факторов со стороны предложения (например, зависимость от сельскохозяйственного урожая).

[2] При разработке прогноза Банк России учитывает проектировки бюджета, представленные в проекте «Основных направлений бюджетной политики на 2017 год и на плановый период 2018–2019 годов».

[3] Подход к применению бюджетного правила представлен в проекте «Основных направлений бюджетной политики на 2017 год и на плановый период 2018–2019 годов».

Для преодоления отмеченных ограничений, как показывает опыт России и других стран, как правило, требуется достаточно длительный период, превышающий прогнозный трехлетний горизонт. Вместе с тем по мере развития ситуации и появления большей определенности относительно возможностей повышения потенциала роста российской экономики, в том числе за счет реализации мер государственной политики, Банк России будет уточнять свои среднесрочные прогнозы и набор сценариев. По мере разработки и законодательного утверждения конкретных мер государственной политики, направленных на преодоление структурных проблем и смену модели экономического развития, станет возможной подготовка Банком России соответствующего сценария с расчетом всех его параметров. Банк России учитывает, что при смягчении структурных ограничений российской экономики может происходить ускорение ее роста, определяемое факторами со стороны предложения и не сопровождающееся усилением инфляционного давления со стороны спроса, а также ростом рисков в финансовой сфере. В таком случае повышение темпов роста внутреннего спроса (относительно прогнозов в соответствующих сценариях) не потребует дополнительного изменения ключевой ставки, так как этот рост будет сопровождаться повышением производительности труда и увеличением эффективности производства.

В части внутренних финансовых условий во всех сценариях предполагается, что они будут оставаться умеренно жесткими достаточно длительное время и потенциал снижения номинальных процентных ставок в экономике будет ограничен с учетом проводимой Банком России денежно-кредитной политики. Затем, по мере закрепления инфляции вблизи 4%, денежно-кредитные условия будут постепенно смягчаться, поддерживая восстановление роста экономической активности. Сохранение умеренной жесткости денежно-кредитных условий в экономике в первой части прогнозного периода будет определяться двумя основными факторами. С одной стороны, денежно-кредитная политика Банка России будет поддерживать положительные реальные процентные ставки. На среднесрочном горизонте их равновесный уровень для экономики оценивается в 2,5–3%, в переходный период для снижения инфляционных ожиданий и инфляции они должны быть несколько выше. Это будет формировать условия для сохранения привлекательности рублевых сбережений и умеренной склонности к заимствованию внутри экономики, что, в свою очередь, будет отражаться на динамике цен как через сдержанную динамику внутреннего потребительского спроса, так и через формирование трансграничных потоков капитала и, соответственно, валютного курса.

С другой стороны, одним из результатов реализации ряда внешних рисков и замедления экономического роста в предыдущие периоды являлось повышение уровня долговой нагрузки в экономике. В текущих условиях обслуживание задолженности по кредитам, сформированной в период более быстрого экономического роста, остается источником рисков для финансовой устойчивости многих заемщиков, прежде всего корпоративного сектора. Как ожидается, это обстоятельство будет являться дополнительным фактором, ограничивающим возможности смягчения кредитных условий в первой половине трехлетнего прогнозного периода, определяя более консервативное поведение как банков-кредиторов (в части формирования ценовых и неценовых условий кредитования), так и самих заемщиков. Корректировка отдельными категориями заемщиков долговой нагрузки для приведения ее в соответствие с объективно изменившимися условиями формирования их доходов будет в том числе поддерживаться осуществлением умеренно жесткой денежно-кредитной политики. Этот процесс является необходимым условием сохранения стабильности финансового сектора и запуска устойчивого роста экономики в дальнейшем.

Меры Банка России, направленные на развитие и повышение эффективности банковского сектора, финансовых рынков, оптимизацию подходов к их регулированию, повышение доступности и степени проникновения финансовых услуг, уровня финансовой грамотности населения и бизнеса, будут способствовать сбалансированному развитию финансовой системы в целом и улучшению условий реализации денежно-кредитной политики, повышая действенность транс-миссионного механизма[4].

Для поддержки отдельных сегментов кредитования, развитие которых важно для изменения структуры экономики, но затруднено в рыночных условиях, Банк России продолжит использовать специализированные инструменты рефинансирования. Как и прежде, чтобы избежать необоснованного смягчения денежно-кредитных условий, объем предоставления средств в рамках данных механизмов будет ограничен, а круг кредитов, принимаемых в обеспечение, строго определен. При этом, учитывая прогнозируемое наличие избытка ликвидности в банковском секторе в целом в предстоящий период и ожидаемое снижение рыночных процентных ставок по мере замедления инфляции, спрос кредитных организаций на специализированные инструменты рефинансирования может снизиться.

В части внешних условий в прогнозах учитываются следующие предпосылки. На трехлетнем

[4] Вопрос о влиянии развития финансового рынка на трансмиссионный механизм денежно-кредитной политики более подробно раскрывается в разделе 1.

прогнозном горизонте ожидается продолжение медленного роста глобальной экономики при сохранении неоднородности тенденций по странам с развитыми и формирующимися рынками. Предполагается, что структура внешнеторговых отношений России в этот период по-прежнему будет относительно стабильной. Годовые темпы роста ВВП стран – торговых партнеров в течение прогнозного периода останутся на уровне 2015–2016 годов, составляя около 2%. В такой ситуации спрос на мировых товарных рынках будет по-прежнему сдержанным. Сохранение относительно высокого уровня предложения и запасов сырья (с учетом технологических изменений и действия отдельных геополитических факторов) будет ограничивать рост товарных цен. При этом под действием, в частности, краткосрочных факторов со стороны предложения может сохраняться повышенная волатильность цен на энергоносители.

В условиях сдержанного глобального спроса и ожидаемой динамики цен на сырье и мировых продовольственных цен внешнее инфляционное давление в целом останется ограниченным. На этом фоне денежно-кредитная политика большинства мировых центральных банков в ближайшее время будет иметь преимущественно стимулирующий характер, а затем начнется ее постепенная нормализация. Это будет способствовать достаточно продолжительному сохранению относительно низкого уровня процентных ставок на мировых финансовых рынках. На среднесрочном горизонте ожидается постепенное повышение ставок центральными банками развитых стран (прежде всего ФРС США), которое будет проводиться с учетом темпов восстановления их экономик.

Несмотря на сохранение относительно благоприятных внешних финансовых условий, возможности привлечения средств на мировых рынках для российских заемщиков будут по-прежнему ограничены действием международных финансовых санкций в отношении России, сохранение которых на всем прогнозном горизонте учитывается в сценариях. Вместе с тем сдерживающий эффект этих ограничений продолжит ослабевать, в том числе за счет диверсификации источников привлечения финансовых средств с международных рынков, включая не затронутые санкциями источники. При этом в условиях стабилизации цен на нефть и отсутствия значительных изменений в тенденциях развития глобальной экономики предполагается сохранение премии за страновой риск на Россию на уровне, близком к показателям 2016 года. В совокупности внешние финансовые и торговые условия для России на прогнозном горизонте останутся фактором, сдерживающим экономическое развитие.

Следует отметить, что свободное курсообразование – по-прежнему важный фактор приспособления российской экономики к влиянию внешних условий. Гибкая реакция валютного курса рубля при изменении внешней конъюнктуры будет обеспечивать подстройку платежного баланса России и увеличивать устойчивость производства и занятости. Так, в случае неблагоприятного изменения внешних условий ослабление рубля будет создавать естественные стимулы к сокращению импорта, одновременно поддерживая конкурентоспособность внутреннего производства. При этом произошедшая адаптация субъектов экономики к эпизодам повышения волатильности валютного курса существенно ограничивает риски для финансовой и ценовой стабильности со стороны курсовой динамики.

Учитывая, что изменение цен на нефть на прогнозном горизонте будет оставаться важным фактором, влияющим на российскую экономику (в части формирования платежного баланса России, курса национальной валюты и привлекательности российской экономики для внешних инвесторов), и при этом их динамика, как отмечено выше, может остаться волатильной и труднопредсказуемой, Банк России рассматривает несколько сценариев ее изменения. **Сценарий I** (**базовый сценарий**), который рассматривается как наиболее вероятный, основан на предположениях о том, что заметного изменения конъюнктуры мировых сырьевых рынков не произойдет и цена на нефть марки «Юралс» на всем прогнозном горизонте будет находиться вблизи средних значений 2016 года – около 40 долл. США за баррель в условиях сохранения высокого уровня предложения на рынке энергоносителей, совершенствования технологий добычи нефти, а также низких темпов роста мировой экономики. Достигнутые в сентябре 2016 года договоренности стран – членов ОПЕК о снижении добычи нефти окажут лишь временную поддержку ценам, учитывая возможное ответное расширение добычи сланцевой нефти. Базовый сценарий Банка России по своим основным параметрам близок к базовому прогнозу Министерства экономического развития России. В дополнение к базовому сценарию Банк России рассматривает **сценарий II** и **сценарий III**, предполагающие, соответственно, более медленное и более быстрое восстановление роста мировой экономики, что приведет к формированию более низкой или более высокой траектории цен на нефть.

В **базовом сценарии** (**сценарий I**) ожидается, что, несмотря на действие указанных выше сдерживающих внешних и внутренних факторов, сохранение стабильности в финансовой сфере, предсказуемость и последовательность денежно-кредитной и бюджетной политики и адаптация субъектов экономики к изменению внешних условий, в том числе за счет свободного курсообразования, создаст условия для постепенного улучшения настроений,

оживления потребительского и инвестиционного спроса и восстановления экономического роста. Вместе с тем потенциальные темпы роста российской экономики будут невысокими с учетом имеющихся структурных ограничений, обозначенных ранее. Как ожидается, в базовом сценарии темп роста экономики составит около 0,5–1,0% в 2017 году, а затем повысится до 1,5–2,0% в 2018–2019 годах.

Ожидаемое замедление инфляции до 4% в 2017 году и ее стабилизация вблизи целевого уровня создадут во второй половине трехлетнего прогнозного периода условия для постепенного смягчения денежно-кредитной политики. На его фоне будет происходить снижение кратко- и долгосрочных рыночных процентных ставок как в номинальном, так и в реальном выражении. Вместе с тем уровень реальных процентных ставок останется в положительной области, что с учетом текущих характеристик развития экономики необходимо для сохранения сбалансированной сберегательной и кредитной активности. Дополнительным фактором смягчения ценовых и неценовых условий кредитования станет ожидаемая нормализация долговой нагрузки и соответствующее последовательное снижение кредитных рисков, что будет обеспечиваться консервативным подходом к изменению соотношения кредитной задолженности и доходов заемщиков. В базовом сценарии прогнозируется, что годовой темп прироста кредита экономике со стороны банковского сектора составит 4–6% в 2017 году, а затем ускорится до 7–11% в 2018–2019 годах. Смягчение кредитных условий наряду с улучшением экономических настроений и ожиданий внесет вклад в постепенное восстановление роста как потребительского, так и инвестиционного спроса.

В разрезе компонентов совокупного спроса прогнозируется, что восстановление экономики будет происходить постепенно и относительно равномерно, что приведет к сохранению относительно стабильной структуры ВВП. Ожидается, что годовые темпы прироста расходов на конечное потребление составят 0,2–0,6% в 2017 году, 1,7–2,5% – в 2018–2019 годах. По мере укрепления уверенности производителей в восстановлении спроса, а также на фоне постепенного смягчения финансовых условий будет осуществляться оживление инвестиционной активности. Годовые темпы прироста валового накопления основного капитала в 2017 году составят 1,2–1,7%, а в 2018–2019 годах увеличатся до 2,7–3,2 и 3,2–3,7% соответственно. Вместе с тем после восстановительного роста инвестиционного спроса, компенсирующего его глубокое падение в предыдущие периоды, темп роста инвестиций, сдерживаемый особенностями экономики, может вновь замедлиться. Динамика запасов в условиях ожидаемого постепенного восстановления потребительского спроса будет вносить дополнительный вклад в прирост валового накопления в 2017–2018 годах.

Постепенное оживление потребительского и инвестиционного спроса при ожидаемой стабильности курсовой динамики будет сопровождаться восстановительным ростом импорта. В то же время с учетом предполагаемых показателей роста стран – торговых партнеров России, а также действующих объективных ограничений для наращивания сырьевого экспорта, имеющего большой вес в структуре экспорта России, годовые темпы роста экспорта в реальном выражении останутся устойчивыми, но невысокими – 1–2%.

При указанной динамике физических объемов экспорта и импорта товаров и услуг, а также с учетом стабилизации цен на энергоносители положительное сальдо текущего счета платежного баланса в течение прогнозного периода будет постепенно сокращаться. Вместе с тем, как ожидается, чистый отток частного капитала на трехлетнем горизонте также сохранится на низком уровне – около 2% ВВП. Во-первых, это будет обусловлено ожидаемым снижением интенсивности выплат по внешнему долгу на фоне расширения возможностей по его рефинансированию на международных рынках. Во-вторых, сохранение внутренних процентных ставок на относительно высоком уровне по сравнению с процентными ставками на внешних рынках, а также улучшение ожиданий восстановления экономической активности в России и реализация взвешенной макроэкономической политики будут способствовать сохранению привлекательности рублевых вложений как для российских, так и для глобальных инвесторов. Согласно базовому прогнозу, поступлений по текущему счету в предстоящие годы будет достаточно для обслуживания российскими кредитными и нефинансовыми организациями внешней задолженности. В этих условиях Банк России продолжит постепенно сворачивать операции рефинансирования в иностранной валюте и ожидает, что кредитные организации смогут полностью погасить задолженность по данным операциям до конца 2017 года. С учетом сочетания указанных тенденций на прогнозном горизонте ожидается сохранение в целом стабильной динамики курса рубля, что обусловит отсутствие дополнительного инфляционного давления со стороны этого фактора.

Помимо сдерживающего воздействия умеренного спроса и курсовой динамики, дополнительное понижательное влияние на темпы роста потребительских цен в прогнозный период будет оказывать ограниченный рост издержек производителей. Прежде всего это будет обусловлено сохранением относительно низких мировых цен на энергоносители при отсутствии значительных колебаний курса,

а также отмеченным выше поддержанием умеренных темпов индексации административно регулируемых тарифов на услуги естественных монополий.

В целом ожидается, что в 2017 году с учетом относительно слабого потребительского спроса, стабильной курсовой динамики и отсутствия дополнительного инфляционного давления со стороны факторов издержек годовая инфляция продолжит постепенно снижаться с 5,5–6% в декабре 2016 года до целевого уровня 4% в конце 2017 года и затем стабилизируется вблизи этого уровня.

В альтернативных сценариях Банка России заложены снижение цены на нефть до 25 долл. США за баррель в начале 2017 года, ее сохранение вблизи этого уровня до конца 2019 года (**сценарий II**) и постепенный рост цены на нефть до 55 долл. США за баррель в 2019 году (**сценарий III**).

Динамика цен на нефть, предполагаемая в **сценарии II**, может сформироваться на фоне сочетания ослабления роста мировой экономики и спроса на нефть в целом, с одной стороны, и действия дополнительных факторов увеличения предложения на отдельно взятом сегменте рынка энергоносителей – с другой. В том числе возможны ускорение восстановления поставок нефти из Нигерии и Ливии и значительное расширение предложения со стороны других стран – экспортеров нефти (прежде всего Ирана и Ирака).

Подобные негативные изменения внешних условий будут влиять на российскую экономику через сокращение доходов от экспорта, в том числе бюджетных (что потребует дополнительного использования средств суверенных фондов), снижение платежеспособности заемщиков, имеющих задолженность в иностранной валюте, ухудшение ожиданий относительно перспектив роста российской экономики и существенное снижение привлекательности вложений в нее для российских и внешних инвесторов. Вместе с тем следует учитывать возросшую устойчивость экономики к таким внешним шокам, поддерживаемую соответствующей реакцией денежно-кредитной и бюджетной политики, а также гибким изменением валютного курса. Это должно сдержать спад совокупного выпуска. Темпы снижения ВВП могут составить 1,0–1,5% в 2017 г. и 0,1–0,5% в 2018 г., после чего начнется восстановительный рост.

Замедление экономической активности станет фактором, сдерживающим инфляцию. Однако ослабление рубля на фоне ухудшения внешней конъюнктуры будет создавать повышательное давление на цены. В этих условиях достижение целевого уровня инфляции 4% станет более вероятным не к концу 2017 г., а в 2018 году. При этом потребуется поддержание относительно жестких денежно-кредитных условий на протяжении более длительного периода, чем в сценарии I. Это необходимо для сохранения привлекательности рублевых сбережений, предотвращения дестабилизации курсовых и инфляционных ожиданий и обеспечения ценовой и финансовой стабильности. Кроме того, при развитии негативного сценария Банк России будет оценивать необходимость проведения валютных интервенций в целях поддержания финансовой стабильности, а также увеличения объемов предоставления кредитным организациям иностранной валюты на возвратной основе в случае возникновения проблем с обслуживанием внешней задолженности у компаний и банков.

Сценарию III соответствует предположение о несколько более динамичном и сбалансированном росте глобальной экономики, повышении оптимизма инвесторов на мировых рынках, снижении имеющихся экономических и финансовых рисков развития ситуации в крупнейших странах с формирующимися рынками, прежде всего в Китае. При этом повышение процентных ставок мировыми центральными банками (прежде всего ФРС США) может происходить несколько быстрее, чем в базовом сценарии.

С учетом указанных предпосылок основным отличием развития ситуации в сценарии III является более высокий темп восстановления экономического роста – поддерживаемый повышением внешнего, а затем и внутреннего оптимизма, он может составить 1,2–1,7% в 2017 году и увеличиться до 2–2,5% в 2018–2019 годах.

Вместе с тем следует учитывать, что относительное улучшение внешней ситуации само по себе не способно существенным образом повлиять на среднесрочный потенциал роста российской экономики, для повышения которого требуется преодоление действующих структурных ограничений. С учетом этого темпы прироста российской экономики после восстановительного периода 2018–2019 годов стабилизируются вблизи темпов прироста потенциального ВВП в 1–1,5% и не будут превышать показатели базового сценария при сходной динамике инфляции и денежно-кредитных условий. В случае реализации данного сценария при принятии решений в области денежно-кредитной политики и государственной политики в целом крайне важным будет предупреждение формирования в экономике избыточного оптимизма. Его появление может снижать стимулы к реализации структурных преобразований, вести к накоплению экономических дисбалансов и возникновению финансовых пузырей. Своевременная реакция со стороны денежно-кредитной и макропруденциальной политики на возникновение признаков перегрева на товарных и кредитных рынках является крайне важной для противодействия рискам ускорения инфляции, чрезмерного роста долговой нагрузки и дестабилизации финансовых рынков.

В краткосрочном периоде в сценарии III влияние улучшения условий торговли на инфляцию будет разнонаправленным. С одной стороны, укрепление рубля на фоне предполагаемого роста цен на нефть будет оказывать сдерживающее воздействие на инфляцию. С другой стороны, повышение доходов экономических агентов и оживление спроса станут способствовать росту потребительских расходов, что будет иметь проинфляционный эффект. Тем не менее сдерживающее влияние динамики валютного курса на инфляцию в данном сценарии, по оценкам, реализуется быстрее, что обеспечит сближение инфляции с целевым уровнем 4% во второй половине 2017 года и при этом создаст возможности для несколько более быстрого снижения ключевой ставки при сохранении умеренно жесткой денежно-кредитной политики.

На развитие ситуации в данном сценарии также будет влиять подход к бюджетной политике. Параметры расходов бюджета, скорость сокращения дефицита и структура его финансирования будут оказывать влияние на экономическую динамику и условия проведения денежно-кредитной политики. В частности, при реализации данного сценария возобновится пополнение средств суверенных фондов в случае утверждения переходных положений бюджетного правила. С учетом этого Банк России рассчитывает на продолжение бюджетной консолидации при повышательной динамике цен на нефть. Банк России будет учитывать меры в области бюджетной политики при принятии решений по ключевой ставке, а также по операционным вопросам, включая определение параметров проведения своих операций в рублях и иностранной валюте.

Учитывая, что в данном случае внешние и внутренние условия будут несколько лучше, чем ожидается в базовом сценарии, Банк России рассмотрит возможность возобновления покупок иностранной валюты в целях пополнения международных резервов до уровня 500 млрд долл. США. Указанные операции могут проводиться в рамках применения механизма бюджетного правила. Уровень в 500 млрд долл. США — выше показателей достаточности резервов, рассчитанной по стандартным критериям, в том числе исходя из покрытия стоимости импорта товаров в страну за 3–4 месяца и выплат краткосрочного внешнего долга. Однако именно такой, более высокий уровень международных резервов представляется желательным для стабильного функционирования российской экономики в условиях неблагоприятной внешнеэкономической конъюнктуры и действия международных торговых и финансовых санкций. Банк России не устанавливает конкретных сроков для достижения 500 млрд долл. США по международным резервам, поскольку текущий уровень международных резервов страны уже является достаточно комфортным и Банк России регулярно пополняет эти резервы за счет приобретения золота на внутреннем рынке. Возобновление покупок иностранной валюты в целях пополнения международных резервов будет рассматриваться только в том случае, если проведение данных операций не будет противоречить выполнению цели по обеспечению ценовой и финансовой стабильности.

В рамках любого из рассмотренных сценариев Банк России не исключает возможности реализации дополнительных рисков, которые могут повлиять на инфляционную динамику. Значимыми рисками для прогноза инфляции на горизонте трех лет могут являться не предусмотренные в рассматриваемых сценариях скачки внутренних и внешних продовольственных цен (под влиянием факторов предложения), изменения бюджетной политики, включающие возможное ускорение индексации расходов или повышение налогов, а также ускорение роста административно регулируемых цен и тарифов. Необходимая степень реакции денежно-кредитной политики в ответ на реализацию указанных рисков будет определяться с учетом оценки масштаба и длительности их воздействия на инфляционные процессы. В частности, в случае отклонения от заявленных планов консолидации бюджета и увеличения его дефицита Банк России будет вынужден проводить более жесткую денежно-кредитную политику.

Банк России на регулярной основе по мере поступления новых данных осуществляет оценку и уточнение параметров прогноза макроэкономического развития, которые могут оказать влияние на решения в области реализации денежно-кредитной политики. Соответствующая информация будет оперативно публиковаться в ежеквартальном Докладе о денежно-кредитной политике Банка России.

Полный текст см. на сайте Банка России: www.cbr.ru

Стабильность банковской системы

НАФИ АНАЛИТИЧЕСКИЙ ЦЕНТР

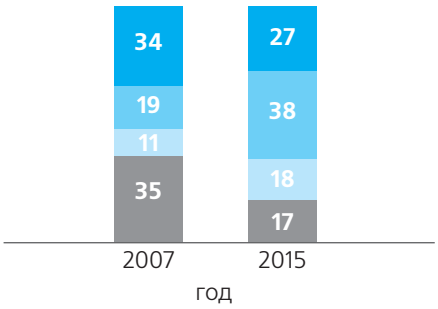
В связи с участившимися случаями отзыва лицензий у банков мы спросили россиян, как они оценивают стабильность банковской системы.

Более трети опрошенных отметили, что не ожидают в ближайший год-два масштабного банковского кризиса, тем не менее не исключают возможность банкротства одного или двух крупных банков (38%). Особенно часто такое предположение высказывают 35–44-летние граждане (44%).

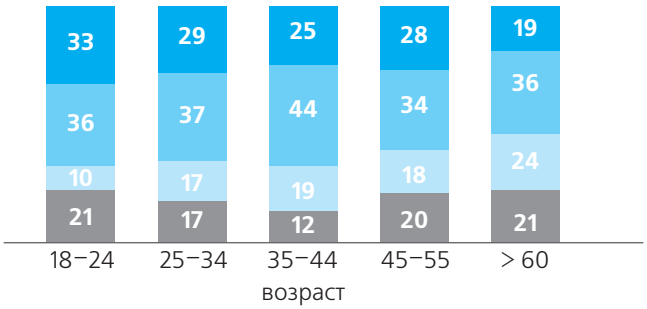
Около четверти наших сограждан (27%) верят в стабильность системы и прогнозируют банкротство только отдельных мелких и редких банков. Оптимистичные настроения свойственны в большей мере молодежи до 24 лет (33%) и в меньшей мере пенсионерам (19%).

18% россиян считают возможным повторение кризисной ситуации 1998 года и одновременное банкротство ряда ведущих банков. Пессимистичный сценарий склонны ожидать опрошенные старше 60 лет (24%).

«Как вы считаете, насколько стабильной будет банковская система в ближайшие год-два?», в % от всех опрошенных



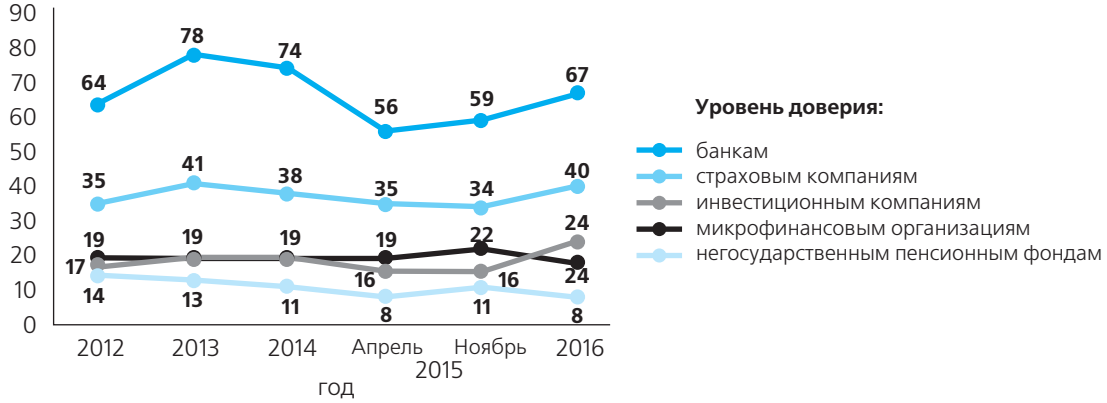
«Как вы считаете, насколько стабильной будет банковская система в ближайшие год-два», в % от опрошенных в разных возрастных группах



- Думаю, что ситуация будет по-прежнему стабильна и банкротиться будут только отдельные мелкие и средние банки
- Масштабного кризиса не ожидаю, но банкротство одного-двух крупных банков считаю возможным
- Вполне вероятно повторение кризиса наподобие августа 1998 года и одновременное банкротство ряда ведущих банков
- Затрудняюсь ответить

УРОВЕНЬ ДОВЕРИЯ БАНКАМ

«Скажите, пожалуйста, насколько вы доверяете следующим финансовым организациям?», % опрошенных, выбравших ответы «полностью доверяю» и «скорее доверяю»



ЛОЯЛЬНОСТЬ КЛИЕНТОВ БАНКАМ

Клиенты российских банков в целом демонстрируют достаточно высокий уровень лояльности к своим кредитно-финансовым организациям. Что касается основного банка, то среднее значение NPS[1] среди клиентов российских банков — 44 пункта (в марте 2016 года было 43 пункта), что является хорошим показателем для рынков услуг, предполагающих длительные отношения поставщика и потребителя. Более половины клиентов (59%) готовы рекомендовать свой банк другим, и только 15% скорее всего не станут этого делать.

Если посмотреть на индекс NPS по всем банкам, которыми пользуются опрошенные, то значение NPS ниже — 30 пунктов. Половина (51%) охотно порекомендовали бы банки, услугами которых пользуются, а каждый пятый (21%) не стал бы этого делать.

Чаще всего россияне (включая членов семьи) пользуются услугами одного банка (63%). Клиентами двух банков являются 22%, а трех — 5%. Каждый десятый опрошенный (9%) не пользуется услугами таких кредитно-финансовых учреждений.

«Продуктами и услугами скольких банков вы или ваша семья пользуетесь сейчас?»,
% от всех опрошенных

«Насколько вероятно, что вы порекомендуете этот банк родственникам, друзьям, знакомым? При ответе используйте шкалу, где 0 — точно не порекомендую, а 10 — точно порекомендую»,
в % от всех опрошенных (вопрос задавался по основному банку)

	Март 2016	Июль 2016
Промоутеры/Сторонники (9–10 баллов) — клиенты, которые лояльны банку и готовы рекомендовать его своим знакомым	57	59
Нейтралы (7–8 баллов) — пассивные клиенты банка, которые в целом удовлетворены им, но не обладают стремлением рекомендовать его другим	29	26
Критики (0–6 баллов) — не удовлетворены банком, не будут его рекомендовать, возможно, находятся в поиске альтернативы	14	15
Коэффициент лояльности (Net Promoter Score) — разница между долей критиков и сторонников, в пунктах	43	44

«Насколько вероятно, что вы порекомендуете этот банк родственникам, друзьям, знакомым? При ответе используйте шкалу, где 0 — точно не порекомендую, а 10 — точно порекомендую»,
в % от всех опрошенных (вопрос задавался по каждому банку, услугами которого пользуется респондент)

	Март 2016	Июль 2016
Промоутеры/Сторонники (9–10 баллов) — клиенты, которые лояльны банку и готовы рекомендовать его своим знакомым	50	51
Нейтралы (7–8 баллов) — пассивные клиенты банка, которые в целом удовлетворены им, но не обладают стремлением рекомендовать его другим	26	29
Критики (0–6 баллов) — не удовлетворены банком, не будут его рекомендовать, возможно, находятся в поиске альтернативы	24	20
Коэффициент лояльности (Net Promoter Score) — разница между долей критиков и сторонников, в пунктах	26	30

[1] Индекс NPS (Net Promoter Score) рассчитывается на основании условного отнесения клиентов к одной из трех групп — «промоутеров», или сторонников, «нейтралов» и «критиков» в зависимости от того, готовы ли они рекомендовать банк своим друзьям и знакомым. Индекс NPS по банковскому рынку рассчитывается НАФИ как по основному банку (каковым его определяют сами опрошенные), так и по всем банкам, услугами которых пользуются россияне.

ЖАЛОБЫ НА БАНКИ

Каждый десятый россиянин указал, что за последний год был недоволен финансовыми организациями, услугами которых пользовался. И только 4% из них выразили свою жалобу в устном или письменном виде. Оценка удовлетворенности качеством банковских услуг проводилась с помощью вопроса о наличии жалоб, претензий.

Заёмщики, имеющие «проблемный» кредит, чаще остальных выражали претензии (21% были недовольны, из них высказали жалобы – 8%). Основными формами выражения недовольства стали устная жалоба сотруднику организации (51% от всех высказавших претензии), жалобы знакомым во время разговоров (28%). На официальную письменную претензию руководству банка решились 28% недовольных респондентов.

Сравнительно редко использовалась как канал обратной связи книга жалоб и предложений (9%), только 1% недовольных оформили судебный иск.

Чем выше субъективная оценка финансовой грамотности опрошенных, тем они более склонны высказывать претензии. Так, в группе с отсутствием и низким уровнем знаний были недовольны 8%, а с хорошими и отличными знаниями – 13%; при этом доля обращавшихся с претензией к банку в два раза выше среди опрошенных с отличными знаниями (11%), чем с хорошими (5%).

«Вспомните, за последние 12 месяцев у вас были претензии к финансовым организациям (банкам, микрофинансовым организациям, кредитным кооперативам), услугами которых вы пользовались?», % от всех опрошенных

«Уточните, в каком формате вы выразили жалобу, претензию? (если было несколько случаев недовольства, то расскажите про последний по времени)»*, в % от указавших наличие заявленной жалобы

* Сумма ответов превышает 100%, так как респонденты могли выбрать несколько вариантов ответов

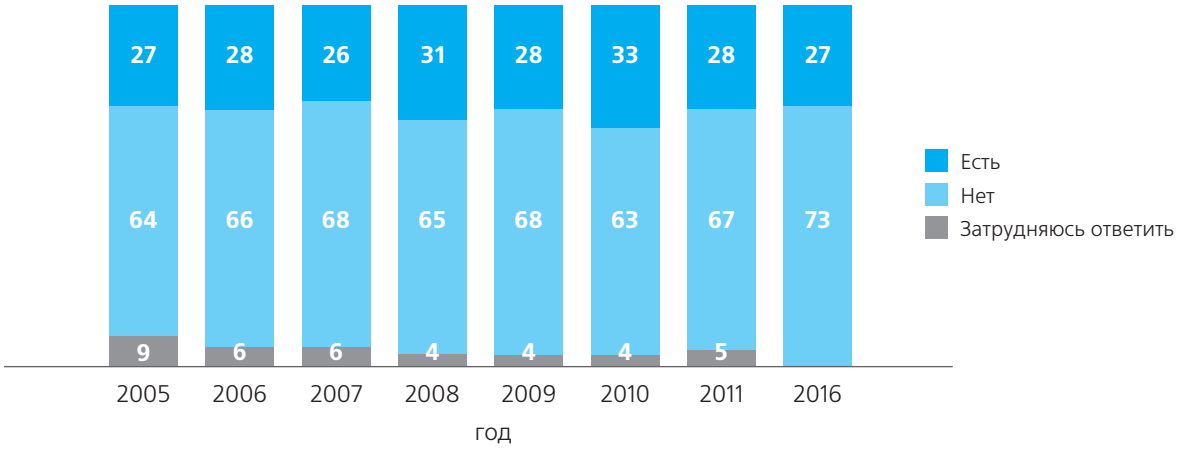
МАТЕРИАЛЬНОЕ ПОЛОЖЕНИЕ РОССИЯН

«К какой из следующих групп населения вы скорее могли бы себя отнести?», % от всех опрошенных

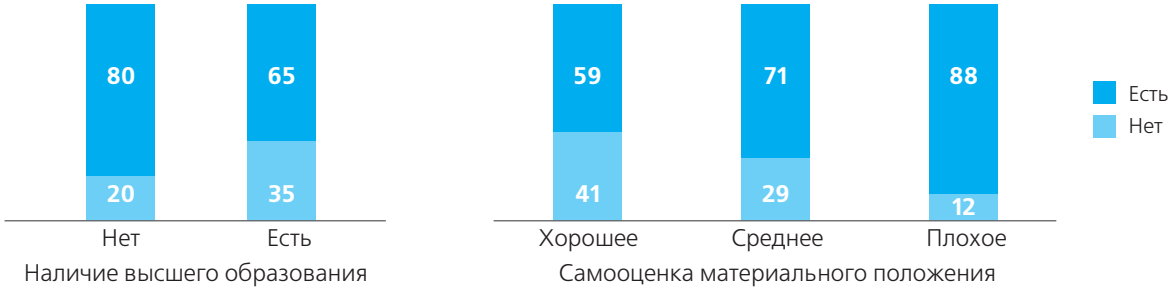
СБЕРЕЖЕНИЯ И НАКОПЛЕНИЯ

27% россиян сообщили, что в их семье есть сбережения (вклады в банках, накопительные страховые полисы, акции, облигации и другие ценные бумаги, наличные деньги). Доля таковых практически не меняется с 2005 года (за исключением некоторых лет). В большей степени склонны сберегать высокообразованные сограждане (35% против 20% не имеющих высшее образование), а также опрошенные, которые оценивают свое материальное положение выше среднего (41%).

«Есть ли у вас (вашей семьи) сбережения, накопления? Под сбережениями, накоплениями мы понимаем вклады в банках, накопительные страховые полисы, имеющиеся у вас (членов вашей семьи) акции, облигации и другие ценные бумаги, наличные деньги, которые вы отложили (не тратите на текущие нужды)», % от всех опрошенных



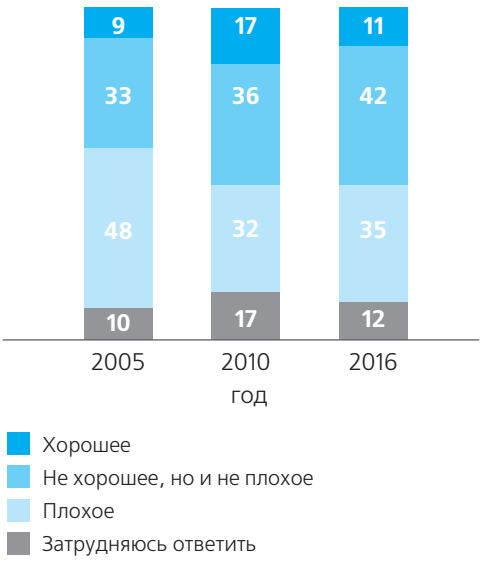
«Есть ли у вас (вашей семьи) сбережения, накопления? Под сбережениями, накоплениями мы понимаем вклады в банках, накопительные страховые полисы, имеющиеся у вас (членов вашей семьи) акции, облигации и другие ценные бумаги, наличные деньги, которые вы отложили (не тратите на текущие нужды)», % от всех опрошенных с разным уровнем образования и с разным материальным положением



Каждый десятый считает, что сейчас хорошее время для того, чтобы откладывать деньги (11%), и чаще это высказывают имеющие сбережения опрошенные (17%). В 2010 году так отвечали 17% россиян. Каждый третий, наоборот, полагает, что для сбережений не время (35%). 42% не могут однозначно сказать, хороший или плохой в настоящее время период для этого.

Каждый пятый опрошенный, имеющий работу, откладывает деньги на случай ее потери (24%), и столько же — не делают этого, но планируют начать (24%). Половина работающих сограждан не намерены создать «подушку безопасности» на случай потери источника средств (52%). Наиболее уязвимая группа — опрошенные 45–54 лет (среди них только 16% сберегают) и те, кто оценивает свое материальное положение как плохое (10% сберегают на случай потери работы).

«Как вы считаете, сейчас хорошее или плохое время для того, чтобы делать сбережения?», % от всех опрошенных



«Откладываете ли вы в настоящий момент деньги на случай потери работы или нет?», % от всех опрошенных, работающих в настоящее время

НАДЕЖНЫЕ И ВЫГОДНЫЕ СПОСОБЫ ВЛОЖЕНИЯ ДЕНЕГ

Недвижимость остается одним из наиболее надежных и выгодных способов вложения средств, по мнению большинства россиян. А такой способ как покупка валюты может быть выгодным, но не надежным.

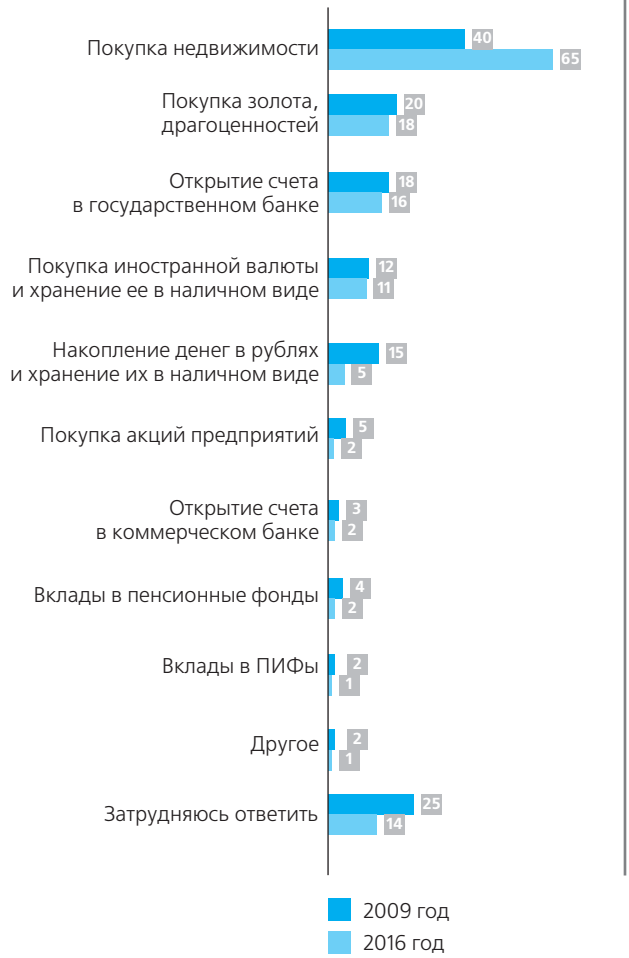
На протяжении 6 лет россияне считают недвижимость самым надежным вложением денег, причем доля высказывающих такую позицию выросла с 40% в 2009 году до 65% в 2016 году. Этот же способ считается и самым выгодным (69%).

На 2-м месте по надежности и выгодности — покупка золота и драгоценностей (18% — надежность и 23% выгодность). **Замыкает тройку самых выгодных вложений покупка евро и хранение их в наличном виде (19%). Надежность такого способа оценивается значительно ниже выгодности (только 8%).** Примечательно, что выгодность приобретения долларов отмечают 16%, а надежность этой валюты — 6%.

По надежности на 3-м месте — открытие счета в государственном банке (16%), однако выгодным такой способ вложения денег считают не более 18% опрошенных.

Потерял актуальность такой вид вложения средств, как хранение рублей в наличном виде: шесть лет назад на его надежность указывали 15% россиян, сейчас — втрое меньше (5%). Выгодность «наличного рубля» также оценивается невысоко (отметили не более 8%).

«Какие из следующих способов вложения денег представляются вам сейчас наиболее надежными?»*, в % от всех опрошенных



«Какие из следующих способов вложения денег представляются вам сейчас наиболее надежными? Какие из следующих способов вложения денег представляются вам сейчас наиболее выгодными?»*, в % от всех опрошенных

* Сумма ответов превышает 100%, так как респонденты могли выбрать несколько вариантов ответов

УДК 657.6

О. М. РАЗИНА,
кандидат экономических наук,
независимый эксперт,
член СРО «Содружество»

Внутренний аудит в банковской деятельности: основные направления и перспективы развития

В рамках данной публикации будут рассмотрены вопросы повышения ценности внутреннего аудита для кредитной организации, а также принципы, лежащие в основе совершенствования данной практики.

The issues of increasing the value of the internal audit will be considered part of this publication to the credit institution and the principles underlying the improvement of the practice.

Ключевые слова: внутренний аудит, ценность внутреннего аудита, риски, эффективность, международные стандарты аудита.

Key words: internal audit, the value of the internal audit, risks, efficiency, international standards on auditing.

Задачи по повышению ценности внутреннего аудита в банке являются наиболее значимыми в условиях современных требований, предъявляемых к совершенствованию общих принципов корпоративного управления, которые регламентированы в нормативном документе Базельского комитета «Принципы совершенствования корпоративного управления» (BCBS, Principles for Enhancing Corporate Governance-2015)[1], где система управления определена, как набор правил и элементов, регулирующих организационные и операционные системы банка, включая порядок формирования отчетности, процессов и управления рисками, функций внутреннего аудита.

Последнее десятилетие в банковской сфере во многом характеризуется увеличением рисков, обусловленных влиянием финансовой глобализации, а также усложнением информационных и банковских технологий, что требует совершенствования системы оценки и их управления в части:

– непрерывного измерения рисков, связанных с основным портфелем активов;

– идентификации профиля риска банка с целью информирования заинтересованных лиц и надзорных органов;

– возможности нейтрализации риска с целью снижения потенциальных потерь.

Необходимо учитывать, что руководство кредитной организации несет персональную ответственность за потенциальные риски, возникающие в банковской деятельности, установление их приемлемого уровня; обеспечение необходимых мер для их выявления, измерение и мониторинг. В связи с чем роль внутреннего аудита заключается в поддержке руководства кредитной организации, в достижении поставленных целей путем внедрения системных подходов в управлении рисками и повышении эффективности такой работы.

Международные стандарты профессиональной практики внутреннего аудита, в частности, стандарт 2120 «Управление риском» (IIA, 2012)[2], предусматривают необходимость проведения внутренней аудиторской деятельности для определения эффективности и оптимизации процесса управления рисками. При реализации оценки эффективности риска, процессов его управления внутренний аудит ставит перед собой задачи, связанные: с оценкой основных рисков; определением риск-аппетита; идентификацией событий, связанных с риском.

В соответствии со стандартом 2120 (IIA, 2012 года) заключения внутреннего аудита могут включать:

– оценку подверженности к риску в связи с особенностями управления, операциями и используемыми информационными системами кредитной организации;

– оценку потенциала риска мошенничества и способах управления этим риском;

– оценку способов нейтрализации рисков и используемую систему мониторинга.

Несмотря на ответственность, возложенную на внутренних аудиторов, их оценочные суждения

[1] Документ размещен на официальном сайте Базельского комитета. – URL: http://www.bis.org/publ/bcbs176.pdf

[2] International Standards for the Professional Practice of Internal Auditing (Standards). – URL: http://www.iia-ru.ru/files/

не должны отражать их личную ответственность в отношении процесса управления рисками. С другой стороны, рекомендации внутренних аудиторов позволяют преодолеть проблемы, связанные с возникновением рисков в результате использования структурного и организационного подхода к их выявлению.

Ценность внутреннего аудита для кредитной организации

В соответствии с определением, приведенным в Международных стандартах профессиональной практики внутреннего аудита (IIA, 2012), «Внутренний аудит повышает ценность организации (и ее заинтересованных сторон) только тогда, когда обеспечивает объективные гарантии, а также способствует повышению эффективности управления рисками и операционными процессами», тем самым формируя добавленную стоимость. Разделяя позицию отдельных авторов, считаем, что добавленная стоимость внутреннего аудита формируется на основе гарантий и консультаций. В одних аудиторских проектах (assurance) внутренние аудиторы дают разумные гарантии — ответ на вопрос, работает ли система внутреннего контроля, требует ли она улучшений. В других проектах (consulting) внутренние аудиторы могут содействовать менеджерам в процессе принятия управленческих решений.

С нашей точки зрения, гарантии и консультации, формируя ценность внутреннего аудита кредитной организации, неразрывно связаны с профессиональным уровнем аудитора. На этот счет в принципах осуществления внутреннего аудита в банках (BCBS)[3], регламентированных Базельским комитетом, существуют требования к профессиональной компетентности аудиторов. В частности, в третьем принципе[4] регламентированы не только критерии профессионализма для внутреннего аудитора, но и необходимые требования, предъявляемые к руководителю службы в целях профессионального соответствия сотрудников растущим компетенциям. Например, в данном принципе регламентирован подход, на основе которого руководитель службы внутреннего аудита должен обеспечить получение сотрудниками необходимого уровня квалификации с учетом растущей сложности и технических особенностей новых бизнес-процессов и банковских продуктов. Внедрение данного принципа на практике уже предусматривает необходимость постоянного повышения квалификации в рамках существующих профессиональных компетенций и должностных обязанностей.

Аналогичные требования к уровню профессиональной подготовки внутренних аудиторов можно встретить в международных стандартах профессиональной практики внутренних аудиторов (стандарт 1210 «Профессионализм»)[5], раскрывающих общие подходы и интерпретацию к уровню квалификации для руководителя и специалистов среднего звена. Так, в параграфе 1210.А3 стандарта обоснована необходимость знания внутренними аудиторами ключевых рисков и процедур их контроля, включая использование информационных технологий и автоматизированных методов аудита в объеме, достаточном для выполнения порученных заданий. Однако в стандарте обращается особое внимание на то, что не все аудиторы должны обладать соответствующими компетенциями при осуществлении контрольных процедур, связанных с использованием информационных технологий, чья основная функция не предполагает таких профессиональных обязанностей. Кроме того, стандарт 1210 уточняет необходимость постоянного совершенствования знаний внутренних аудиторов путем непрерывного профессионального развития.

Таким образом, обобщающим элементом уровня компетентности, опыта и профессиональных знаний аудиторов являются не только базовые компетенции, определенные в стандарте, но и возможность использования информационных технологий, позволяющих анализировать и оценивать информацию в рамках передовых инструментов и методов внутреннего аудита.

Научно-практический интерес представляет интерпретация международного стандарта профессиональной практики внутреннего аудита 1300 «Программа гарантии и повышения качества внутреннего аудита»[6], в соответствии с которой руководитель службы внутреннего аудита должен разработать и поддерживать актуализацию программы гарантии и повышения качества аудиторской деятельности. В число обязательных направлений такой программы входит анализ эффективности и результативности внутреннего аудита для совершенствования внутренней практики его реализации в банке, включая внутренние и внешние оценки.

Одним из основных вопросов, рассматриваемых при оценке функций внутреннего аудита, является его эффективность, в том числе и порядок реализации и выполнения планов. Например, результаты исследования аудиторской консалтинговой компании Делойт Туш[7], проведенные в 2014

[3] Документ размещен на официальном сайте Базельского комитета. — URL: http://www.bis.org/publ/bcbs176.pdf

[4] Третий принцип. Для эффективного осуществления внутреннего аудита важное значение имеет уровень профессиональной компетентности внутренних аудиторов, как всех вместе, так и каждого в отдельности, их знания и опыт. — *Прим. автора.*

[5] International Standards for the Professional Practice of Internal Auditing (Standards). — URL: http://www.iia-ru.ru/files/

[6] Там же.

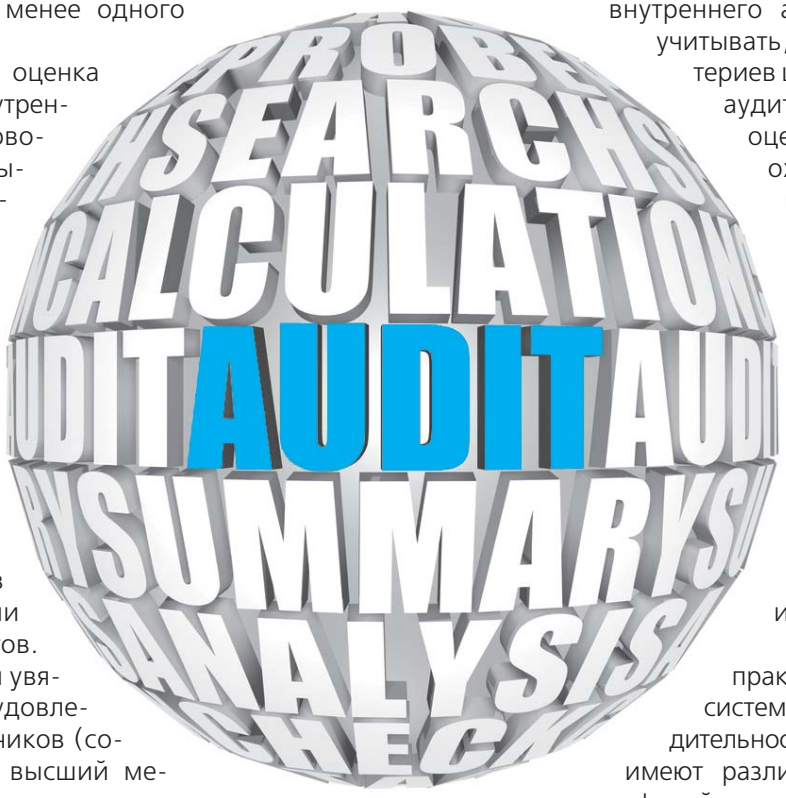
[7] Deloitte (2014), Head of Internal Audit Survey 2014. — URL: http://www2.deloitte.com/content/dam/Deloitte

году, позволили сделать следующие выводы в отношении оценки эффективности внутреннего аудита:

– 97% респондентов подтвердили, что оценка эффективности внутреннего аудита производится в соответствии с определенной методикой;

– 95% респондентов отметили использование методологии в соответствии со стандартами Института внутренних аудиторов (IIA);

– 67% респондентов подтвердили, что методология оценки эффективности внутреннего аудита включает в себя процесс внешней оценки его качества, учитывая, что стандарты IIA требуют обеспечения совершенствования уже существующих программ и отчетов об оценке с максимальной частотой, не менее одного раза в пять лет.



Традиционно оценка эффективности внутреннего аудита проводится в целях повышения объективности работы при использовании качественных и количественных показателей, определяющих не только степень выполнения годового плана, но и конкретные трудозатраты и проблемы в рамках реализации отдельных проектов. Данные показатели увязаны со степенью удовлетворенности заказчиков (совет директоров и высший менеджмент банка) с учетом выполненной аудиторами работы.

К таким показателям относятся:

• количество и состав выявленных рисков в результате внутреннего аудита;

• сумма потенциальных и реализованных рисков в рамках полученного экономического эффекта по итогам работы службы внутреннего аудита;

• степень выполнения годового плана в разрезе направлений и бизнес-процессов в банке;

• степень выполнения рекомендаций внутреннего аудита, а также доля принятых и непринятых рекомендаций со стороны структурных подразделений банка;

• наличие повторных рекомендаций, ранее не выполненных в ходе проведения внутреннего аудита;

• степень зрелости горизонтальной культуры внутреннего аудита и в целом кредитной организации с учетом внедряемых принципов корпоративной этики;

• оценка качества взаимодействия сотрудников службы внутреннего аудита с подразделениями банка;

• наличие текучести кадров в структуре внутреннего аудита в рамках годовой динамики и причин, послуживших увольнению;

• общая оценка удовлетворенности заказчиков (совет директоров и высший менеджмент банка) от выполненной аудиторами работы за текущий период.

Критерии для измерения ценности внутреннего аудита. Необходимо учитывать, что разработка критериев ценности внутреннего аудита, в отличие от оценки эффективности, охватывает основные направления его деятельности, включая общую производительность. Измерение производительности имеет огромное значение в целях дальнейшего совершенствования деятельности внутреннего аудита и внедрения новых методов и процедур.

Существующие в практике классификации систем измерения производительности внутреннего аудита имеют различия, обусловленные спецификой и направлениями аудиторских процедур. Однако наиболее используемой считается система сбалансированных показателей, когда посредством выбора комбинации индикаторов / показателей производится их привязка к определенной категории заинтересованных сторон.

Второй по популярности метод именуется как «вход – процесс – выход» (IPO – «input – process – output»), позволяющий выявить наиболее ценные характеристики внутреннего аудита на основе процессного подхода:

• вход (оценка опыта, квалификации персонала, утвержденного бюджета и других факторов, влияющих на качество организации внутреннего аудита);

• процесс (оценка основных процессов, сопровождающих направления внутреннего аудита);

Классификация показателей, используемая для измерения ценности внутреннего аудита

Основные категории	Инструменты и показатели, используемые для измерения ценности внутреннего аудита
По степени удовлетворения заинтересованных сторон	• Обзоры деятельности/Вопросы заинтересованных сторон • Интервью/Встречи с представителями заинтересованных сторон • Основные факторы производительности аудита/индикаторы
В разрезе процессов внутреннего аудита	• Соответствующие планы внутреннего аудита, устанавливаемые для каждого направления, включая: степень охвата, задачи, сроки, распределение ресурсов • Проведение проверок в соответствии с установленными методиками и практикой • Обратная связь, которая получена от ключевых заинтересованных сторон в отношении процедур эффективного снижения рисков
Инновации и производительность	• Осуществление мероприятий по обеспечению надлежащей профессиональной подготовки сотрудников аудита • Измерение количества сертификатов, полученных сотрудниками службы внутреннего аудита • Осуществление мер, которые позволяют обеспечивать достижение поставленных целей и задач миссии кредитной организации

• результат (оценка конечных результатов деятельности внутреннего аудита, заключающаяся в предоставлении гарантий, консультационных услуг, предложенных рекомендаций, оптимизации качества бизнес-процессов на основе заключений внутренних аудиторов).

Вместе с тем многочисленные опросы и исследования, характеризующие ценность внутреннего аудита, свидетельствуют, что среди основных категорий, подлежащих измерению и оценке аудиторской деятельности: степень удовлетворенности заинтересованных сторон, процессы внутреннего аудита и их способность к инновациям.

В таблице приведена классификация показателей, используемая для измерения ценности внутреннего аудита[8].

С нашей точки зрения, вне зависимости от инструментов и методов для измерения эффективности и производительности, необходимо в первую очередь опираться на мнение и позиции заинтересованных сторон, включая Комитет по аудиту и ключевых руководителей (топ-менеджмента), что в целом позволяет обеспечить повышение ценности внутреннего аудита для всей кредитной организации.

Кроме того, важное значение приобретают индикаторы, используемые для измерения ценности внутреннего аудита. Среди наиболее известных и популярных можно выделить следующие:

– процент завершенных планов аудита;

– процент принятых и/или реализованных рекомендаций;

– обзор обратной связи от заинтересованных сторон (экспертные оценки и профессиональные суждения);

– обзор обратной связи от проверяемых подразделений банка;

– оценки внешних аудиторов о деятельности Службы внутреннего аудита;

– процент своевременного завершения проверочных мероприятий и отчетов;

– количество значимых результатов внутреннего аудита (количество проверок, результаты которых позволили предотвратить или выявить существенные риски и проблемы);

– оборачиваемость аудиторского цикла (время начала и окончания аудита);

– отсутствие существенных сбоев в работе (нарушение сроков выполнения плана, проверки, другие проблемы, связанные с невыполнением аудиторского задания и пр.).

Меры для поддержания ценности внутреннего аудита. Поддержание ценности внутреннего аудита является первостепенной задачей для руководства кредитной организации в целях нейтрализации и снижения банковских рисков. Приведем основные мероприятия, реализация которых, на наш взгляд, будет способствовать эффективной работе внутреннего аудита в банке.

1. Проведение регулярной оценки эффективности внутреннего аудита путем проведения обзоров уже реализованных аудиторских проверок при выявлении операционных убытков для выявления слабых сторон в существующих процедурах, а также с целью более глубокого понимания реальных рисков от основной деятельности.

2. Организация открытых форумов и информационных площадок между подразделениями второй и третьей линии защиты кредитной организации с целью обмена информацией и выработки наиболее эффективных мер по снижению событий

[8] Составлена автором.

риска, а также эффективного мониторинга и оценки рисков.

3. Повышение качества IT-экспертизы и профессиональных навыков сотрудников внутреннего аудита в части использования информационных технологий и повышения качества внутренних процедур для автоматизации аудиторской деятельности.

4. Использование сравнительного анализа результатов аудиторской деятельности в части применения общих подходов к тестированию плановых и реально полученных показателей деятельности внутреннего аудита за период.

5. Гармонизация деятельности внутреннего аудита со стратегией деятельности кредитной организации с целью оценки соотношения затрат и реальных выгод от проведенных проверочных мероприятий.

6. Реализация мероприятий по адаптации инновационных практик внутреннего аудита с целью своевременного реагирования за факторы изменения внутренней и внешней среды, а также снижения последствий от основных рисков банковской деятельности.

7. Использование непрерывного совершенствования методологии внутреннего аудита, основанной на принципах Six Sigma[9], для цели оптимизации общих подходов к организации аудиторской деятельности и повышения эффективности качества внутренних коммуникаций.

Источники

1. Принципы совершенствования корпоративного управления. – URL: http://www.bis.org/publ/bcbs176.pdf

2. International Standards for the Professional Practice of Internal Auditing (Standards). – URL: http://www.iia-ru.ru/files

3. Deloitte (2014), Head of Internal Audit Survey 2014. – URL: http://www2.deloitte.com/content/dam/Deloitte

[9] В основе данной методологии лежат следующие принципы: стремление к установлению устойчивого и предсказуемого протекания процессов; показатели оценки эффективности бизнес-процессов должны быть измеряемыми, контролируемыми и улучшаемыми, а также отражать изменения в протекании процессов; для достижения постоянного улучшения качества необходимо вовлечение персонала организации на всех уровнях, особенно высшего руководства. – *Прим. автора.*

УДК 336.71

Ю. В. МОРОЗОВ,
заместитель директора департамента
банковского аудита ООО «Внешаудит консалтинг»,
кандидат экономических наук

Аудит системы внутреннего контроля в целях ПОД/ФТ[1]: взгляд практикующего специалиста

Статья посвящена аудиту системы внутреннего контроля в целях противодействия отмыванию доходов, полученных преступным путем, и финансированию терроризма. Изложены наиболее часто встречающиеся недостатки и нарушения, выявляемые в процессе аудита деятельности банков. Автором предложены оригинальные форматы запроса информации для повышения эффективности проведения аудиторской проверки.

The article is devoted to audit of internal control system in order to counter anti-money laundering and terrorism financing. The most frequently occurring deficiencies and violations during the audit of the activities of banks are stated. The original information request formats to improve the efficiency of the audit were proposed.

Ключевые слова: аудит, противодействие легализации доходов, полученных преступным путем, и финансированию терроризма (ПОД/ФТ), банки.

Key words: audit, anti-money laundering and counter terrorism financing (AML/CFT), banks.

С момента принятия Федерального закона от 7 августа 2001 года № 115-ФЗ «О противодействии легализации (отмыванию) доходов, полученных преступным путем, и финансированию терроризма» (далее – Закон № 115-ФЗ) прошло уже 15 лет, и большинством коммерческих банков накоплен немалый опыт в работе по ПОД/ФТ.

Созданы организационные, нормативно-правовые и программно-технические предпосылки и условия для проведения эффективной работы в области ПОД/ФТ:

– сформированы соответствующие подразделения по ПОД/ФТ (в крупных банках – департаменты (как правило, имеют название «Департамент финансового мониторинга», в средних и мелких банках – соответствующие управления или отделы, иногда – службы (например, Служба специального контроля);

– разработаны и применяются на практике Правила внутреннего контроля в целях ПОД/ФТ и многие другие внутренние регламенты в виде положений, инструкций и т. п.;

– внедрены различные программно-технические комплексы, позволяющие в автоматизированном режиме выявлять операции, подлежащие обязательному контролю, и сомнительные сделки, формировать сообщения и направлять их в уполномоченный орган – Федеральную службу по финансовому мониторингу (далее – Росфинмониторинг).

Вместе с тем Банком России ежегодно отзываются лицензии у десятков банков, вовлеченных в противоправные действия, связанные с легализацией (отмыванием) доходов, полученных преступным путем. Как отметил Президент РФ В.В. Путин в своем ежегодном Послании Федеральному Собранию 1 декабря 2016 года, «благодаря последовательной и решительной работе Центрального банка банковская система очищается от контор, которые нарушают закон, права клиентов, ведут сомнительные финансовые операции. С рынка ушли многие из них, во всяком случае слабые игроки. Проведено оздоровление банковской сферы, оно и продолжается Центральным банком» [2].

Сегодня у ряда коммерческих банков существуют проблемы в организации эффективной работы подразделений по ПОД/ФТ. Службы внутреннего аудита таких банков не выявляют в полном объеме и своевременно нарушения и недостатки в построении бизнес-процессов, связанных с

[1] ПОД/ФТ – противодействие отмыванию доходов, полученных преступным путем, и финансированию терроризма (планируется цикл статей о проблемах организации работы по ПОД/ФТ в коммерческих банках и нарушениях, выявленных в ходе аудиторских проверок их деятельности).

[2] Послание Президента Федеральному Собранию, 1 декабря 2016 года. – URL: http://www.kremlin.ru

ПОД/ФТ, внешний аудит также не в полной мере справляется с возложенными на него задачами по оценке качества и эффективности функционирования системы внутреннего контроля в целом и деятельности должностных лиц, ответственных за соблюдение правил по ПОД/ФТ, в частности.

В связи с этим цель данной статьи – поделиться наблюдениями о наиболее часто встречающихся недостатках и нарушениях, выявляемых в процессе аудита деятельности банков, высказать некоторые соображения по организации и проведению отдельных аудиторских процедур и дать ряд рекомендаций подразделениям по ПОД/ФТ, службам внутреннего аудита и аудиторским организациям по совершенствованию работы в области ПОД/ФТ и ее проверкам.

Аудиторская проверка работы по ПОД/ФТ проводится с целью установления фактов соблюдения (несоблюдения) банком при осуществлении своей деятельности предписанных действующим законодательством и нормативными актами Банка России мер, направленных на ПОД/ФТ, полноты и своевременности информирования Росфинмониторинга о сделках клиентов и собственных операциях, подлежащих обязательному контролю, и формирование аудиторского мнения о соответствии системы внутреннего контроля кредитной организации в целях ПОД/ФТ характеру и масштабам проводимых операций. Важность достижения указанной цели аудита обусловливается высокой вероятностью применения к банкам пруденциальных мер воздействия со стороны Банка России. Это, в свою очередь, может привести к невозможности применения банком допущения о непрерывности деятельности, которое является основополагающим принципом подготовки бухгалтерской (финансовой) отчетности аудируемого лица (п. 2 Международного стандарта аудита 570 «Непрерывность деятельности»). Так, вследствие несоблюдения банком процедур обязательного контроля сделок, отвечающих критериям операций, которые могут быть направлены на легализацию доходов, полученных преступным путем, и финансированию терроризма, Банк России имеет право взыскивать штраф в размере до 0,1% минимального размера уставного капитала либо ограничивать проведение банком отдельных операций (ст. 74 Федерального закона от 10 июля 2002 года № 86-ФЗ «О Центральном банке Российской Федерации (Банке России)»). Невыполнение установленных требований обязательного контроля может повлечь отзыв (аннулирование) лицензии кредитной организации (ст. 13 Закона № 115-ФЗ).

Рассмотрим поэтапно организацию и проведение аудиторской проверки по ПОД/ФТ.

По нашему мнению, чрезвычайно важное значение имеет подготовительный этап проверки, в ходе которого осуществляется запрос первичной информации по ПОД/ФТ и ее обработка.

В ходе подготовительного этапа проверки по ПОД/ФТ решаются принципиальные задачи на двух уровнях:

1. Определяется степень вовлеченности банка в проведение сомнительных операций[3] и выявляется наличие/отсутствие обстоятельств, свидетельствующих о быстром ухудшении его финансового положения, что может привести к возникновению ситуаций, угрожающих интересам кредиторов и вкладчиков банка (**макроуровень**).

2. Определяются отдельные клиенты, которые, возможно, осуществляют операции, имеющие признаки сомнительных (**микроуровень**).

Для решения **первой задачи** аудиторами специально используются внутрифирменные программные продукты, которые позволяют проводить аудиторские процедуры в виде тестирования с целью определения риска вовлеченности Банка в обслуживание сомнительных операций, осуществляемых клиентами Банка, а также с целью определения быстрого ухудшении финансового положения банка.

В качестве критериев сомнительности используются рекомендации Банка России, изложенные в Письме Банка России от 15 апреля 2013 года № 69-Т «О неотложных мерах оперативного надзорного реагирования» и Письме Банка России от 4 сентября 2013 года № 172-Т «О приоритетных мерах при осуществлении банковского надзора».

Исходными данными для тестирования являются месячные формы отчетности: 0409101 «Оборотная ведомость по счетам бухгалтерского учета кредитной организации», 0409664 «Отчет о валютных операциях, осуществляемых по банковским счетам клиентов в уполномоченных банках», 0409202 «Отчет о наличном денежном обороте», 0409134 «Расчет собственных средств (капитала)», 0409135 «Информация об обязательных нормативах и о других показателях деятельности кредитной организации». Результаты тестирования оформляются в форме таблиц (примерные форматы приведены в *табл. 1* и *2*).

Следует отметить, что Банк России регулярно пересматривает параметры критериев определения признаков высокой вовлеченности кредитной организации в проведение сомнительных безналичных и (или) наличных операций.

---

[3] Сомнительные операции – операции, осуществляемые клиентами кредитных организаций, имеющие необычный характер и признаки отсутствия явного экономического смысла и очевидных законных целей, которые могут проводиться для вывода капитала из страны, финансирования «серого» импорта, перевода денежных средств из безналичной в наличную форму и последующего ухода от налогообложения, а также для финансовой поддержки коррупции и других противозаконных целей (Письмо Банка России от 4 сентября 2013 года № 172-Т).

Таблица 1

Степень вовлеченности кредитной организации в проведение сомнительных операций
(по Письму ЦБ РФ №172-Т)

Дата / Показатель	Доля сомнительных операций в безналичных расчетах	Доля сомнительных операций в наличных расчетах	Индекс сомнительных операций	Степень вовлеченности в сомнительные операции
1-е число месяца				
1-е число месяца				
. . .				

При этом граничные значения следующие:

Индекс сомнительных операций	Степень вовлеченности в сомнительные операции
индекс СО < 2	низкая
5 > индекс СО > 2	умеренный риск
10 > индекс СО > 5	средний риск
20 > индекс СО > 10	высокий риск
индекс СО > 20	крайне высокий риск

Первоначально, в 2013 году, Банк России установил, что под признаками высокой вовлеченности кредитной организации в проведение сомнительных безналичных и (или) наличных операций понимается одно из следующих обстоятельств[4]:

– превышение за последний квартал суммарного значения удельного веса (доли) объема сомнительных наличных операций в объемах дебетовых оборотов по счетам юридических и физических лиц и удельного веса (доли) объема сомнительных безналичных операций в объемах дебетовых оборотов по счетам юридических лиц величины 5%;

– и (или) превышение за последний квартал объема сомнительных безналичных операций величины 5 млрд руб.;

– и (или) превышение за последний квартал объема сомнительных наличных операций величины 5 млрд руб.

В 2014 году критерии определения признаков высокой вовлеченности кредитной организации в проведение сомнительных безналичных и (или) наличных операций были уточнены[5]:

– превышение величины 4% за последний квартал суммарного значения удельного веса (доли) объема сомнительных наличных операций в объемах дебетовых оборотов по счетам юридических и физических лиц и удельного веса (доли) объема сомнительных безналичных операций в объемах дебетовых оборотов по счетам юридических лиц;

– и (или) превышение величины 3 млрд руб. за последний квартал объема сомнительных операций клиентов с безналичными и наличными денежными средствами в совокупности.

С III квартала 2016 года действуют следующие новые параметры вышеуказанных критериев, установленные Банком России[6]:

– превышение величины 3% за последний квартал суммарного значения удельного веса (доли) объема сомнительных наличных операций в объемах дебетовых оборотов по счетам юридических и физических лиц и удельного веса (доли) объема сомнительных безналичных операций в объемах дебетовых оборотов по счетам юридических лиц;

– и (или) превышение величины 2 млрд руб. за последний квартал объема сомнительных операций клиентов с безналичными и наличными денежными средствами в совокупности.

В случае если по результатам тестирования выявляются признаки высокой вовлеченности банка в проведение сомнительных операций, аудитор, в целях формирования окончательных выводов об уровне работы по ПОД/ФТ, должен запросить в ходе проверки у банка доказательства того, что операции, имевшие признаки сомнительных, проводились клиентами в соответствии с принципами добросовестности и разумности, установленными гражданским законодательством, обычаями делового оборота, а также доказательства того, что банк осуществил необходимые и достаточные меры, направленные на исключение проведения клиентами сомнительных операций.

Одновременно аудитор осуществляет тестирование наличия/отсутствия признаков ухудшения финансового состояния банка на основе внутрифирменного программного обеспечения *(см. табл. 2)*.

Оперативный анализ представленной банком отчетности по формам 0409101, 0409134 и 0409135 позволяет установить экономическое содержание проводимых операций и оценить достоверность представленных форм отчетности, выявить нарушения федеральных законов и издаваемых в соответствии с ними нормативных актов Банка России,

[4] Письмо Банка России от 4 сентября 2013 года № 172-Т «О приоритетных мерах при осуществлении банковского надзора».

[5] Письмо Банка России от 21 мая 2014 года № 92-Т «О критериях признаков высокой вовлеченности кредитной организации в проведение сомнительных безналичных и наличных операций».

Таблица 2

Обстоятельства, свидетельствующие о быстром ухудшении финансового положения кредитной организации

Критерий	**Дата (на 1-е число месяца)**	**Дата (на 1-е число месяца)**	**. . .**	**Пороговые значения (границы),** *%*
ПРИЛОЖЕНИЕ 1 К ПИСЬМУ ЦБ РФ № 69-Т				
Существенное увеличение остатков на счетах и во вкладах физических лиц в целом по кредитной организации				> 20
Отношение дебетовых оборотов по корсчету в Банке России к кредитовым оборотам по вкладам физических лиц				> 100
Остатки в кассе составляют существенный удельный вес в активах кредитной организации				> 25
Существенный объем операций по покупке учтенных векселей (отношение дебетовых оборотов за месяц по счетам по учету векселей к активам)				> 30
Существенный объем операций по продаже учтенных векселей (отношение кредитовых оборотов за месяц по счетам по учету векселей к активам)				> 30
Существенный рост остатков на счетах по учету выпущенных кредитной организацией векселей и банковских акцептов при удельном весе остатков на счетах по учету выпущенных кредитной организацией векселей и акцептов в пассивах 10% и более				> 50
ПРИЛОЖЕНИЕ 2 К ПИСЬМУ ЦБ РФ № 69-Т				
Соотношение суммарных оборотов за месяц по кассе (счет 20202) и по счетам по учету денежных средств в пути (счет 20209) к сумме оборотов по счетам, которые превышают величину активов-нетто				> 10
Соотношение общего объема дебетовых оборотов по счетам выданных кредитов (учтенных векселей) за месяц к общему объему денежных средств, списанных с корреспондентских счетов кредитной организации (кредитовые обороты за месяц по счетам НОСТРО)				> 25
Соотношение общего объема кредитовых оборотов за месяц по счетам погашенных кредитов (учтенных векселей) к общему объему денежных средств, поступивших на корреспондентские счета кредитной организации (дебетовые обороты за месяц по счетам НОСТРО)				> 25
Обороты за месяц по выпуску векселей и банковских акцептов в процентах от общего объема пассивов				> 10
Существенное увеличение остатков на счетах и во вкладах физических лиц отдельно по головному офису или филиалу кредитной организации				> 50 за месяц
Существенный рост объема ссудной задолженности по кредитной организации в целом				> 10 за месяц

оценить характер допущенных нарушений, причины их возникновения и влияния на экономическое положение банка.

На основе результатов данного тестирования аудиторы получают обобщенную информацию о наличии/отсутствии признаков ухудшения финансового состояния банка и степени его вовлеченности в проведение сомнительных операций.

Кроме того, для получения общей информации о деятельности Банка в области ПОД/ФТ следует направить запрос о предоставлении следующих документов (приводим примерный перечень).

1. Приказ о создании структурного подразделения (если есть такое подразделение) по противодействию легализации (отмыванию) доходов, полученных преступным путем.

2. Приказ о назначении ответственного лица по проведению мер по противодействию легализации (отмывания) доходов, полученных преступным путем, и документы, определяющие его должностные обязанности.

3. Правила по осуществлению в Банке внутреннего контроля в целях противодействия осуществлению легализации (отмыванию) доходов, полученных преступным путем, и финансированию терроризма.

4. Акты проверок контролирующего органа осуществления Банком противодействия легализации (отмыванию) доходов, полученных преступным путем, и финансированию терроризма (если имели место).

5. Все письма и предписания контролирующего органа по указанному вопросу.

6. Внутренние сообщения сотрудников кредитной организации при выявлении операции, подлежащей обязательному контролю, или необычной сделки.

7. Анкеты клиентов Банка (юридических, физических лиц и ПБОЮЛ) за анализируемый период, в том числе: резиденты и нерезиденты – физические и юридические лица (выборочно в ходе проверки).

8. Отчеты в виде электронного документа (ОЭД) по операциям за проверяемый период.

9. Все отчеты Ответственного сотрудника о результатах реализации правил внутреннего контроля в целях противодействия легализации (отмыванию) доходов, полученных преступным путем, и финансированию терроризма, в том числе программ его осуществления по итогам года.

10. Внутренние положения и документацию по обучению сотрудников кредитной организации по вопросам противодействия легализации (отмыванию) доходов, полученных преступным путем.

Полученная информация также принимается во внимание аудитором при решении **второй задачи** подготовительного этапа – подготовки запроса информации о масштабах и характере операций клиентов для формирования выборки с целью определения отдельных клиентов, осуществляющих операции, имеющие признаки сомнительных (**микроуровень**).

При проведении выборки аудитор должен руководствоваться МСА 530 «Аудиторская выборка». На наш взгляд, целесообразно применить в данном случае «стратификацию» – процесс разделения генеральной совокупности на подмножества, каждое из которых представляет собой группу элементов выборки, обладающих сходными характеристиками.

Как показывает практика, сделки/операции юридических лиц – отдельных компаний или организаций (а не физических лиц) – наиболее часто подпадают под признаки обязательного контроля или могут носить сомнительный характер, причем в крупных объемах.

В свою очередь, с точки зрения повышения эффективности анализа работы по ПОД/ФТ, целесообразно, по нашему мнению, разделить на 2 крупные группы юридические лица, находящиеся на обслуживании в банке:

– «новые клиенты», открывшие счета в банке в проверяемом периоде (год, 9 месяцев и т. п.);

– «старые клиенты», открывшие счета в банке в предыдущие годы (до проверяемого периода).

В данном случае на основе профессионального суждения мы используем метод нестатистической выборки для отбора элементов выборки (п. А12 МСА 530).

Выборка «новых клиентов»

Этап 1. В качестве одной из подготовительных аудиторских процедур предлагаем перед началом проверки запрашивать информацию в следующем формате *(табл. 3)*.

На наш взгляд, получение информации о клиентах – юридических лицах и индивидуальных предпринимателях, открывших расчетные счета в течение анализируемого периода в вышеуказанном формате, имеет ряд преимуществ, позволяющих в дальнейшем обеспечить качественную выборку клиентов для анализа их операций:

– аудитор получает полную информацию о новых корпоративных клиентах банка еще до начала проверки, что имеет важное значение как для выборочной проверки операций вновь созданных компаний с точки зрения обязательного контроля, так и для анализа операций новых клиентов на предмет их законного/сомнительного характера (как показывает наш опыт, подавляющая часть выявленных сомнительных операций клиентов Банка в основном приходится на новые компании, открывшие расчетные/валютные счета в анализируе-

Таблица 3

Список клиентов, юридических лиц и индивидуальных предпринимателей, открывших расчетные счета в течение анализируемого периода (год, 9 месяцев и т. п., в формате Excel)

Наименование клиента	**ИНН**	**№ расчетного счета**	**Дата открытия расчетного счета**	**Дата закрытия расчетного счета**	**Дата регистрации компании**	**Обороты по дебету расчетного счета,** *руб.*	**Обороты по кредиту расчетного счета,** *руб.*

мом периоде; «старые» клиенты, находящиеся на обслуживании в банке не один год, значительно реже проводят операции, имеющие признаки сомнительных, их деятельность, как правило, достаточно глубоко и всесторонне изучена сотрудниками банка в предыдущие годы);

– на основе полученной информации можно прежде всего сформировать группу клиентов с наиболее крупными дебетовыми и кредитовыми оборотами по расчетному счету, так как наибольшие риски для банка в области ПОД/ФТ генерируют компании со значительными объемами платежей;

– исходя из даты регистрации компании в выборку должны попасть как вновь созданные компании (например, в данном анализируемом периоде), так и компании, работающие несколько лет и более;

– важное значение для аудитора, по нашему мнению, имеет информация о закрытии счета в банке (если такое событие было); как показывает практика, вновь открывшие счета компании зачастую проводят операции, имеющие признаки сомнительных, на десятки или даже сотни миллионов рублей в течение нескольких месяцев работы, а потом свертывают свою деятельность в данном банке либо по собственной инициативе, либо под воздействием предпринимаемых банком мер в целях ПОД/ФТ, причем в ходе аудиторских проверок выясняется, что банки зачастую не направляют сообщения об операциях такой категории клиентов: то ли не успев завершить проводимый анализ и квалификацию данных операций как сомнительных до закрытия счета, то ли успокаиваясь тем фактом, что раз клиент счет закрыл, то проблема решена (об операциях «бывших» клиентов банк не обязан направлять сообщения в Росфинмониторинг). По нашему мнению, такая категория «кочующих» из банка в банк клиентов представляет серьезную опасность для экономики страны, так как непредставление сведений об их операциях в Росфинмониторинг позволяет таким клиентам существовать довольно длительный период, нанося экономике значительный ущерб вследствие использования схем уклонения от налогов, вывода капитала за рубеж и т.п.;

– для формирования репрезентативной выборки имеет важное значение дополнительная информация, которую можно получить из информационной сети Интернет, в частности, из такого информационного ресурса как СПАРК-Интерфакс, с помощью ИНН клиента. В течение нескольких минут можно получить первоначальное мнение о предполагаемой для выборки компании: являются ли ее учредители и руководители массовыми или нет, является ли ее адрес регистрации массовым или нет, какова ее сфера и направления деятельности, данные бухгалтерской (финансовой) отчетности и т. п. Такой подход целесообразно применять для решения вопроса о включении или невключении одной или нескольких компаний в аудиторскую выборку.

Этап 2. На основе информации, полученной в запрашиваемом формате, производится выборка, взвешенная по стоимости (оборотам по счетам), что позволяет аудитору сосредоточиться на анализе клиентов, активно проводящих операции с крупными объемами денежных средств (используется метод произвольного отбора элементов с тем, чтобы в отобранную совокупность элементов попали также клиенты с другими признаками:

– новые компании, зарегистрированные в анализируемом периоде;

– клиенты, закрывшие счета в анализируемом периоде;

– индивидуальные предприниматели, которые наряду с корпоративными клиентами относятся к группе юридических лиц).

В результате вышеуказанных аудиторских процедур формируется выборка «новых клиентов» с позиций ПОД/ФТ, отражающая следующие основные моменты:

– клиенты с большим платежным оборотом;

– вновь зарегистрированные клиенты;

– клиенты с бизнес-опытом и отчетностью, созданные в прошлые годы;

– клиенты, закрывшие счета в анализируемом периоде;

– индивидуальные предприниматели.

Выборка «старых клиентов»

Для формирования данной выборки используется внутрифирменная методика, которая реализуется с применением внутрифирменного программного обеспечения с задаваемыми аудитором определенными параметрами, такими как аудиторский риск, неотъемлемый риск, риск управления, риск необнаружения, уровень доверия, уровень существенности и др.

Вышеуказанная методика базируется на следующих основах:

– выборка осуществляется на базе оборотно-сальдовой ведомости Банка в разрезе лицевых счетов;

– выборка – монетарная, т.е. каждый денежный элемент на счетах генеральной совокупности имеет равновероятную возможность быть отобранным для проверки;

– выборка формируется комбинированная, включающая лицевые счета, существенные как с точки зрения существенности их остатков, так и существенности их оборотов.

Сформированная таким способом в Excel выборка из нескольких десятков клиентов требует определенной корректировки аудитора на проверку наличия в ней уже отобранных «новых клиентов» или хорошо известных «старых» клиентов,

деятельность которых проверялась аудитором, например, в ходе предыдущей проверки (руководствуясь собственным многолетним опытом, отмечаем, что вероятность проведения стабильно работающими крупными компаниями операций, подпадающих под признаки ПОД/ФТ, является незначительной). На окончательный выбор аудитора может также повлиять информация, полученная аудитором в ходе проверки других направлений деятельности банка, например, кассовых операций, операций с ценными бумагами, валютных операций и др.

Таким образом, используя метод произвольного отбора из предварительно сформированной выборки, возможно, по нашему мнению, сократить число «старых клиентов» для выборки до 10–15 (как показывает практика, аудит такого количества «старых клиентов» для мелких и средних банков оказывается вполне достаточным для формирования выводов об операциях всей генеральной совокупности «старых клиентов» (которые, как правило, также ранее проверялись службами банка по ПОД/ФТ и внутреннего аудита). Для некоторых банков весьма актуальным является включение в выборку клиентов-нерезидентов, масштабы и характер операций которых имеют существенное значение для деятельности банка в целом.

После получения запрошенных документов и информации аудиторская проверка начинается с ознакомления с организационными основами внутреннего контроля в целях ПОД/ФТ, устанавления степени соответствия организационной структуры контроля особенностям бизнеса, характеру деятельности, клиентской базе, осуществляемым операциям. Кроме того, аудитор изучает порядок взаимодействия структурных подразделений банка по вопросам реализации ПВК в целях ПОД/ФТ. Основными факторами риска данного элемента внутреннего контроля в целях ПОД/ФТ являются прямые нарушения законодательства или ведомственного акта, такие как отсутствие необходимых документов, а также выявленные при проверке несоответствия фактического регламента финансового мониторинга утвержденному.

На современном этапе реализации противолегализационного законодательства крайне редко выявляются *организационные нарушения,* которые были характерны для первоначального этапа становления работы по ПОД/ФТ, в частности:

– неправомерность назначения на должность Ответственного сотрудника по ПОД/ФТ лица, являющегося одновременно руководителем структурного подразделения банка (Операционного отдела, Отдела валютного контроля, Службы безопасности и др.);

– некорректные должностные инструкции Ответственного сотрудника по ПОД/ФТ (сотрудников подразделений по ПОД/ФТ);

– отсутствие приказа о назначении лица, временно исполняющего обязанности Ответственного сотрудника по ПОД/ФТ, на период его отсутствия по уважительной причине (отпуска, болезни);

– назначение на должность Ответственного сотрудника по ПОД/ФТ (лица, временно исполняющего его обязанности) сотрудника, не отвечающего квалификационным требованиям, предъявляемым нормативными актами Банка России;

– несвоевременное утверждение актуальной редакции правил по ПОД/ФТ, учитывающей последние изменения в законодательстве и нормативных актах Банка России;

– включение в перечень подразделений банка, сотрудники которых должны проходить обязательное ежегодное обучение по ПОД/ФТ, не всех соответствующих подразделений согласно нормативным требованиям Банка России;

– непроведение либо несвоевременное проведение инструктажей или проведение их не для всех сотрудников;

– нарушения в формировании личных дел сотрудников в части ПОД/ФТ (отсутствие документов, подтверждающих проведение вводного (первичного) инструктажа по ПОД/ФТ, других документов по обучению по ПОД/ФТ).

(Продолжение следует)

Список литературы

1. Федеральный закон от 7 августа 2001 года № 115-ФЗ «О противодействии легализации (отмыванию) доходов, полученных преступным путем, и финансированию терроризма».

2. Федеральный закон от 10 июля 2002 года № 86-ФЗ «О Центральном банке Российской Федерации (Банке России)».

3. Послание Президента Федеральному Собранию, 1 декабря 2016 года. – URL: http//www.kremlin.ru

4. Положение Банка России от 2 марта 2012 года № 375-П «О требованиях к Правилам внутреннего контроля кредитной организации в целях противодействия легализации (отмыванию) доходов, полученных преступным путем, и финансированию терроризма».

5. Международные стандарты аудита (МСА) на русском языке. – URL: http://www.ifac.org

6. Core Principles for Effective Banking Supervision. Basel Committee on Banking Supervision. September 2012. – URL: http://www.bis.org

7. International Standards on Combating Money Laundering and the Financing of Terrorism & Proliferation. The FATF Recommendations. FATF. February 2012. – URL: http://www. fatf-gafi.org

УДК 336.71

В. Ю. БЕРЕГОВОЙ,
начальник отдела коммуникаций и IT
ООО «Внешаудит консалтинг»

Киберпреступность в финансовой сфере в России

Статья посвящена внедрению антифрод-систем в банках, совершенствованию нормативных и методических документов, проблемам технической защиты информации и их решения.

The article is devoted to the implementation of antifraud systems at banks, improve the regulatory and methodological documents, problems of technical protection of information and their solutions.

Ключевые слова: кибермошенничество, антифрод, банки, информационная безопасность, социальная инженерия, Банк России, FinCERT.

Key words: cyber fraud, antifraud, banks, information security, social engineering, the Bank of Russia, FinCERT.

В России в современных условиях борьба с киберпреступностью стала одним из ключевых приоритетов. На всех крупнейших форумах за последние два года в своих выступлениях глава Банка России Эльвира Набиуллина уделяет этим проблемам первоочередное внимание. Приведем выдержки из двух последних.

«Мы должны все вместе повысить защищенность нашей финансовой системы от такого рода преступлений. Современные технологии усугубляют данные риски», – подчеркнула Эльвира Набиуллина на итоговом заседании XIV Международного банковского форума «Банки России – XXI век» в Сочи 9 сентября.

«Угроза будет возрастать, и легкомысленно к киберпреступности относиться нельзя». Ранее Эльвира Набиуллина предупредила банки о возможном «попадании в ловушку» в связи с развитием финансовых технологий. «Для банковской индустрии это, конечно, огромнейший вызов. И здесь, мне кажется, банки могут попасть в ловушку, потому что в основном они сейчас жалуются на что? На низкие процентные ставки, на жесткое регулирование, на несправедливое регулирование по сравнению с параллельными банковскому секторами и так далее. А в это время сзади незаметно подкрались финансовые технологии. И это основной вызов, на который банкам нужно обращать внимание» (из выступления на форуме Finopolis 2016 в Казани 13 октября).

Рассмотрим более детально причины, угрозы, масштабы и средства борьбы.

Трансформация финансового рынка – это трансформация бизнес-моделей. Это касается не только банков, которые становятся также финтехкомпаниями, но и всех компаний, которые сегодня выходят на рынок с предложениями финансовых услуг.

Европейский Центральный банк признал, что определенный перечень банковских услуг может оказываться и небанками. Конкуренция в финансовом секторе повышается, в Европе решили допустить больше участников к предоставлению финансовых услуг. В результате стоимость услуг для потребителя должна понизиться, а оперативность их предоставления повыситься. Банк России изучает этот опыт, в котором есть много как плюсов, так и минусов, но очевидно, что это устойчивый тренд.

Еще один мировой тренд – все крупные игроки уходят в дистанционные услуги. Американские банки в 2016 году закрывают офисы сотнями. Только Bank of America, Citigroup и JP Morgan ликвидировали за год 389 банковских офисов. Три четверти карточных счетов в американских банках открывается через цифровые каналы, 18% всех трансакций на депозитах совершается через мобильные устройства.

Новые тренды. Даже анализ новостных заголовков последних полутора лет показывает, что сейчас формируется новый вектор страха – перед организованным хакерским сообществом и «серыми зонами» сети Интернет. Понимание, что в новости попадает только видимая часть айсберга, позволяет уверенно говорить о новом стимуле развития информационной безопасности – противодействии киберпреступности.

Что же изменилось за последнее время в действиях внешних злоумышленников и как правильно их называть? Вместо того чтобы вступать в долгие лингвистические споры о терминологии (APT или таргетированные атаки, массовые они или индивидуальные, являются данные атаки новыми или реализуют давно известные алгоритмы и т.д.), хотелось бы отметить несколько трендов.

• Действия злоумышленников стали очень сфокусированными. В атаках прослеживается четкая ориентация на прямую (вывод средств) или косвенную (похищение информации) монетизацию затраченных усилий.

• Практически все атаки используют самый слабый элемент в структуре защиты — человеческий фактор. Социальная инженерия является основным и самым эффективным инструментом доставки вредоносного кода и получения контроля над сетью, что сводит на нет длительные усилия по выстраиванию периметровой защиты организации (но, конечно, не умаляет их значимости и необходимости).

• Сфера киберпреступности расширилась. Эта «профессия» становится все более доступной: чтобы получить возможность использовать вредоносные программы, достаточно желания и небольшого количества времени. Не нужно быть супергением, как того требовалось несколько лет назад. Мошенники выработали бизнес-модель «Crime-as-a-Service» («преступление как сервис») и предоставляют разного рода услуги всем желающим. Соответствующие инструменты продаются практически в открытом доступе. Одни специалисты создают такие средства, другие модифицирует их для того, чтобы сигнатурные базы не умели их опознавать. Отдельные группы отвечают за тестирование инструментов, за их эксплуатацию, внедрение в ИТ-инфраструктуры компаний. Наконец, есть люди, которые проводят атаки, а также те, кто обналичивает полученные таким образом денежные средства. Каждое звено в этой длинной цепочке понимает, за что работает и какую прибыль получает, это является неплохим стимулом к развитию «черного» киберрынка и созданию высокоорганизованной системы взаимодействия.

• Сегодня у каждого крупного банка есть многофункциональный интернет-банк и как обязательное дополнение к нему — мобильное приложение для удобства клиентов. Но это же предоставляет дополнительные возможности для мошенников. Если раньше для доступа к банковским ресурсам использовались защищенные, «тяжелые» компьютеры, то сейчас — гаджеты, исключающие применение даже двухфакторной аутентификации. Последствия таковы: злоумышленники сравнительно легко могут перехватить управление устройством и получить доступ к финансовым потокам, к данным платежных карт и т. д.

События 2016 года заставили обратить внимание на вопросы защиты от атак на АРМ КБР (автоматизированные рабочие места клиентов Банка России), уязвимости автоматизированных банковских систем и ПО банкоматов. Среди новых способов выявлены DDoS-атаки на банки с использованием незащищенных устройств «интернета вещей». Опасность таких атак заключается в том, что они могут быть очень продолжительными. Прогнозируется рост несанкционированных вторжений в P2P-переводы.

Оценивая риски, следует ориентироваться не столько на защищенность конкретного «софта», сколько на защищенность банковских процессов. Основная проблема кроется в слабой защищенности процессов передачи информации внутри банков.

Еще один опасный тренд — массовое заражение клиентов банков, например, с помощью подложных писем. Привыкнув получать большое количество предложений различных услуг, клиенты зачастую не глядя открывают письма и вложения, присланные от имени банка.

Рассылка SMS-сообщений на мобильные телефоны является самой часто используемой атакой. Пользователь получает стандартное сообщение: «Ваша карта заблокирована», с ней подпись «Служба безопасности Банка России» и телефон для обратной связи. При звонке по указанному в сообщении номеру отвечают мошенники, цель которых весьма проста — сбор персональной информации граждан, а именно таких данных как: фамилия, имя, отчество, адрес, паспортные данные, номер банковской карты, PIN-код, CVV-код карты и т. д.

Также иногда владельцу карты предлагают пройти к банкомату и совершить какие-то операции якобы в целях проверки работоспособности карты. Даже если в процессе преступникам и не удастся ничего украсть с карты держателя, его персональная информация, полученная обманным путем, хорошо продается на теневом рынке.

Банк России за последнее время провел достаточно большой объем работ и подготовил ряд инновационных поправок и новых документов, относящихся к обеспечению информационной безопасности. В проектах новых регламентов, разработанных совместно с Минфином, предусмотрены существенные изменения, затрагивающие действующее Положение № 382-П, а также Федеральный закон № ФЗ-161 в рамках противодействия кибератакам и мошенничеству в финансовой сфере с использованием информационных технологий. Помимо антифрод деятельности Банк России также усиливает влияние ведомственного FinCERT (Центр мониторинга и реагирования на компьютерные атаки в финансовой сфере).

Минфин России совместно с Банком России разработал проект документа рекомендаций в области стандартизации Банка России РС БР ИББС-2.X-20XX «Предотвращение переводов денежных средств без согласия клиента (антифрод)», в котором банкам даются полномочия блокировать платежи клиентов, если у них возникнет подозрение, что к платежному процессу причастны хакеры. В на-

стоящий момент законопроект находится на рассмотрении в Государственной Думе. Ознакомиться с проектом документа можно на официальном сайте ТК122 в разделе документы.

В числе наиболее значимых новаций, которые предлагаются в проекте документа, стоит отметить механизм приостановки платежа. Он активизируется в том случае, если есть существенные подозрения, что банк-отправитель или клиент банка были атакованы хакерами. Денежный перевод в этом случае может быть осуществлен только тогда, когда сам клиент подтвердит его легитимность.

Даже если в результате хакерской атаки платеж все-таки был отправлен, законопроект предусматривает действия по возврату незаконно выведенных средств. Минфин опубликовал на официальном портале размещения документов ряд поправок к Федеральному закону № ФЗ-161 «О национальной платежной системе». К примеру, поправка к ст. 9 закона гласит, что банк обязан вернуть средства, если клиент не пропустил срок для оспаривания операции (один день) и если банк не докажет нарушение условий пользования картой. Новые поправки дают банку право приостанавливать на два дня транзакции или блокировать карту, если есть подозрение, что операция совершается без согласия клиента, причем даже при условии, что был введен верный пин-код или использована реальная электронная подпись. При приостановлении операций клиенту направляется запрос, согласен ли он с операцией. Ответ на него и будет определять, проведет ее банк или нет.

FinCERT становится обязательным. Регулятор разработал четкий и обязательный для всех банков регламент кибербезопасности, призванный защитить кредитные организации от хакерских атак. В документе, в частности, вводится обязанность банка в течение трех часов сообщать о готовящейся или свершившейся атаке в FinCERT (ранее отправка данных в FinCERT носила рекомендательный порядок).

Проект положения «О требованиях к защите информации в платежной системе Банка России» был опубликован 1 августа на сайте Банка России. Основная новация состоит в том, что ЦБ РФ установил четкую обязанность банков информировать FinCERT о всех выявленных и потенциально готовящихся инцидентах, связанных с нарушением требований к обеспечению защиты информации при переводе средств через платежную систему Банка России, в том числе о несанкционированных переводах денежных средств. Срок информирования определен в течение трех часов с момента инцидента или выявления нарушения доступа к информации.

Отправлять сообщения банки обязали на электронную почту fincert@cbr.ru вне зависимости от того, участвует банк в информационном обмене с FinCERT или нет. В соответствии с проектом положения банки должны обеспечить исполнение указанных требований не позднее чем к 30 июня 2017 года. «В свете участившихся угроз мы сочли необходимым разработать и обнародовать документ, регламентирующий требования безопасности для всех участников платежной системы» — официальное заявление из пресс-службы ЦБ РФ. Теперь тем, кто будет игнорировать данное требование, грозит наказание. Банк России может применить к банкам, не исполняющим его нормативные акты, ответственность, прямо предусмотренную ст. 74 закона «О Центральном банке». Это может быть и штраф до 1% от размера уставного капитала, и ограничение определенных операций, и другие довольно строгие меры, вплоть до отключения от системы банковских электронных срочных платежей (БЭСП) в отдельных случаях. Четкий порядок действий в случае атаки будет определен «договором информационного обмена» с каждым банком в отдельности.

Собирая информацию из банков, FinCERT получает возможность способствовать тому, что деньги, которые злоумышленники уже вывели из банка, могут быть оперативно остановлены на стороне банка-получателя. Также по итогам взаимодействия с Координационным центром национального домена сети Интернет блокируются домены в Иинтернете, на которых расположены ресурсы, представляющие угрозу. Это подделки (фишинг) под сайты кредитных организаций, ресурсы, где размещается недобросовестная реклама финансовых услуг. К примеру, меньше чем за полгода по обращениям FinCERT было заблокировано свыше 180 ресурсов.

Задача FinCERT — анализировать все поступающие данные и выявлять инциденты. Далее обработанные данные обобщаются и уходят участникам информационного обмена в виде бюллетеней. Вся информация обезличена. Из рассылки FinCERT невозможно почерпнуть информацию, в каком банке что произошло. Гарантированно не создаются репутационные риски для тех, кто с FinCERT делится информацией.

Банк России волен формировать и вести базу данных о случаях совершения перевода денежных средств без согласия клиента, следует из законопроекта.

Рекомендации по критериям подозрительности операций также будут, они уже в стадии подготовки ЦБ РФ. Как сообщили в пресс-службе Банка России, «проект рекомендаций в области стандартизации проходит процедуру обсуждения в рамках подкомитета 1 «Безопасность финансовых (банковских) операций» технического комитета 122 «Стандарты финансовых операций», в состав которого входят кредитные и некредитные финансовые организации, а также организации, оказывающие профес-

Рис. 1. От кого банки узнают об атаках, в %

сиональные услуги в области обеспечения информационной безопасности». Рекомендации взаимосвязаны с текстом законопроекта, текущая их редакция подготовлена представителями банковского сообщества с учетом мнения Банка России.

FinCERT образован 1 июня 2015 года. Опубликован годовой отчет о деятельности центра (с 1 июня 2015 года по 31 мая 2016 года), в котором содержится информация о сотрудничестве с кредитными организациями, а так же самых распространенных угрозах и способах противодействия им. С полной версией отчета можно ознакомиться на официальном сайте.

Банком России выявлено 23 крупных покушения на хищения денежных средств в 2016 году на общую сумму около 3 млрд руб. Всего же за год общая сумма потенциальных потерь денежных средств, с учетом предварительной статистики по коммерческим банкам, оценивается в 5,2 млрд руб. Однако эти цифры будут еще уточняться регулятором по итогам 2016 года.

Как следует из других официальных источников, эффективность борьбы банков с растущим числом таких мошенничеств пока еще низка. Только в январе-сентябре 2016 года хакеры пытались совершить с помощью платежных сервисов 102,7 тыс. несанкционированных операций со счетами физлиц, тогда как за аналогичный период 2015 года таких попыток было зафиксировано всего 16 тыс. При этом ущерб частным клиентам от действий мошенников за три квартала этого года составил около 1,25 млрд руб. Как свидетельствует статистика, банкам и регулятору в 2016 году удалось предотвратить хищение не более чем 2–3% средств.

Банк России подготовит национальные стандарты информационной безопасности. В конце сентября 2016 года первый заместитель Председателя Банка России Георгий Лунтовский информировал о том, что Банк России ведет работу по подготовке таких национальных стандартов по информационной безопасности (ИБ), на основе которых будет создан ГОСТ, который станет обязательным для соблюдения всеми участниками финансового рынка с 2017 года.

На данный момент многие кредитные организации проводят оценку соответствия на выполнение требований по информационной безопасности (в первую очередь – стандарта СТО БР ИББС1 и Положения № 382-П) самостоятельно в форме «Самооценки», зачастую результаты таких самооценок являются высокими. В 2016 году значительно вырос уровень инцидентов, связанных с информационной безопасностью в кредитных организациях, о чем свидетельствуют документы FinCERT. Соответственно, высокий уровень «Самооценок по ИБ», проводимых самостоятельно кредитными организациями, противоречит информации, полученной из открытых источников, по инцидентам ИБ.

Как показывает практика, преступники изучают любые рекомендации, находящиеся как в открытом, так и в ограниченном доступе, причем изучают чуть ли не внимательнее, чем сами специалисты по информационной безопасности в банках. Ярким примером может служить атака на банки, выполненная в виде очередной рассылки FinCERT и вызвавшая резонанс в банковском сообществе и в СМИ. Фальшивая рассылка была осуществлена не по адресам участников FinCERT, но по базе так называемого Клуба антидропперов. Эта атака в числе прочего продемонстрировала, что злоумышленники более чем внимательно читают все рассылки FinCERT, это следует в том числе из скрупулезно скопированной в фальшивых письмах стилистики и вводных данных, что позволило ввести в заблуждение более 400 банков, ставших целями атаки, и внедрить в их системах вредоносный вирус. Одновременно перед нами наглядный пример надлежащего уровня подготовки «специалистов по ИБ» в банках в 2016 году.

Появление обязательных для исполнения кредитными организациями документов должно положительно отразиться на повышении уровня ИБ в кредитных организациях. Недавно был принят Федеральный закон № 162-ФЗ «О стандартизации в Российской Федерации», по которому с 1 июля 2016 года национальный стандарт, определяющий требования по защите сведений ограниченного доступа (для кредитных организаций – в первую оче-

редь защита банковской тайны), является обязательным для исполнения. Это позволит установить ответственность за невыполнение требований по информационной безопасности, в том числе путем применения меры воздействия. Невыполнение этих требований ведет к серьезным проблемам с ликвидностью и собственным капиталом финансовых организаций.

В новых стандартах будет сделан упор на обязательность, например, проведения тестов на проникновение, то есть в сторону реальной практической безопасности, в предполагаемом ГОСТе будут даны базовые определения таким угрозам, как спам, скимминг, фишинг и другим.

Кроме того, недавно было подписано распоряжение о введении стандарта по расследованию инцидентов информационной безопасности. Этот документ, подготовленный совместно Банком России, МВД, ФСБ, Следственным комитетом при участии ряда кредитных организаций, призван помочь банкам правильно собирать необходимую для расследования доказательную базу, а правоохранительным органам — быстрее ее получать.

Еще одна инициатива ЦБ РФ — создание собственной лаборатории по компьютерной криминалистике. Лаборатория аккумулирует в себе компетенции Банка России в области как технических вопросов, так и вопросов проведения банковских операций. При ее создании учитывается международный опыт и практика взаимодействия с правоохранительными органами.

Вектор атак на SWIFT. В 2016 году зафиксированы первые хакерские атаки российских банков через систему межбанковских коммуникаций SWIFT. По данным СМИ, кибермошенники увели из пострадавших банков около 2 млн евро. Эксперты уверены, что в дальнейшем ущерб от краж денег через SWIFT будет расти.

Технически схема кибератаки на систему Society for Worldwide Interbank Financial Telecommunications (SWIFT) по своей сути не отличается от атаки на стандартные корсчета банков. Мошенники используют вредоносное ПО для проникновения в корпоративную сеть и дальнейшего взлома АБС кредитной организации (в данном случае — SWIFT). Чаще всего через рассылку фишинговых писем. После проникновения идет захват информационной инфраструктуры банка — злоумышленники начинают управлять АБС банка, им становится доступна информация обо всех операциях банка, частоте и объеме транзакций, остатке по корсчету. Хакеры «сидят» таким образом в сети банка неделю, максимум две. Затем готовятся к операции по выводу (обналичиванию) похищенных средств, формируются фальшивые документы о списании средств с корсчета, заверяемые легальными подписями ответственных лиц банка. Платежные поручения направляются в платежную систему, для которой это легальный платежный документ, поэтому она обязана его исполнить в соответствии с договором и законодательством.

По прогнозам представителя Positive Technologies, кибератак на российские банки через SWIFT в 2017 году «точно станет больше».

Таким образом у крупных банков есть ресурсы, чтобы заниматься безопасностью на системном уровне. У небольших банков таких ресурсов нет и не будет в ближайшее время, даже если их начнут наказывать за нарушение требований информационной безопасности. Ответом на это может стать аутсорсинг безопасности. Предполагается обычный путь: сначала будут выработаны рекомендации, потом что-то из этих рекомендаций станет частью стандарта, а потом уже что-то будет включено в нормативный документ. Первые документы Банк России предполагает представить к очередному Уральскому форуму по информационной безопасности в начале 2017 года.

Источники

1. Материалы VII Международного форума по борьбе с кибермошенничеством AntiFraud Russia 2016 (1 декабря 2016 года, Москва).
2. Материалы XIII Международной выставки InfoSecurity Russia 2016 (20–22 сентября 2016 года, Москва).
3. Материалы VIII Уральского форума «Информационная безопасность финансовой сферы» (16–20 февраля 2016 года, Республика Башкортостан).

УДК 336.2

С. В. БРОВКИН,
генеральный директор ООО «Макс-Аудит»

Актуальные вопросы налогообложения

В статье описаны изменения в налоговом законодательстве, вступающие в силу с 1 января 2017 года, а также вопросы о возможности вычета НДС по объектам основных средств, не введенных в эксплуатацию.

This article describes the changes in the tax laws that come into force on 1 January 2017, as well as questions about the deductibility of VAT on fixed assets are not put into operation.

Ключевые слова: изменения, налог на прибыль, налоговый учет, новый классификатор, налоговая база, ценные бумаги, вычет НДС, основные средства.

Key words: change, income tax, tax accounting, the new classifier, the tax base, securities, deduction of VAT, fixed assets.

Проанализировав изменения в области налога на прибыль, вступающие в силу с 1 января 2017 года, можно прийти к выводу, что наиболее существенными из них являются:

- введение нового классификатора основных средств;
- изменения в области критериев контролируемой задолженности;
- пополнение списка расходов затратами на оценку квалификации работников.

Также планируются некоторые другие нововведения, связанные с отдельными отраслями и видами деятельности. Остановимся на каждом моменте для более детального анализа.

Новый классификатор ОКОФ. С 1 января 2017 года организации будут определять амортизационные группы и сроки амортизации для ОС по новому классификатору основных средств.

На данный момент действует классификатор основных средств ОКОФ ОК 013-94, утвержденный Постановлением Госстандарта РФ от 26 декабря 1994 года № 359.

С 2017 года вступит в силу новый классификатор ОК 013-2014 (СНС 2008), утвержденный Приказом Росстандарта от 12 декабря 2014 года № 2018-ст.

Благодаря новому ОКОФ не только начнут применяться новые коды классификации, но и изменятся амортизационные группы для некоторых основных средств, что, в свою очередь, повлечет за собой изменение срока их полезного использования.

Соответствие между старыми и новыми кодами ОКОФ устанавливает Приказ Росстандарта от 21 апреля 2016 года № 458.

Внимание! Для основных средств, введенных в эксплуатацию до 1 января 2017 года, не нужно будет пересчитывать норму амортизации, даже если согласно новому классификатору данные ОС будут относиться к другой амортизационной группе. При этом для тех основных средств, которые будут введены в эксплуатацию с 1 января 2017 года, налогоплательщики будут обязаны применять амортизационные группы и сроки полезного использования согласно новому справочнику.

Налоговый учет контролируемой задолженности. С 1 января 2017 года Федеральным законом от 15 февраля 2016 года № 25-ФЗ будут внесены существенные изменения в ст. 269 НК РФ. Изменятся критерии признания задолженности российской компании контролируемой, проценты по которой, как известно, в целях налогообложения подлежат нормированию.

В результате количество ситуаций, при которых задолженность может быть признана контролируемой, существенно увеличится.

С начала 2017 года размер контролируемой задолженности будет рассчитываться исходя из совокупности всех обязательств налогоплательщика, которые обладают признаками такой задолженности.

Кроме того, Закон № 25-ФЗ внесет уточнения в п. 4 ст. 269 НК РФ. В соответствии с ним, в случае изменения коэффициента капитализации в последующем отчетном периоде или по итогам налогового периода по сравнению с предыдущими отчетными периодами предельный размер процентов, подлежащих включению в состав расходов, по контролируемой задолженности за предыдущий отчетный период изменению не подлежит.

(Коэффициент капитализации зависит от суммы долга, величины собственного капитала заемщика и доли участия иностранной компании, контролирующей задолженность, в его капитале.)

Затраты на независимую оценку квалификации. С 2017 года вступает в силу Закон о независимой оценке квалификации работников. Чтобы мотивировать работодателей на проведение оценки,

законодатели приняли решение внести изменения в ст. 264 НК РФ. В результате затраты на проведение независимой оценки будут учитываться в расходах при исчислении налога на прибыль (дополнения к пп. 23 п. 1 ст. 264 НК РФ вносит Федеральный закон от 3 июля 2016 года № 251-ФЗ).

Новое в применении коэффициента ускоренной амортизации. Согласно Закону № 144-ФЗ с 1 января 2017 года плательщики налога на прибыль – участники специальных инвестиционных контрактов смогут применять коэффициент ускоренной амортизации (не выше 3) в отношении амортизируемых основных средств, включенных в I–VII амортизационные группы. Порядок отнесения амортизируемых основных средств к произведенным в соответствии с условиями специального инвестиционного контракта будет определять Правительство РФ.

Налоговая база по операциям с ценными бумагами. С 1 января 2017 года уточняется порядок определения налоговой базы по операциям с ценными бумагами.

В частности, Законом № 242-ФЗ в ст. 280 НК РФ вводится пункт 30. Теперь по облигациям российских организаций, условиями выпуска и обращения которых предусмотрено получение дохода в виде процентов, подлежащих налогообложению по налоговой ставке, предусмотренной пп. 1 п. 4 ст. 284 НК РФ (15%), при обращении которых в цену сделки включается часть накопленного купонного дохода, при исчислении общей налоговой базы не будет учитываться начисленный купонный доход, по которому применяется указанная налоговая ставка.

Рассмотрим вопрос о возможности вычета «входного» НДС по объекту, учтенному на счете 08 «Вложения во внеоборотные активы», когда по каким-либо причинам он не введен в эксплуатацию.

Предположим, что налогоплательщик приобретает объект основных средств как резервное (запасное) оборудование, например, на случай поломки действующего основного средства. Приобретенные объекты могут находиться в резерве (на складе) длительное время. Такое «резервное» оборудование учитывается на счете 08 «Вложения во внеоборотные активы» до того момента, пока оно не будет введено в эксплуатацию с отражением на счете 01 «Основные средства». В нашем примере находящееся на складе оборудование будет введено в эксплуатацию в случае поломки действующего основного средства. Вправе ли налогоплательщик принять к вычету НДС по приобретенному «будущему» основному средству на дату отражения на счете 08, или же к вычету НДС принимается только на дату ввода объекта в эксплуатацию?

Вычет НДС по приобретенному объекту (ОС). Основанием для принятия «входного» НДС к вычету является выполнение ряда условий, приведенных в ст. 171, 172 Налогового кодекса (далее – Кодекс).

Одним из условий применения вычета сумм НДС, предъявленных налогоплательщику при приобретении основных средств, является «принятие на учет данных основных средств» (абз. 3 п. 1 ст. 172 НК РФ).

Как мы видим, в п. 1 ст. 172 Кодекса прямо не сказано, на каком счете должно быть учтено имущество, которое будет использоваться в качестве основного средства. Не определено в Кодексе и само понятие «принятие на учет». Тем самым приведенная формулировка допускает в том числе и следующее толкование: право на получение вычета по НДС при приобретении внеоборотных активов, не требующих монтажа, возникает в момент их постановки на бухгалтерский учет в качестве объектов основных средств на счет 01 «Основные средства» (или 03 «Доходные вложения в материальные ценности»). Принимая во внимание, что отражение объекта на счете 01 «Основные средства» правомерно только после ввода его в эксплуатацию, можно сделать следующий вывод: если объект числится в бухгалтерском учете на счете 08, предъявить «входной» НДС к вычету по нему нельзя.

Именно такого подхода придерживаются контролирующие органы в отношении приобретенных основных средств. По их мнению, для вычета НДС необходимо, чтобы объект был принят к учету в качестве основного средства (письма Минфина России от 12 декабря 2015 года № 03-07-11/6141, от 29 января 2013 года № 03-07-14/06, от 24 января 2013 года № 03-07-11/19, от 28 августа 2012 года № 03-07-11/330, от 16 августа 2012 года № 03-07-11/303).

В судебной практике встречаются отдельные решения, в которых выражена аналогичная позиция (постановление ФАС ПО от 30 сентября 2010 года по делу № А12-24919/2009). Но в большинстве судебных споров судьи приходят к противоположному выводу (определение ВС РФ от 21 сентября 2015 года № 309-КГ15-11146; постановление ФАС ВВО от 13 мая 2014 года № Ф01-1266/14, ФАС ПО от 5 сентября 2013 года № Ф06-7762/13 по делу № А72-13061/2012 (определением ВАС РФ от 7 ноября 2013 года № ВАС-15354/13 отказано в передаче дела в Президиум ВАС РФ для пересмотра в порядке надзора), ФАС МО от 21 августа 2013 года № Ф05-7760/13). При этом они придерживаются иной трактовки тех же положений ст. 171, 172 Кодекса, отмечая, что законодатель не связывает право на вычет по НДС с датой ввода в эксплуатацию основного средства. Суды признают отражение на счете 08 «принятием на учет» и считают основанием для получения вычета по НДС. Причем

нередко такие решения суды выносили по заявлению налоговиков. Например, последние отказывали в вычете НДС в ситуации, когда с момента принятия объекта к учету на счете 08 до ввода в эксплуатацию (с отражением на счете 01) проходило более трех лет, а налогоплательщик при этом перестраховывался и принимал НДС к вычету на дату ввода объекта в эксплуатацию. Суды же в таких ситуациях указывали, что факт отражения стоимости приобретенных работ и товара на счете 08, а не на счете 01 не может служить основанием для увеличения срока, предусмотренного п. 2 ст. 173 Кодекса.

К примеру, в одном из судебных дел (определение ВС РФ от 21 сентября 2015 года № 309-КГ15-11146) рассматривалась такая ситуация. Налогоплательщик приобрел оборудование и в IV квартале 2009 года отразил его на счете 08 «Вложения во внеоборотные активы». На учет в качестве основного средства оборудование было принято в III квартале 2010 года. Считая, что 3 года отсчитываются от даты принятия на учет в качестве основных средств (то есть с III квартала 2010 года), налогоплательщик принял «входной» НДС к вычету во II квартале 2013 года. Но налоговая инспекция отказала в праве на вычет, поскольку он был предъявлен за пределами трехлетнего срока. Суд посчитал позицию налоговиков правомерной, указав, что трехлетний срок вычета НДС отсчитывается от IV квартала 2009 года, то есть с момента, когда объект был приобретен. Напомним, что чуть позже Минфин России в своем Письме от 20 ноября 2015 № 03-07-РЗ/67429 разъяснил: налоговые вычеты, предусмотренные п. 2 ст. 171 Кодекса, могут быть заявлены в налоговых периодах в пределах трех лет после принятия на учет приобретенных налогоплательщиком товаров (работ, услуг), имущественных прав (в соответствии с п. 1.1 ст. 172 НК РФ, вступившим в силу с 1 января 2015 года), а также что это положение относится и к основным средствам.

Вычет «входного» НДС, когда приобретенный объект ставят на ремонт. В этом же письме затронут вопрос о вычете НДС по приобретенному объекту недвижимости, который в связи с его предстоящим ремонтом и установкой оборудования был учтен на счете 08 (см. также Письмо Минфина России от 5 февраля 2016 года № 03-07-11/5851). По мнению Минфина России, в рассматриваемом случае вычет сумм НДС, предъявленного налогоплательщику при приобретении объекта недвижимости, производится после принятия на учет на счет 08 «Вложения во внеоборотные активы». В ходе своих разъяснений финансисты ссылаются на положения п. 2 ст. 171 и п. 1 ст. 172 Кодекса, согласно которым вычетам подлежат суммы НДС, предъявленные налогоплательщику при приобретении товаров (работ, услуг). Аналогичное мнение финансисты высказывали ранее, в Письме Минфина России от 16 июля 2012 года № 03-07-11/185. В нем речь также шла об объекте недвижимости, учтенном на счете 08, который был приобретен с целью реконструкции и дальнейшего использования в облагаемой НДС деятельности (в этом письме вывод был основан на норме п. 6 ст. 171 Кодекса, который регулирует порядок применения вычетов сумм НДС, предъявленных налогоплательщику подрядчиками, при приобретении объектов незавершенного капстроительства, а также по товарам, приобретенным для выполнения СМР).

Но изменилась ли позиция чиновников в отношении права на вычет НДС по приобретенным основным средствам в случае, когда налогоплательщик не планирует перед использованием их ремонтировать, реконструировать и т.п., но по каким-то причинам они не введены в эксплуатацию (учитываются на счете 08, но их стоимость уже сформирована)? Пока очередные разъяснения (письмо Минфина России от 30 июня 2016 № 03-07-11/38360) по применению п. 1 ст. 172 Кодекса в части вычета «входного» НДС по основным средствам дают отрицательный ответ на этот вопрос.

Источники

1. Федеральный закон РФ от 3 июля 2016 года № 242-ФЗ «О внесении изменений в статью 105.15 части первой и часть вторую Налогового кодекса Российской Федерации и признании утратившими силу отдельных положений законодательных актов Российской Федерации».
2. Налоговый кодекс РФ (с изменениями и дополнениями).
3. Письма Минфина России от 28 августа 2012 № 03-07-11/330, от 19 марта 2012 года № 03-03-06/4/20, от 16 июля 2012 года № 03-07-11/185, от 16 августа 2012 года № 03-07-11/303, от 24 января 2013 года № 03-07-11/19, от 29 января 2013 года № 03-07-14/06, от 12 февраля 2015 года № 03-07-11/6141, от 20 ноября 2015 года № 03-07-РЗ/67429, от 5 февраля 2016 года № 03-07-11/5851, от 30 июня 2016 года № 03-07-11/38360.
4. Письма УФНС России по г. Москве от 20 мая 2011 года № 16-15/049561@, от 30 марта 2005 № 19-11/20943@.
5. Письмо УМНС по г. Москве от 12 августа 2004 года № 26-12/52934.
6. Постановление ФАС ВВО от 13 мая 2014 года № Ф01-1266/14.
7. Постановление ФАС ПО от 5 сентября 2013 года № Ф06-7762/13.
8. Определение ВС РФ от 21.09.2015 № 309-КГ15-11146.

ЦЕНТРАЛЬНЫЙ БАНК РОССИЙСКОЙ ФЕДЕРАЦИИ
(БАНК РОССИИ)

СТАНДАРТ

Обеспечение информационной безопасности организаций банковской системы Российской Федерации

Сбор и анализ технических данных при реагировании на инциденты информационной безопасности при осуществлении переводов денежных средств

Дата введения: 1 января 2017 года

1. Область применения

Настоящий стандарт распространяется на организации БС РФ, реализующие функции операторов по переводу денежных средств или операторов услуг платежной инфраструктуры, и устанавливает рекомендации к организационным, технологическим и техническим подходам, связанным со сбором, обработкой, анализом и распространением (обменом) технических данных, в рамках деятельности по выявлению следующих типов инцидентов ИБ и реагированию на них:

– инциденты ИБ, информация о которых получена от клиентов операторов по переводу денежных средств (далее – клиентов), в том числе инциденты ИБ (события ИБ), выявленные клиентами, классифицированные клиентами как потенциальные попытки несанкционированных переводов денежных средств от их имени;

– инциденты ИБ (события ИБ), выявленные организацией БС РФ, классифицированные организацией БС РФ как попытки реализации угроз ИБ или как приготовление к их реализации;

– инциденты ИБ, информация о которых получена организацией БС РФ от Центра мониторинга и реагирования на компьютерные атаки в кредитно-финансовой сфере Банка России (далее – FinCert Банка России), а также иных организаций, например, операторов связи, провайдеров сети Интернет. Положения настоящего стандарта могут применяться организациями, не входящими в БС РФ, реализующими функции операторов услуг платежной инфраструктуры, банковских платежных агентов (субагентов).

В настоящем стандарте не рассматриваются рекомендации, направленные на обеспечение выявления несанкционированных переводов денежных средств на основе анализа реквизитов распоряжений на осуществление переводов денежных средств, в том числе рекомендации к правилам настройки автоматизированных систем, реализующим функции противодействия мошенническим операциям («системы антифрод»).

Настоящий стандарт не устанавливает рекомендации к реализации системы менеджмента инцидентов ИБ, в том числе не регламентирует процедуры обнаружения инцидентов ИБ и классификации отдельных событий ИБ или их групп в качестве инцидентов ИБ. В настоящем стандарте предполагается, что реализация системы менеджмента инцидентов ИБ осуществлена организацией БС РФ в соответствии с положениями РС БР ИББС-2.5. При этом настоящий стандарт развивает положения РС БР ИББС-2.5 в части сбора и анализа технических данных.

Настоящий стандарт рекомендован для применения путем включения ссылок на него и (или) прямого использования устанавливаемых в нем положений во внутренних документах организаций БС РФ, а также в договорах.

Положения настоящего стандарта имеют рекомендательный характер, если только в отношении отдельных положений обязательность их применения не установлена законодательством РФ, норма-

тивными правовыми актами, в том числе нормативными актами Банка России.

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

2. Нормативные ссылки

В настоящем стандарте использованы нормативные ссылки на следующие стандарты:

– СТО БР ИББС-1.0;

– РС БР ИББС-2.5;

– рекомендации в области стандартизации Банка России РС БР ИББС-2.6 «Обеспечение информационной безопасности организаций банковской системы Российской Федерации. Обеспечение информационной безопасности на стадиях жизненного цикла автоматизированных банковских систем» (далее – РС БР ИББС-2.6).

3. Термины и определения

В настоящем стандарте применяются термины в соответствии с СТО БР ИББС-1.0, РС БР ИББС-2.5, РС БР ИББС-2.6, а также следующие термины с соответствующими определениями.

3.1. Инцидент ИБ при осуществлении переводов денежных средств, Инцидент ИБ – событие ИБ или их комбинация, указывающие на свершившуюся, предпринимаемую или вероятную реализацию угрозы ИБ, результатом которой являются:

– несанкционированные переводы денежных средств, которые привели или могут привести к:

• осуществлению переводов денежных средств по распоряжению лиц, не обладающих правом распоряжения этими денежными средствами;

• несвоевременности осуществления переводов денежных средств;

• осуществлению переводов денежных средств с использованием искаженной информации, содержащейся в распоряжениях на осуществление переводов денежных средств (реквизитов платежей);

– деструктивные воздействия на информационную инфраструктуру, используемую для осуществления переводов денежных средств, которые привели или могут привести к нарушению непрерывности оказания платежных услуг.

3.2. Несанкционированный перевод денежных средств – перевод денежных средств лицами, не обладающими правом распоряжения денежными средствами.

4. Обозначения и сокращения

АБС – автоматизированная банковская система;

ИБ – информационная безопасность;

БС – банковская система;

ДБО – дистанционное банковское обслуживание;

НСД – несанкционированный доступ;

РФ – Российская Федерация;

СУБД – система управления базами данных;

СВТ – средство вычислительной техники;

СКЗИ – средство криптографической защиты информации.

5. Общие положения по организации процесса обработки технических данных в рамках реагирования на инциденты ИБ

5.1. В настоящем стандарте рассматриваются следующие группы рекомендаций по организации обработки технических данных при выявлении инцидентов ИБ и реагировании на них:

– рекомендации по сбору технических данных с компонентов информационной инфраструктуры, задействованных в осуществлении переводов денежных средств;

– рекомендации по проведению поиска (выделения) из собранных технических данных содержательной (семантической) информации, ее анализу и оформлению;

– рекомендации по распространению (передаче) выделенной и оформленной содержательной (семантической) информации;

– рекомендации по распределению зон ответственности подразделений организации БС РФ в рамках процесса обработки технических данных, включая анализ, оформление и распространение (передачу) содержательной (семантической) информации;

– рекомендации по взаимодействию с клиентами организации БС РФ в рамках процесса сбора технических данных;

– рекомендации по компетенции персонала организации БС РФ и (или) иных внешних организаций, задействованных в процессах обработки технических данных;

– рекомендации по обеспечению наличия технических данных на этапах создания и эксплуатации информационной инфраструктуры, используемой для осуществления переводов денежных средств или для обеспечения защиты информации при осуществлении переводов денежных средств.

5.2. При организации обработки технических данных рекомендуется соблюдать следующие общие принципы:

– любые выполняемые процедуры и сервисные команды обработки технических данных, реализуемые организацией БС РФ и (или) ее клиентами (в том числе процедуры сбора, хранения, передачи технических данных), не должны вносить

изменения в исходные технические данные и (или) их эталонные копии;

– сбор технических данных, поиск (выделение) из технических данных содержательной (семантической) информации, ее анализ должны проводиться лицами, обладающими необходимым опытом и компетенцией;

– выполнение всех процедур и сервисных команд обработки технических данных, реализуемых организацией БС РФ и (или) ее клиентами (в том числе процедуры и сервисные команды их сбора, хранения и передачи), должно сопровождаться выполнением процедур и сервисных команд, обеспечивающих возможность последующего контроля целостности (неизменности) технических данных;

– обработка технических данных должна сопровождаться описанием и протоколированием:

• всех выполняемых процедур и сервисных команд, использованных для сбора, сохранения и передачи технических данных. Реализация описания и протоколирования выполненных процедур и сервисных команд должна обеспечивать возможность их точного повторного выполнения;

• перечня использованных технических средств и инструментов, применяемых для сбора, сохранения и передачи технических данных, а также параметров их настройки;

• места, даты и времени[1] выполнения сбора, сохранения и передачи технических данных;

• места, даты и времени выполнения процедур и сервисных команд;

• идентификационных данных лиц, выполнивших процедуры и сервисные команды сбора, сохранения и передачи технических данных;

– обеспечение хранения указанных описаний и протоколов совместно с обрабатываемыми техническими данными, а также обеспечение их доступности для представления;

– обеспечение протоколирования действий по передаче копий собранных технических данных между лицами, участвующими в расследовании инцидентов ИБ, хранения указанных протоколов совместно с обрабатываемыми техническими данными, а также обеспечение их доступности для представления.

При наличии соответствующих знаний рекомендуется сопровождать выполнение процедур и сервисных команд обработки технических данных описанием и протоколированием ожидаемого изменения в состоянии информационной инфраструктуры (например, появления временных файлов, изменения даты и времени последнего обращения к файлу).

Описание возможного формата и содержания протокола выполнения процедур и сервисных команд обработки технических данных приведено в приложении А к настоящему стандарту. Пример протокола снятия криминалистической копии (создание образа) накопителя на жестких магнитных дисках приведено в приложении Б к настоящему стандарту.

Рекомендуется осуществлять указанные выше описание и протоколирование не менее чем двумя лицами.

5.3. Организация процесса обработки технических данных должна обеспечивать:

– сохранность и неизменность технических данных;

– относимость собранных и обрабатываемых технических данных к конкретному инциденту ИБ;

– доступность, целостность и конфиденциальность технических данных при их обработке.

При этом организация сбора технических данных должна быть организована с учетом возможности:

– изменения, повреждения и (или) уничтожения исходных технических данных;

– потери исходных технических данных с течением времени.

5.4. Обеспечение возможности контроля целостности (неизменности) технических данных в большинстве случаев может быть реализовано:

– использованием технических средств для вычисления контрольных сумм или значений хэш-функций исходных и копий технических данных с последующим:

• сравнением вычисленных значений для фиксации целостности данных;

• составлением акта с документированием полученного вычисления контрольной суммы или значения хэш-функций;

• обеспечением хранения акта совместно с обрабатываемыми техническими данными;

– документированием отдельных технических данных незначительного объема на бумажном носителе с:

• составлением акта о соответствии содержания задокументированных технических данных на бумажном носителе и исходных технических данных на машинном носителе;

• сшиванием документов с техническими данными и акта в единый пакет или их упаковкой в пакеты (контейнеры), обеспечивающие невозможность доступа без видимого нарушения целостности упаковки.

Рекомендуется осуществлять составление и заверение указанных актов не менее чем двумя лицами. Вычисление значений хэш-функций рекомендуется реализовывать в соответствии с ГОСТ Р 34.11-2102 [2].

[1] Здесь и далее рекомендуется протоколирование времени с указанием часового пояса.

5.4.1. Для собираемых технических данных рекомендуется обеспечить наличие как минимум четырех копий, одна их которых используется для последующей обработки и анализа, а остальные хранятся организацией БС РФ в неизменном (эталонном) виде для целей:

– возможной передачи в правоохранительные органы;

– возможной передачи в FinCert Банка России;

– собственного использования организацией БС РФ.

5.5. Особое внимание при распространении (передаче) технических данных и выделенной из них содержательной (семантической) информации следует уделять обеспечению сохранности (нераспространению) информации, защищаемой в соответствии с требованиями законодательства РФ, в первую очередь содержащей банковскую тайну и персональные данные. Для этого при реализации поиска (выделения) из технических данных содержательной (семантической) информации рекомендуется руководствоваться следующими общими правилами:

– при наличии возможности следует разделять содержательную (семантическую) информацию, защищаемую в соответствии с требованиями законодательства РФ, от не являющейся таковой методом группирования информации:

• в отдельных постраничных разделах документов, а также путем помещения ее в раздельные документы на бумажном носителе;

• в различных файлах данных;

– следует обеспечить поиск (выделение) только той содержательной (семантической) информации, защищаемой в соответствии с требованиями законодательства РФ, которая имеет отношение к конкретному инциденту ИБ (или их группе);

– обработка содержательной (семантической) информации не должна приводить к формированию сводной информации обо всех клиентах организации БС РФ или информации о клиентах организации БС РФ, не имеющих отношения к конкретному инциденту ИБ (или их группе), в отношении которого осуществляется реагирование.

В случае отсутствия возможности разделить содержательную (семантическую) информацию, защищаемую в соответствии с требованиями законодательства РФ, от не являющейся таковой носители содержательной (семантической) информации, передаваемые в правоохранительные органы, должны быть классифицированы и маркированы в соответствии с правилами, установленными в организации БС РФ, и передаваться по акту, в котором среди прочего определяется обязанность принимающей стороны обеспечить конфиденциальность передаваемой информации.

6. Рекомендации по сбору технических данных

6.1. Сбор технических данных рекомендуется реализовывать в рамках установленной и документированной деятельности по сбору и фиксации информации об инцидентах ИБ, выполняемой в соответствии с РС БР ИББС-2.5.

В рамках деятельности по сбору и фиксации информации об инцидентах ИБ рекомендуется для каждого инцидента ИБ обеспечить, помимо сбора технических данных, сбор и документирование обзорной информации об инциденте ИБ – профиля инцидента ИБ, описывающего:

– способ выявления инцидента ИБ;

– источник информации об инциденте ИБ;

– содержание информации об инциденте ИБ, полученной от источника;

– сценарий реализации инцидента ИБ;

– дату и время выявления инцидента ИБ;

– состав информационной инфраструктуры, задействованной в реализации инцидента ИБ, в том числе пострадавшей от инцидента ИБ, уровень ее критичности для деятельности организации БС РФ;

– способы подключения информационной инфраструктуры, задействованной в реализации инцидента ИБ, к сети Интернет или сетям общего пользования;

– контактная информация работников организации БС РФ, в зону ответственности которых входит обеспечение эксплуатации информационной инфраструктуры, задействованной в реализации инцидента ИБ;

– информация об операторе связи и провайдере сети Интернет.

Непосредственный сбор технических данных рекомендуется осуществлять в рамках установленной и документированной деятельности по сбору и фиксации информации о следующих инцидентах ИБ:

– инциденты ИБ, результатом которых являются и (или) могут являться несанкционированные переводы денежных средств (далее – инциденты ИБ, связанные с несанкционированными переводами денежных средств);

– инциденты ИБ, результатом которых является деструктивное воздействие на объекты информационной инфраструктуры организации БС РФ, которые привели или могут привести к нарушению непрерывности оказания платежных услуг (далее – инциденты ИБ, связанные с деструктивным воздействием).

В составе инцидентов ИБ, связанных с несанкционированными переводами денежных средств, рекомендуется рассматривать:

– инциденты ИБ, связанные с несанкционированным доступом (далее – НСД) к объектам информационной инфраструктуры клиентов;

– спам-рассылки, осуществляемые в отношении клиентов, реализуемые в рамках реализации методов «социального инжиниринга»[2], предпринимаемые с целью распространения компьютерных вирусов, функционально предназначенного для совершения несанкционированных переводов денежных средств;

– атаки типа «отказ в обслуживании» (DDOS-атаки), реализуемые применительно к информационной инфраструктуре клиентов, предпринимаемые с целью блокирования нормального функционирования информационной инфраструктуры после успешной реализации несанкционированных переводов денежных средств;

– воздействие компьютерных вирусов на информационную инфраструктуру клиентов, потенциально функционально предназначенного для совершения несанкционированных переводов денежных средств;

– инциденты ИБ, связанные с НСД к объектам информационной инфраструктуры систем дистанционного банковского обслуживания (далее – систем ДБО) организаций БС РФ;

– инциденты ИБ, связанные с НСД к объектам информационной инфраструктуры автоматизированных банковских систем (далее – АБС) организаций БС РФ;

– инциденты ИБ, связанные с НСД к объектам информационной инфраструктуры систем обработки карточных транзакций (далее – систем фронт-офиса) организаций БС РФ;

– инциденты ИБ, связанные с НСД к объектам информационной инфраструктуры систем посттранзакционного обслуживания карточных операций (далее – систем бэк-офиса) организаций БС РФ, в том числе система электронного документооборота, формирования платежных клиринговых позиций, клиринга и подготовки данных для проведения расчетов.

В составе инцидентов ИБ, связанных с деструктивным воздействием, рекомендуется рассматривать:

– атаки типа «отказ в обслуживании» (DDOS-атаки), реализуемые применительно к информационной инфраструктуре систем ДБО, систем фронт-офиса организаций БС РФ;

– деструктивное воздействие компьютерных вирусов на информационную инфраструктуру организации БС РФ.

6.2. Организацию сбора технических данных рекомендуется проводить в следующем порядке:

– предварительное планирование и создание условий для сбора технических данных:

• разработка и утверждение плана (регламента) сбора технических данных, реализуемого в случае выявления инцидентов ИБ;

• включение ответственных за выполнение ролей в рамках процессов обработки технических данных в группу реагирования на инциденты ИБ, создаваемую в соответствии с РС БР ИББС-2.5;

• обеспечение необходимых технических средств и инструментов для сбора и обработки технических данных;

– сбор технических данных при выявлении инцидента ИБ:

• оперативное определение перечня компонентов информационной инфраструктуры, задействованной в реализации инцидента ИБ;

• оперативное ограничение доступа к компонентам информационной инфраструктуры, задействованной в реализации инцидента ИБ, а также техническим данным для цели обеспечения их сохранности до выполнения сбора;

• сбор и документирование сведений об официально назначенном эксплуатационном персонале (администраторах) информационной инфраструктуры, задействованной в реализации инцидента ИБ, получение документально оформленных подтверждений лиц из состава эксплуатационного персонала о предоставлении/непредоставлении их аутентификационных данных третьим лицам и о внесении изменений/невнесении изменений в протоколы (журналы) регистрации, формируемые компонентами информационной инфраструктуры;

• непосредственный сбор технических данных, в том числе проверка и обеспечение целостности (неизменности) собранных данных, маркирование носителей собранных данных;

– обеспечение сохранности машинных носителей информации и защиту от воздействий, которые могут повредить их информационное содержимое, путем безопасной упаковки, опечатывания, исключающего возможность несанкционированного использования (подключения) носителя данных без нарушения целостности упаковки (печати), а также безопасного хранения и транспортировки носителей собранных данных.

6.3. Рекомендации к предварительному планированию сбора технических данных. В плане (регламенте) сбора технических данных рекомендуется определить для каждого потенциального инцидента ИБ из числа указанных в подпункте 6.1 настоящего раздела следующие положения:

– состав собираемых технических данных;

– приоритеты (последовательность) сбора технических данных;

– инструкции по использованию технических средств инструментов, описание процедур и сервисных команд, необходимых для сбора технических данных;

[2] Реагирование на инциденты ИБ, связанные со спам-рассылками, целесообразно осуществлять в случаях наличия в телепочтовых сообщениях ссылок на потенциально вредоносный (в том числе фишинговый) сайт, размещенный в сети Интернет.

– описание процедур и сервисных команд, в том числе технических, проверки (контроля) целостности собранных данных;

– правила описания и протоколирования выполненных процедур и сервисных команд, описания места сбора технических данных;

– правила создания копий собираемых технических данных и требования к их количеству;

– правила маркирования, безопасной упаковки и хранения носителей собранных технических данных;

– правила регистрации и хранения описаний и протоколов, связанных со сбором технических данных.

В плане (регламенте) сбора технических данных рекомендуется также определить необходимость и условия подготовки обращения в МВД России, его территориальные подразделения и (или) FinCert Банка России.

При планировании сбора технических данных возможно рассмотрение следующих типовых сценариев, определяющих степень оперативности предпринимаемых действий:

– сбор данных в реальном масштабе времени в случае, когда система ДБО, АБС, система фронт-офиса, система бэк-офиса (далее при совместном упоминании – целевые системы) непосредственно не подвержена компьютерной атаке, а компьютерная атака выявлена на периметре информационной инфраструктуры;

– сбор данных непосредственно после реализации инцидента ИБ (например, в течение 24 часов);

– сбор данных по прошествии значительного времени после инцидента ИБ.

Рекомендуется реализовать сбор следующих технических данных:

6.3.1. Информационная инфраструктура клиента[3]:

– энергонезависимые технические данные, расположенные на запоминающих устройствах средств вычислительной техники (СВТ), используемых клиентами для осуществления доступа к системам ДБО:

- серверном оборудовании;
- настольных компьютерах, ноутбуках;
- мобильных устройствах и планшетах;

– энергозависимые технические данные, расположенные в оперативной памяти СВТ, используемые клиентами для осуществления доступа к системам ДБО;

– энергозависимые технические данные операционных систем СВТ, используемых клиентами для осуществления доступа к системам ДБО:

- данные о сетевых конфигурациях;
- данные о сетевых соединениях;
- данные о запущенных программных процессах;
- данные об открытых файлах;
- список открытых сессий доступа;
- системные дата и время операционной системы;

– протоколы (журналы) регистрации телекоммуникационного оборудования, используемого клиентами для осуществления доступа к системам ДБО:

- маршрутизаторы, коммутаторы, точки и контроллеры беспроводного доступа, модемы;
- DHCP-сервисы;

– протоколы (журналы) регистрации средств защиты информации:

- средства (системы) аутентификации, авторизации и разграничения доступа к системам ДБО;
- средства защиты от НСД, размещенные на СВТ, используемых клиентами для осуществления доступа к системам ДБО;
- средства межсетевого экранирования;
- средства обнаружения вторжений и сетевых атак;
- средства антивирусной защиты;
- средства криптографической защиты информации (далее – СКЗИ), используемые в системах ДБО;

– протоколы (журналы) регистрации и данные почтовых серверов и средств контентной фильтрации электронной почты;

– данные сетевого трафика[4] из (в) сегмента (сегмент) вычислительной сети, в котором расположены СВТ, используемые клиентами для осуществления доступа к системам ДБО;

– протоколы (журналы) регистрации автоматических телефонных станций;

– протоколы (журналы) регистрации и данные систем видеонаблюдения и систем контроля доступа, используемые для контроля доступа в помещения, в которых расположены СВТ, используемые клиентами для осуществления доступа к системам ДБО;

– носители ключевой информации СКЗИ, используемой в системах ДБО.

6.3.2. Информационная инфраструктура организации БС РФ[5]:

– энергонезависимые технические данные, расположенные на запоминающих устройствах СВТ целевых систем:

[3] В настоящем стандарте предполагается, что сбор технических данных реализуется при наличии технической возможности с использованием функциональных возможностей объектов информационной инфраструктуры, эксплуатация которых осуществляется или организована клиентом.

[4] Копия и (или) заголовки сетевого трафика.

[5] В настоящем стандарте предполагается, что сбор технических данных реализуется при наличии технической возможности с использованием функциональных возможностей объектов информационной инфраструктуры, эксплуатация которых осуществляется или организована организацией БС РФ.

• серверном оборудовании целевых систем;
• серверном оборудовании, поддерживающем функционирование информационной инфраструктуры целевых систем;
• СВТ, используемых для администрирования целевых систем;
• банкоматах и POS-терминалах;
– энергозависимые технические данные, расположенные в оперативной памяти СВТ целевых систем:
• СВТ, используемых для администрирования информационной инфраструктуры целевых систем;
• серверного оборудования целевых систем;
• серверного оборудования, поддерживающего функционирование информационной инфраструктуры целевых систем;
– энергозависимые технические данные СВТ целевых систем в составе следующих данных:
• данные о сетевых конфигурациях;
• данные о сетевых соединениях;
• данные о запущенных программных процессах;
• данные об открытых файлах;
• список открытых сессий доступа;
• системные дата и время операционной системы;
– протоколы (журналы) регистрации целевых систем;
– протоколы (журналы) регистрации телекоммуникационного оборудования, используемого в информационной инфраструктуре целевых систем:
• маршрутизаторы, коммутаторы, точки и контроллеры беспроводного доступа, модемы;
• средства, используемые для предоставления удаленного доступа (VPN-шлюзы);
– протоколы (журналы) регистрации средств защиты информации, используемых в информационной инфраструктуре целевых систем:
• средства (системы) аутентификации, авторизации и разграничения доступа;
• средства межсетевого экранирования;
• средства обнаружения вторжений и сетевых атак, в том числе DDOS-атак;
• DHCP-сервисы;
• средства защиты от НСД, размещенные на СВТ, используемых для администрирования информационной инфраструктуры целевых систем;
• средства антивирусной защиты информационной инфраструктуры;
• СКЗИ;
– протоколы (журналы) регистрации и данные почтовых серверов и средств контентной фильтрации электронной почты;
– протоколы (журналы) регистрации и данные web-серверов и средств контентной фильтрации web-протоколов;
– протоколы (журналы) регистрации систем управления базами данных (далее – СУБД);
– данные сетевого трафика из (в) сегмента (сегмент) вычислительной сети, в котором расположены СВТ целевых систем;
– протоколы (журналы) регистрации автоматических телефонных станций;
– протоколы (журналы) регистрации и данные систем видеонаблюдения и систем контроля доступа, используемые для контроля доступа в помещения, в которых расположены СВТ целевых систем.

6.3.3. Для сбора технических данных могут выполняться следующие возможные действия:
– отключение СВТ от вычислительной сети путем отключения сетевого кабеля, отключения и (или) выключения сетевых устройств (в том числе Wi-Fi адаптера, GSM/LTE модема, Bluetooth адаптера, отключение виртуального коммутатора виртуальной машины);
– «криминалистическое» копирование энергозависимых технических данных СВТ, в том числе:
• копирование содержимого оперативной памяти СВТ;
• копирование данных операционных систем;
– отключение СВТ путем прерывания питания (отключение шнура питания или извлечение аккумуляторной батареи, отключение сетевого кабеля[6]) с последующим извлечением запоминающих устройств;
– обеспечение сохранности носителей ключевой информации СКЗИ, используемой в системах ДБО;
– «криминалистическое» копирование (создание образов) энергонезависимых технических данных запоминающих устройств СВТ методом побитного копирования и (или) методом копирования «bit-copy plus», в том числе копирование (создание образов) жестких магнитных дисков СВТ;
– копирование протоколов (журналов) регистрации;
– копирование сетевого трафика.

При отключении СВТ путем прерывания питания следует учитывать возможность:
– наличия источников бесперебойного питания;
– наличия для разных типов СВТ различающихся схем реагирования на прерывание питания – запуск процедуры штатной остановки, мгновенное отключение, переключение на резервный источник питания;
– наличия необходимости использования комбинации действий, например, одновременного отключения шнура питания и извлечения аккумуляторной батареи совместно с извлечением сетевого кабеля из сетевого интерфейса;

[6] Для случаев использования сетевых интерфейсов, поддерживающих питание по вычислительной сети (например, технология Power over Ethernet, PoE).

– существования типов СВТ, для которых конструктивно не предусмотрена процедура прерывания питания (например, для некоторых типов мобильных устройств).

Приоритеты и последовательность выполнения действий и операций по сбору технических данных рекомендуется определять на основе следующих факторов:

– фактор минимизации риска возникновения существенного ущерба от инцидента ИБ, в том числе риска совершения несанкционированных переводов денежных средств;

– фактор первоочередного получения технических данных из энергозависимой памяти;

– фактор учета возможности удаления и (или) перезаписи технических данных в энергонезависимой памяти;

– значимость технических данных для цели реагирования на инцидент ИБ с учетом реализации конкретных процедур обработки информации;

– объем требуемых усилий для сбора технических данных с определенных источников, в частности, наличия у работников необходимой компетенции по сбору технических данных с определенных источников, предполагаемых временных затрат, стоимость специализированных технических средств и инструментов или услуг внешних организаций.

Рекомендуемой реализацией является локальный сбор технических данных без удаленного доступа с использованием вычислительных сетей.

С учетом указанных факторов рекомендуется следующая последовательность действий при сборе технических данных:

6.3.4. Инциденты ИБ, связанные с НСД к объектам информационной инфраструктуры клиентов[7]:

1) получение данных операционных систем СВТ (сетевые соединения, список открытых сессий доступа), используемых клиентом для осуществления доступа к системам ДБО (рекомендуется к выполнению с высоким приоритетом значимости);

2) копирование сетевого трафика из (в) сегмента (сегмент) вычислительной сети, в котором расположены СВТ, указанные в пункте 1;

3) отключение СВТ, указанных в пункте 1, путем прерывания питания[8] с последующим извлечением запоминающих устройств и их передачей в адрес организации БС РФ и (или) экспертам FinCert Банка России (рекомендуется к выполнению с высоким приоритетом значимости);

4) в случае отсутствия технической возможности выполнения пункта 3 – отключение СВТ, указанных в пункте 1, от вычислительной сети путем отключения сетевого кабеля, отключения и (или) выключения сетевых устройств (рекомендуется к выполнению с высоким приоритетом значимости);

5) в случае отсутствия технической возможности выполнения пункта 3 – копирование содержимого оперативной памяти СВТ, указанных в пункте 1 (рекомендуется к выполнению с высоким приоритетом значимости);

6) в случае отсутствия технической возможности выполнения пункта 3 – получение данных операционных систем СВТ, указанных в пункте 1 (список запущенных программных процессов, список открытых файлов, сетевые конфигурации, системные дата и время операционной системы) (рекомендуется к выполнению с высоким приоритетом значимости);

7) в случае отсутствия технической возможности выполнения пункта 3 – «криминалистическое» копирование (создание образов) данных запоминающих устройств СВТ, указанных в пункте 1 (рекомендуется к выполнению с высоким приоритетом значимости);

8) копирование протоколов (журналов) регистрации средств защиты информации информационной инфраструктуры клиента за три месяца, предшествующих инциденту ИБ (рекомендуется к выполнению с высоким приоритетом значимости);

9) обеспечение сохранности носителей ключевой информации СКЗИ, используемой в системах ДБО (рекомендуется к выполнению с высоким приоритетом значимости);

10) копирование протоколов (журналов) регистрации телекоммуникационного оборудования, используемого клиентом для осуществления доступа к системам ДБО, за три месяца, предшествующих инциденту ИБ;

11) копирование протоколов (журналов) регистрации автоматических телефонных станций;

12) копирование протоколов (журналов) регистрации систем видеонаблюдения и систем контроля доступа, используемых для контроля доступа в помещения, предназначенные для размещения СВТ, указанных в пункте 1, за 1 неделю, предшествующую инциденту ИБ;

13) получение и документирование информации о местоположении клиента – физического лица, осуществляющего доступ к системе ДБО.

6.3.5. Спам-рассылки, осуществляемые в отношении клиентов, реализуемые в рамках реализации методов «социального инжиниринга»:

1) копирование протоколов (журналов) регистрации и данных почтовых серверов и средств контентной фильтрации электронной почты за период времени реализации спам-рассылки (реко-

[7] В случае наличия риска осуществления несанкционированных переводов денежных средств клиенту следует обеспечить максимально быстрое отключение от вычислительных сетей СВТ, используемых для осуществления доступа к системам ДБО, игнорируя потерю отдельных технических данных.

[8] Прерывание питания осуществляется с учетом описанных выше особенностей данной операции.

мендуется к выполнению с высоким приоритетом значимости);

2) копирование протоколов (журналов) регистрации телекоммуникационного оборудования, используемого клиентом для осуществления доступа к системам ДБО, за три месяца, предшествующих инциденту ИБ;

3) копирование протоколов (журналов) регистрации средств межсетевого экранирования информационной инфраструктуры клиента за период времени реализации DDOS-атаки.

6.3.6. Атаки типа «отказ в обслуживании» (DDOS-атаки), реализуемые применительно к информационной инфраструктуре клиентов:

1) копирование протоколов (журналов) регистрации средств межсетевого экранирования информационной инфраструктуры клиента за период времени реализации DDOS-атаки (рекомендуется к выполнению с высоким приоритетом значимости);

2) копирование протоколов (журналов) регистрации средств обнаружения вторжений и сетевых атак информационной инфраструктуры клиента за период времени реализации DDOS-атаки (рекомендуется к выполнению с высоким приоритетом значимости);

3) копирование протоколов (журналов) регистрации телекоммуникационного оборудования, используемого клиентом для осуществления доступа к системам ДБО за период времени реализации DDOS-атаки (рекомендуется к выполнению с высоким приоритетом значимости);

4) копирование сетевого трафика из (в) сегмента (сегмент) вычислительной сети, в котором расположены СВТ, используемые клиентом для осуществления доступа к системам ДБО за период времени реализации DDOS-атаки, а также за короткий период времени до и после реализации DDOS-атаки;

5) Дополнительно организации БС РФ рекомендуется:

– идентифицировать владельца СВТ, входящих в состав бот-сетей, задействованных в реализации DDOS-атаки (далее – СВТ бот-сетей);

– совместно с владельцем СВТ бот-сетей организовать сбор следующих технических данных:

6) получение данных операционных систем СВТ (сетевые соединения, список открытых сессий доступа, данные о запущенных программных процессах), задействованных в реализации DDOS-атаки (рекомендуется к выполнению с высоким приоритетом значимости);

7) копирование содержимого оперативной памяти СВТ, указанного в пункте 6 (рекомендуется к выполнению с высоким приоритетом значимости);

8) получение данных операционных СВТ (список запущенных программных процессов, список открытых файлов, сетевые конфигурации, системное время операционной системы), указанных в пункте 5 (рекомендуется к выполнению с высоким приоритетом значимости);

9) копирование протоколов (журналов) регистрации телекоммуникационного оборудования, используемого в информационной инфраструктуре размещения СВТ бот-сетей;

10) копирование протоколов (журналов) регистрации средств межсетевого экранирования, используемых в информационной инфраструктуре размещения СВТ бот-сетей;

11) копирование протоколов (журналов) регистрации средств обнаружения вторжений и сетевых атак информационной инфраструктуры размещения СВТ бот-сетей;

12) «криминалистическое» копирование (создание образов) данных запоминающих устройств СВТ, указанных в пункте 5 (рекомендуется к выполнению с высоким приоритетом значимости).

6.3.7. Инциденты ИБ, связанные с НСД к объектам информационной инфраструктуры целевых систем организации БС РФ[9]:

1) копирование протоколов (журналов) регистрации целевых систем организации БС РФ за период времени, связанный с инцидентом ИБ (рекомендуется к выполнению с высоким приоритетом значимости);

2) копирование протоколов (журналов) регистрации и данных web-серверов, средств контентной фильтрации web-протоколов за три месяца, предшествующих инциденту ИБ (рекомендуется к выполнению с высоким приоритетом значимости);

3) копирование протоколов (журналов) регистрации СУБД за три месяца, предшествующих инциденту ИБ (рекомендуется к выполнению с высоким приоритетом значимости);

4) копирование протоколов (журналов) регистрации средств защиты информации, используемых в информационной инфраструктуре целевых систем, за три месяца, предшествующих инциденту ИБ (рекомендуется к выполнению с высоким приоритетом значимости);

5) копирование протоколов (журналов) телекоммуникационного оборудования, используемого в информационной инфраструктуре целевых систем, за три месяца, предшествующих инциденту ИБ;

6) получение данных операционных систем СВТ целевых систем (сетевые соединения, список открытых сессий доступа);

---

[9] В случае наличия риска осуществления несанкционированных переводов денежных средств организации БС РФ следует обеспечить максимально быстрое отключение от вычислительных сетей СВТ, используемых для осуществления доступа к платежным системам, игнорируя потерю отдельных технических данных.

7) копирование содержимого оперативной памяти СВТ целевых систем;

8) получение данных операционных систем СВТ целевых систем (список запущенных программных процессов, список открытых файлов, сетевые конфигурации, системное время операционной системы;

9) копирование сетевого трафика из (в) сегмента (сегмент) вычислительной сети, в котором расположены СВТ целевых систем;

10) «криминалистическое» копирование (создание образов) данных запоминающих устройств СВТ, указанных в пункте 6;

11) копирование протоколов (журналов) регистрации автоматических телефонных станций;

12) копирование протоколов (журналов) регистрации систем видеонаблюдения и систем контроля доступа, используемых для контроля доступа в помещения, предназначенные для размещения СВТ целевых систем, за 1 неделю, предшествующую инциденту ИБ.

6.3.8. Атаки типа «отказ в обслуживании» (DDOS-атаки), реализуемые применительно к информационной инфраструктуре целевых систем организаций БС РФ:

1) копирование протоколов (журналов) регистрации средств межсетевого экранирования информационной инфраструктуры целевых систем за период времени реализации DDOS-атаки (рекомендуется к выполнению с высоким приоритетом значимости);

2) копирование протоколов (журналов) регистрации средств обнаружения вторжений и сетевых атак в информационную инфраструктуру целевых систем за период времени реализации DDOS-атаки (рекомендуется к выполнению с высоким приоритетом значимости);

3) копирование протоколов (журналов) регистрации телекоммуникационного оборудования, используемого в информационной инфраструктуре целевых систем за период времени реализации DDOS-атаки (рекомендуется к выполнению с высоким приоритетом значимости);

4) копирование сетевого из (в) сегмента (сегмент) вычислительной сети, в котором расположены СВТ целевых систем, за период времени реализации DDOS-атаки, а также за короткий период времени до и после реализации DDOS-атаки;

5) Дополнительно организации БС РФ рекомендуется:

– документировать сведения:

• о пропускной способности и провайдерах используемых каналов связи;

• об использовании сервиса защиты от DDOS-атак, предоставляемого внешними организациями;

– идентифицировать владельца СВТ бот-сетей, задействованных в реализации DDOS-атаки;

– совместно с владельцем СВТ бот-сетей организовать сбор технических данных по аналогии с рекомендациями, установленными для случая сбора технических данных при атаках типа «отказ в обслуживании» (DDOS-атаки), реализуемые применительно к информационной инфраструктуре клиентов.

6.3.9. Деструктивное воздействие компьютерных вирусов на информационную инфраструктуру организации БС РФ[10]:

1) получение данных операционных систем СВТ целевых систем (сетевые соединения, список открытых сессий доступа) (рекомендуется к выполнению с высоким приоритетом значимости);

2) копирование сетевого из (в) сегмента (сегмент) вычислительной сети, в котором расположены СВТ целевых систем;

3) копирование содержимого оперативной памяти СВТ целевых систем (рекомендуется к выполнению с высоким приоритетом значимости);

4) отключение СВТ целевых систем от вычислительной сети путем отключения сетевого кабеля, отключения и (или) выключения сетевых устройств (рекомендуется к выполнению с высоким приоритетом значимости);

5) получение данных операционных систем СВТ целевых систем (список запущенных программных процессов, список открытых файлов, сетевые конфигурации, системное время операционной системы) (рекомендуется к выполнению с высоким приоритетом значимости);

6) криминалистическое копирование (создание образов) запоминающих устройств СВТ целевых систем (рекомендуется к выполнению с высоким приоритетом значимости);

7) копирование протоколов (журналов) регистрации средств антивирусной защиты информационной инфраструктуры клиента за три месяца, предшествующих инциденту ИБ (рекомендуется к выполнению с высоким приоритетом значимости);

8) копирование протоколов (журналов) регистрации и данных почтовых серверов, средств контентной фильтрации электронной почты за три месяца, предшествующих инциденту ИБ (рекомендуется к выполнению с высоким приоритетом значимости);

9) копирование протоколов (журналов) регистрации и данные web-серверов, средств контентной фильтрации web-протоколов за три месяца, предшествующих инциденту ИБ (рекомендуется к выполнению с высоким приоритетом значимости);

10) копирование протоколов (журналов) регистрации средств защиты информации, исполь-

[10] До выполнения действий по сбору технических данных не следует проводить антивирусную проверку.

зуемых в информационной инфраструктуре целевых систем, за три месяца, предшествующих инциденту ИБ (рекомендуется к выполнению с высоким приоритетом значимости);

11) копирование протоколов (журналов) регистрации телекоммуникационного оборудования, используемого в информационной инфраструктуре целевых систем, за три месяца, предшествующих инциденту ИБ.

6.3.10. Деструктивное воздействие компьютерных вирусов на информационную инфраструктуру клиентов[11]:

1) копирование протоколов (журналов) регистрации средств антивирусной защиты информационной инфраструктуры клиента за три месяца, предшествующих инциденту ИБ (рекомендуется к выполнению с высоким приоритетом значимости);

2) получение данных операционных систем СВТ (сетевые соединения, список открытых сессий доступа), используемых клиентом для осуществления доступа к системам ДБО (рекомендуется к выполнению с высоким приоритетом значимости);

3) копирование сетевого трафика из (в) сегмента (сегмент) вычислительной сети, в котором расположены СВТ, указанные в пункте 2;

4) отключение СВТ, указанных в пункте 2, от вычислительной сети путем отключения сетевого кабеля, отключения и (или) выключения сетевых устройств (рекомендуется к выполнению с высоким приоритетом значимости);

5) копирование содержимого оперативной памяти СВТ, указанных в пункте 2 (рекомендуется к выполнению с высоким приоритетом значимости);

6) отключение СВТ, указанных в пункте 2, путем прерывания питания[12] с последующим извлечением запоминающих устройств и их передачей в адрес организации БС РФ и (или) экспертам FinCert Банка России (рекомендуется к выполнению с высоким приоритетом значимости);

7) в случае отсутствия технической возможности выполнения пункта 5 – «криминалистическое» копирование (создание образов) данных запоминающих устройств СВТ, указанных в пункте 2 (рекомендуется к выполнению с высоким приоритетом значимости);

8) в случае отсутствия технической возможности выполнения пункта 5 – получение данных операционных систем СВТ (список запущенных программных процессов, список открытых файлов, сетевые конфигурации, системное время операционной системы), указанных в пункте 2 (рекомендуется к выполнению с высоким приоритетом значимости);

9) копирование протоколов (журналов) регистрации и данных почтовых серверов, средств контентной фильтрации электронной почты за три месяца, предшествующих инциденту ИБ (рекомендуется к выполнению с высоким приоритетом значимости);

10) копирование протоколов (журналов) регистрации средств защиты информации информационной инфраструктуры клиента, за три месяца, предшествующих инциденту ИБ (рекомендуется к выполнению с высоким приоритетом значимости);

11) копирование протоколов (журналов) регистрации телекоммуникационного оборудования, используемого клиентом для осуществления доступа к системам ДБО, за три месяца, предшествующих инциденту ИБ.

6.4. Рекомендации по обеспечению необходимыми техническими средствами и инструментами для сбора и обработки технических данных.

Для реализации сбора и обработки технических данных организации БС РФ рекомендуется обеспечить наличие следующих готовых к использованию технических средств и инструментов:

– специально выделенные автоматизированные рабочие места для обработки технических данных, в том числе для поиска (выделения) содержательной (семантической) информации, ее анализа и оформления. Рекомендуется использование автономных автоматизированных рабочих мест, не подключенных к вычислительным сетям[13];

– технические, в том числе программные, средства для сбора технических данных и проверки (контроля) целостности собранных данных;

– технические средства централизованного сбо-ра, хранения и анализа протоколов (журналов) регистрации, а также автоматизированной обработки собранных технических данных (например, систем управления журналами регистрации, SIEM систем);

– технические средства записи и хранения данных сетевого трафика;

– носители данных для сбора и хранения собранных технических данных. При этом рекомендуется:

- использование носителей, объем хранения которых заведомо превышает объем собираемых технических данных;
- в случае применения инструментов, реализующих посекторное копирование данных, использование носителей, имеющих ту же физическую основу хранения (данные с HDD-накопителей копируются на HDD-накопители, данные с SSD-накопителей копируются на SSD-накопители). При этом

[11] До выполнения действий по сбору технических данных не следует проводить антивирусную проверку.

[12] Прерывание питания осуществляется с учетом описанных выше особенностей данной операции.

[13] В качестве альтернативы может быть рекомендовано использование для сбора и обработки технических данных выделенных сегментов вычислительных сетей или отдельных виртуальных машин.

носители-приемники должны быть подготовлены (очищены) специальным образом для обеспечения отсутствия каких-либо посторонних данных, для чего рекомендуется использование средств гарантированного уничтожения информации или штатных средств операционной системы, реализующих функцию форматирования с полным удалением (очисткой) записанной информации, сопровождаемое документированием выполненных процедур и сервисных команд;

• в случае копирования данных с SSD-накопителей рекомендуется создание образов в файле данных в формате «RAW». При невозможности создания образов в файле данных в формате «RAW» рекомендуется использование модели SSD-накопителя, идентичной модели накопителя с исходными данными;

– антистатические контейнеры или пакеты для хранения носителей технических данных;

– наклейки, этикетки и перманентные маркеры для маркирования носителей собранных технических данных;

– немагнитные инструменты, используемые для извлечения запоминающих устройств, накопителей на жестких магнитных дисках;

– прошитые книги (блокноты) для фиксации протоколов и описаний выполняемых действий и операций;

– цифровые фотоаппараты и диктофоны.

При сборе технических данных следует избегать использования любых средств и материалов, которые производят или излучают статическое или электромагнитное поле, так как оно может повредить или уничтожить собранные данные.

Рекомендации по составу технических средств сбора технических данных приведены в приложении В к настоящему стандарту.

6.5. Рекомендации по оперативному ограничению доступа к техническим данным для цели обеспечения их сохранности до выполнения сбора.

В планах (регламентах) сбора технических данных должно быть предусмотрено оперативное выполнение действий и операций, направленных на минимизацию риска злоумышленных или случайных действий по изменению, повреждению и (или) уничтожению технических данных до момента их сбора. К таким действиям и операциям относятся:

– реализация ограничений и (или) запрета по физическому доступу к объектам информационной инфраструктуры – источникам технических данных;

– реализация ограничений и (или) запрета по логическому доступу к объектам информационной инфраструктуры – источникам технических данных до момента сбора идентифицированных технических данных;

– проведение сбора технических данных только лицами, обладающими необходимыми опытом и компетенцией.

После обнаружения инцидента ИБ до момента сбора технических данных следует обеспечить запрет выполнения:

– антивирусных проверок СВТ – потенциальных источников технических данных;

– установки обновлений и переустановки операционных систем СВТ – потенциальных источников технических данных;

– отключения от вычислительной сети СВТ – потенциальных источников технических данных, за исключением СВТ, используемых клиентами для осуществления доступа к системам ДБО и СВТ, используемых организациями БС РФ для взаимодействия с платежными системами.

С целью минимизации финансового ущерба от инцидентов ИБ организации БС РФ рекомендуется:

– доведение до клиентов рекомендаций по максимально возможно быстрому отключению от вычислительных сетей СВТ, используемых клиентами для осуществления доступа к системам ДБО;

– максимально возможное быстрое отключение от вычислительных сетей СВТ, используемых организациями БС РФ для взаимодействия с платежными системами.

6.6. Рекомендации по способам непосредственного сбора технических данных, в том числе проверке целостности (неизменности) собранных данных, маркированию носителей собранных данных.

Перед непосредственным сбором технических данных рекомендуется выполнение описания или фиксации места сбора технических данных:

– описание или фиксацию типа, расположения, состояния электропитания СВТ;

– описание или фиксацию наличия и способа подключения СВТ к вычислительным сетям, в том числе беспроводным сетям и к информационно-телекоммуникационной сети Интернет;

– описание или фиксацию информации о событиях и процессах на дисплеях СВТ.

Фиксацию места сбора технических данных рекомендуется осуществлять путем фото- или видеосъемки с отметкой даты и времени, для чего на фото- или видеоаппаратуре должны быть выставлены корректные дата и время. Рекомендуется использование фото- или видеоаппаратуры, формирующей EXIF-данные фотографий, позволяющих подтвердить подлинность графического изображения. Дополнительно рекомендуется документирование данных о производителе, модели и серийном номере используемой фото- или видеоаппаратуры.

6.6.1. Рекомендации по выполнению «криминалистического» копирования (создания образов)

энергонезависимых технических данных запоминающих устройств СВТ методом побитового копирования и (или) методом копирования «bit-copy plus».

Выполнение операций по «созданию образа» энергонезависимых технических данных СВТ должно сопровождаться описанием и протоколированием:

– всех выполненных процедур и сервисных команд, использованных для выполнения операции по «созданию образа» с указанием даты и времени начала и окончания их выполнения;

– характеристик запоминающих устройств (модель, серийный номер, характеристики, емкость) исходных технических данных и их полученных копий;

– использованных технических средств, примененных для выполнения операций по «созданию образа» (наименование, версия, лицензионные сведения).

Для выполнения «криминалистического» копирования (создания образов) запоминающих устройств рекомендуется следующая последовательность действий и операций:

1) отключение СВТ путем прерывания питания[14];

2) в случае применения:

2.1) программных средств «криминалистического» копирования (создания образов):

2.1.1) загрузка операционной системы с предварительно созданного «доверенного» загрузочного носителя, содержащего необходимые программные средства для выполнения операций по «созданию образа», в том числе программные средства создания побитовой копии, вычисления контрольных сумм или значений хэш-функций, программные средства использования запоминающего устройства в режиме «только для чтения»;

2.1.2) принятие мер к обеспечению использования запоминающего устройства в режиме «только для чтения», для чего возможно использование функций операционной системы путем настроек правил ее загрузки с «доверенного» носителя или специализированных аппаратных или программных средств – «write-blocker»[15];

2.1.3) в случае отсутствия технической возможности выполнения пунктов 1) и 2.1.1) подключение к СВТ и использование носителя, содержащего необходимые для создания образа программные средства, в отношении которого приняты меры по обеспечению защиты от записи или несанкционированного изменения; 2.2) аппаратных средств – дубликаторов «криминалистического» копирования (создания образов):

2.2.1) извлечение из СВТ запоминающего устройства и подключение его к дубликатору;

3) вычисление и сохранение контрольной суммы или значения хэш-функций исходных данных запоминающего устройства[16];

4) выполнение операции по «созданию образа» на отдельный, специально подготовленный носитель информации;

5) вычисление и сохранение контрольных сумм или значений хэш-функций скопированных данных и исходных данных запоминающего устройства, сравнение вычисленного значения со значением, вычисленным в рамках выполнения пункта 5, для подтверждения целостности скопированных данных с составлением акта, содержащего полученный результат сравнения;

6) обеспечение безопасной упаковки и хранения носителей информации, содержащих скопированные данные.

6.6.2. Рекомендации по выполнению копирования содержимого оперативной памяти СВТ и получению данных операционных систем.

Выполнение копирования содержимого оперативной памяти СВТ и получение данных операционных систем рекомендуется выполнять с соблюдением следующих правил:

– все программные средства, используемые для копирования оперативной памяти СВТ и получения данных операционных систем, следует размещать на специально выделенных для этих целей носителях, в отношении которых приняты меры по обеспечению защиты от записи или несанкционированного изменения;

– для копирования оперативной памяти СВТ и получения данных операционных систем следует использовать только программные средства, размещенные на указанном выше защищенном носителе;

– для исполняемых модулей программных средств, используемых для копирования оперативной памяти СВТ и получения данных операционных систем, должны быть известны наименования порождаемых ими программных процессов (для их исключения из рассмотрения при дальнейшем анализе).

Выполнение копирования содержимого оперативной памяти СВТ и получение данных операцион-

---

[14] Прерывание питания осуществляется с учетом описанных выше особенностей данной операции.

[15] Также указанные аппаратные или программные средства известны под общим наименованием «forensic bridge». В случае отсутствия технической возможности использования запоминающего устройства в режиме «только для чтения» следует учитывать возможность изменения исходных технических данных, в том числе появление временных файлов данных, изменения временных атрибутов файлов данных и директорий, изменений данных системного реестра операционной системы Windows.

[16] Выполнение операций, указанных в пунктах 4 и 6, технически неприменимо в случае копирования данных с SSD-носителя.

ных систем должно сопровождаться описанием и протоколированием:

– всех выполненных процедур и сервисных команд, использованных программных средств, примененных для копирования содержимого оперативной памяти СВТ и получения данных операционных систем (наименование, версия, лицензионные сведения, точные сервисные команды и параметры команд);

– контрольной суммы или значения хэш-функций исполняемых файлов программных средств, используемых для копирования оперативной памяти СВТ, и получение данных операционных систем;

– даты и времени выполнения процедур и сервисных команд.

Рекомендуемым решением является предварительная подготовка, размещение на специально выделенном носителе и использование программного пакета (скрипта), содержащего все выполняемые процедуры и сервисные команды, необходимые для копирования содержимого оперативной памяти СВТ и получения данных операционных систем.

Выполнение копирования содержимого оперативной памяти СВТ и получение данных операционных систем рекомендуется выполнять в следующем порядке:

– получение данных операционных систем:
- сетевые соединения;
- список открытых сессий доступа;

– копирование содержимого оперативной памяти;

– получение данных операционных систем:
- список запущенных программных процессов;
- список открытых файлов;
- сетевые конфигурации;
- системное время операционной системы с указанием часового пояса.

Дополнительно следует выполнить описание и протоколирование наименования операционной системы, включая данные обо всех установленных обновлениях.

Для выполнения копирования содержимого оперативной памяти СВТ и получения данных операционных систем рекомендуется следующая последовательность действий и операций:

1) выполнение копирования содержимого оперативной памяти СВТ и получение данных операционной системы с использованием программных средств, размещенных на специально выделенных для этих целей носителях, с сохранением полученных результатов в файлах данных, размещенных на накопителе на жестких магнитных дисках СВТ, или в файлах данных, размещенных на внешнем носителе информации[17];

2) отключение СВТ путем прерывания питания[18];

3) загрузка операционной системы с предварительно созданного «доверенного» загрузочного носителя, содержащего необходимые программные средства для выполнения логического копирования файлов данных, программные средства вычисления контрольных сумм или значений хэш-функций, программные средства использования запоминающих устройств в режиме «только для чтения»;

4) вычисление и сохранение контрольной суммы или значения хэш-функций файлов данных, размещенных на накопителе на жестких магнитных дисках СВТ или внешнем носителе информации, созданных в рамках выполнения пункта 1;

5) в случае сохранения полученных результатов в файлах данных, размещенных на накопителе на жестких магнитных дисках СВТ:
- логическое копирование на внешние носители информации исходных файлов данных, размещенных на накопителе на жестких магнитных дисках СВТ, созданных в рамках выполнения пункта 1;
- вычисление и сохранение контрольных сумм или значений хэш-функций исходных файлов данных, созданных в рамках выполнения пункта 1, и полученных файлов данных, скопированных в рамках выполнения пункта 5, сравнение вычисленного значения со значениями, вычисленными в рамках выполнения пункта 4, для подтверждения целостности скопированных данных с составлением акта, содержащего полученный результат сравнения;

6) обеспечение безопасной упаковки и хранения носителей информации, содержащих скопированные файлы.

В качестве внешних носителей информации рекомендуется использование носителей информации, дополнительная запись и (или) перезапись данных на которые невозможна, например, путем выполнения процедуры «финализации» для компакт-дисков, или использование специального аппаратного ограничителя записи – «write-blocker».

6.6.3. Рекомендации по выполнению копирования протоколов (журналов) регистрации. В настоящем стандарте предусматривается целесообразность копирования следующих протоколов (журналов) регистрации:

– протоколы (журналы) регистрации целевых систем;

– протоколы (журналы) регистрации телекоммуникационного оборудования:

[17] Рекомендованным решением является сохранение результатов получения содержимого оперативной памяти СВТ и данных операционной системы в файлах данных, размещенных на внешнем носителе информации, с целью минимизации воздействия на данные запоминающих устройств СВТ, являющихся источниками технических данных.

[18] Прерывание питания осуществляется с учетом описанных выше особенностей данной операции.

• маршрутизаторы, коммутаторы, точки и контроллеры беспроводного доступа, модемы;
• DHCP-сервисы;
• средства, используемые для предоставления удаленного доступа (VPN-шлюзы);
– протоколы (журналы) регистрации средств защиты информации:
• средства (системы) аутентификации, авторизации и разграничения доступа;
• средства межсетевого экранирования;
• средства обнаружения вторжений и сетевых атак, в том числе DDOS-атак;
• средства защиты от НСД;
• средства антивирусной защиты информационной инфраструктуры;
• СКЗИ;
– протоколы (журналы) регистрации и данные почтовых серверов, средств контентной фильтрации электронной почты;
– протоколы (журналы) регистрации и данные web-серверов, средств контентной фильтрации web-протоколов;
– протоколы (журналы) регистрации СУБД;
– протоколы (журналы) регистрации автоматических телефонных станций;
– протоколы (журналы) регистрации и данные систем видеонаблюдения и систем контроля доступа.

В большинстве случаев указанные протоколы (журналы) регистрации хранятся в виде файлов данных, в том числе в проприетарных форматах, текстовых файлах, базах данных, протоколов (журналов) регистрации операционных систем (syslog для UNIX систем, event logs для Windows-систем). При этом для копирования протоколов (журналов) регистрации может быть рекомендована следующая общая последовательность действий:

1) выгрузка (копирование) протоколов (журналов) регистрации за определенный требуемый период времени в файлы данных;

2) вычисление и сохранение контрольных сумм или значений хэш-функций полученных файлов данных;

3) логическое копирование на внешние носители информации (компакт-диски) исходных файлов данных, созданных в рамках выполнения пункта 1;

4) вычисление и сохранение контрольных сумм или значений хэш-функций исходных файлов данных, созданных в рамках выполнения пункта 1, и полученных файлов данных, скопированных в рамках выполнения пункта 3, сравнение вычисленных значений со значениями, вычисленными в рамках выполнения пункта 2, для подтверждения целостности скопированных данных с составлением акта, содержащего полученный результат сравнения;

5) обеспечение безопасной упаковки и хранения носителей информации, содержащих скопированные файлы.

При выполнении копирования протоколов (журналов) и данных телекоммуникационного оборудования необходимо учитывать, что отключение телекоммуникационного оборудования путем прерывания питания, как правило, приводит к удалению всех технических данных. Копирование протоколов (журналов) телекоммуникационного оборудования рекомендуется сопровождать получением данных о его текущем статусе:
– системные дата и время;
– версия программного обеспечения;
– значения контрольных сумм программного обеспечения;
– сетевая информация, таблица маршрутизации;
– текущая конфигурация оборудования;
– конфигурация оборудования, примененная при загрузке;
– состав администраторов оборудования;
– состав запущенных программных процессов.

При копировании протоколов (журналов) регистрации и данных телекоммуникационного оборудования рекомендуется подключение к телекоммуникационному оборудованию через консольный порт (не рекомендуется выполнять удаленное подключение через протоколы Telnet или SSH), при этом категорически не рекомендуется изменять конфигурацию маршрутизатора или вводить какие-либо команды конфигурации.

При организации копирования протоколов (журналов) регистрации рекомендуется обеспечивать:
– принятие необходимых мер к ограничению доступа к собираемым копиям данных с учетом возможного нахождения в копиях данных информации, защищаемой в соответствии с требованиями законодательства Российской Федерации, нормативными актами Банка России, в том числе:
• персональных данных;
• аутентификационных данных;
• данных, используемых для подтверждения распоряжений на перевод денежных средств;
• банковской тайны;
– принятие мер к обеспечению достаточной емкости носителей и хранилищ, используемых для сбора протоколов (журналов) регистрации, позволяющих избежать перезаписи и (или) потери информации;
– использование специализированных технических средств централизованного сбора, анализа и хранения протоколов (журналов) регистрации (например, систем управления журналами регистрации, SIEM систем), позволяющих минимизиро-

вать риски злоумышленных действий по изменению, повреждению и (или) уничтожению протоколов (журналов) регистрации;

– заблаговременное включение в договоры положений, определяющих условия и процедуры получения протоколов (журналов) регистрации СВТ и иных технических средств, находящихся в собственности третьих лиц (например, протоколов (журналов) регистрации почтовых сервисов, сервисов обнаружения и отражения DDOS-атак, технических средств провайдеров сети Интернет и операторов мобильной связи).

6.6.4. Рекомендации по выполнению копирования сетевого трафика.

Для сбора данных сетевого трафика для цели реагирования на инциденты ИБ рекомендуется использование технических средств мониторинга и копирования сетевых пакетов (packet sniffer), а также технических средств, позволяющих автоматизировать анализ собранных сетевых пакетов.

Сбор данных сетевого трафика рекомендуется осуществлять в определенных точках вычислительных сетей, обеспечивающих копирование данных, значимых и существенных для расследования инцидента ИБ, например:

– для информационной инфраструктуры клиента – данные сетевого трафика из (в) сегмента (сегмент) вычислительной сети, в котором расположены СВТ (настольные компьютеры, ноутбуки), используемые клиентом для осуществления доступа к системам ДБО;

– для информационной инфраструктуры организации БС РФ – данные сетевого трафика из (в) сегмента (сегмент) вычислительной сети, в котором расположены СВТ целевых систем.

Для копирования файлов данных, формируемых техническими средствами мониторинга и копирования сетевых пакетов (packet sniffer), может быть использована последовательность действия, определенная в настоящем стандарте для копирования протоколов (журналов) регистрации.

При организации копирования протоколов (журналов) регистрации рекомендуется обеспечивать принятие необходимых мер к ограничению доступа к собираемым копиям данных с учетом возможного нахождения в копиях данных информации, защищаемой в соответствии с требованиями законодательства Российской Федерации, нормативными актами Банка России, и обеспечению достаточной емкости носителей и хранилищ, используемых для сбора данных сетевого трафика, позволяющих избежать перезапись и (или) потерю информации, значимой для цели реагирования на инциденты ИБ.

6.7. Рекомендации по обеспечению безопасной упаковки, хранения и транспортировки носителей собранных данных.

Копии технических данных, используемые в качестве доказательной базы, должны храниться безопасным образом.

Рекомендуется учитывать, что носители собранных технических данных являются хрупкими и чувствительными к экстремальным температурам, влажности, механическим ударам, воздействию света, статическому электричеству и электромагнитным полям.

При проведении упаковки носителей собранных технических данных рекомендуется:

– маркирование и учет носителей собранных технических данных;

– упаковка носителей собранных технических данных и соответствующих сопроводительных описаний и протоколов в антистатические пакеты или контейнеры, включая использование бумажных пакетов, конвертов, коробок. Не рекомендуется использование пластиковых пакетов или контейнеров;

– маркирование пакетов или контейнеров, используемых для хранения носителей собранных технических данных;

– предотвращение деформации и царапин носителей собранных технических данных.

При хранении и транспортировке носителей собранных технических данных рекомендуется:

– обеспечить хранение и транспортировку носителей собранных технических данных вдали от электромагнитных полей;

– исключить хранение носителей собранных технических данных в транспортных средствах в течение длительного времени;

– обеспечение защиты носителей собранных технических данных от ударов и вибраций, влаги или пыли;

– обеспечение защиты от воздействия экстремальных температур и влажности;

– обеспечение контроля работоспособности в течение требуемого времени для технических средств, использующих батарейки и (или) аккумуляторы.

Рекомендуется применять способ упаковки носителей эталонных копий собранных технических данных и соответствующих сопроводительных описаний и протоколов, обеспечивающий невозможность доступа к носителю и (или) использования носителя без видимого нарушения целостности упаковки. Одним из допустимых способов упаковки и опечатывания носителей небольшого размера является их совместное помещение в полиэтиленовый антистатический пакет с последующей перевязкой его горловины нитью, концы которой опечатываются с наклеиванием пояснительной записки, нанесенной шариковой ручкой, с подписями участвующих в опечатывании лиц и печатью организации БС РФ.

7. Рекомендации по проведению поиска (выделения) содержательной (семантической) информации, ее анализу и оформлению

7.1. Основными целями выполнения процедур, связанных с поиском (выделением) в технических данных и последующим анализом содержательной (семантической) информации, являются:

– определение технических способов и схем реализаций угроз ИБ;

– проведение идентификации субъектов, реализующих угрозы ИБ;

– выявление маркеров «скрытого» несанкционированного управления объектами информационной инфраструктуры[19], используемых для осуществления переводов денежных средств.

7.2. Для обеспечения возможности выполнения процедур, связанных с поиском (выделением) в технических данных и последующим анализом содержательной (семантической) информации организации БС РФ, рекомендуется:

– обеспечить участие компетентных аналитиков в области анализа технических данных;

– обеспечить наличие необходимых технических средств и инструментов для выделения и анализа содержательной (семантической) информации;

– определить и обеспечить выполнение правил документирования выделенной содержательной (семантической) информации и результатов ее анализа.

7.3. Для проведения поиска (выделения) и анализа содержательной (семантической) информации организации БС РФ рекомендуется выполнение следующего общего алгоритма действий:

– определить для каждого инцидента ИБ из числа указанных в пункте 6.1 настоящего стандарта перечень событий ИБ, значимых для поиска (выделения) и анализа содержательной (семантической) информации:

• исходные (базовые) события ИБ или их группа, являющиеся отправной точкой дальнейшего поиска и анализа;

• события ИБ или их группа, потенциально имеющие отношение или связанные с инцидентом ИБ;

– провести непосредственный поиск (выделение) из технических данных содержательной (семантической) информации, связанной с указанными событиями ИБ;

– провести анализ, в том числе корреляционный и сравнительный, выделенной содержательной (семантической) информации, в том числе для достижения целей, указанных в пункте 7.1 настоящего стандарта.

7.4. В большинстве случаев деятельность по поиску (выделению) и анализу содержательной (семантической) информации не может быть формализована, а результат ее выполнения определяется опытом и компетенцией аналитика.

Для цели повышения качества и оперативности поиска (выделения) и анализа содержательной (семантической) информации организации БС РФ рекомендуется:

– использование специализированных технических средств и систем централизованного сбора, анализа и хранения протоколов (журналов) регистрации (например, систем управления журналами регистрации или SIEM систем);

– использование известных маркеров «скрытого» несанкционированного управления объектами информационной инфраструктуры, которые могут быть разработаны аналитиками организации БС РФ самостоятельно или получены из внешних источников, осуществляющих реагирование на инциденты ИБ, например, от FinCert Банка России.

7.5. В составе основных событий ИБ организации БС РФ рекомендуется рассматривать следующие:

– события, связанные с идентификацией и аутентификацией администраторов и эксплуатационного персонала, программных процессов (сервисов), клиентов и участников платежной системы (далее при совместном упоминании – субъекты доступа) в целевых системах и информационной инфраструктуре размещения целевых систем и информационной инфраструктуре клиентов;

– события, связанные с управлением доступом в целевых системах и информационной инфраструктуре размещения целевых систем, информационной инфраструктуре клиентов;

– события, связанные с осуществлением доступа к целевым системам и информационной инфраструктуре размещения целевых систем, информационной инфраструктуре клиентов;

– события, связанные с осуществлением удаленного доступа к целевым системам и информационной инфраструктуре размещения целевых систем, информационной инфраструктуре клиентов;

– события, связанные с изменением состояния информационной инфраструктуры размещения целевых систем и информационной инфраструктуры клиентов;

– события, связанные с антивирусной защитой;

– события, связанные с выполнением криптографических преобразований;

– события, связанные с функционированием средств защиты от несанкционированного доступа;

– события, связанные с осуществлением информационного взаимодействия на всех уровнях

[19] Также указанные данные известны под общим наименованием «индикаторы компрометации, indicators of compromise, IOC».

модели взаимодействия открытых систем, определенной в ГОСТ 28906-91.

7.6. Для инцидентов ИБ, связанных с НСД к объектам информационной инфраструктуры клиентов или информационной инфраструктуре целевых систем, рекомендуется рассмотрение следующих событий ИБ, значимых для цели поиска (выделения) и анализа содержательной (семантической) информации:

– исходные (базовые) события ИБ или их группа, являющиеся отправной точкой дальнейшего поиска и анализа:

• события, связанные с осуществлением доступа к целевым системам и информационной инфраструктуре размещения целевых систем, информационной инфраструктуре клиентов;

• события, связанные с осуществлением удаленного доступа к целевым системам и информационной инфраструктуре размещения целевых систем;

• события, связанные с выполнением криптографических преобразований;

– события ИБ или их группа, информация о которых потенциально может быть использована для определения технических способов и схем реализаций угроз ИБ:

• события, связанные с идентификацией и аутентификацией субъектов доступа в целевых системах и информационной инфраструктуре размещения целевых систем, информационной инфраструктуре клиента;

• события, связанные с управлением доступом в целевых системах и информационной инфраструктуре размещения целевых систем, информационной инфраструктуре клиентов;

• события, связанные с изменением состояния информационной инфраструктуры размещения целевых систем, информационной инфраструктуры клиентов;

• события, связанные с функционированием средств защиты от несанкционированного доступа;

• события, связанные с антивирусной защитой;

• события, связанные с выполнением криптографических преобразований;

• события, связанные с осуществлением информационного взаимодействия на прикладном уровне модели взаимодействия открытых систем, определенной в ГОСТ 28906-91;

– события ИБ или их группа, информация о которых потенциально может быть использована для проведения идентификации субъектов, реализующих угрозы ИБ:

• события, связанные с идентификацией и аутентификацией субъектов доступа в целевых системах и информационной инфраструктуре размещения целевых систем, информационной инфраструктуре клиентов;

• события, связанные с осуществлением информационного взаимодействия на аппаратном (физическом), сетевом, транспортном и прикладном уровнях модели взаимодействия открытых систем, определенной в ГОСТ 28906-91;

– события ИБ или их группа, информация о которых потенциально может быть использована для выявления маркеров «скрытого» несанкционированного управления объектами информационной инфраструктуры, используемых для осуществления переводов денежных средств:

• события, связанные с изменением состояния информационной инфраструктуры размещения целевых систем и информационной инфраструктуре клиентов;

• события, связанные с функционированием средств защиты от несанкционированного доступа;

• события, связанные с антивирусной защитой;

• события, связанные с осуществлением информационного взаимодействия на сетевом, транспортном и прикладном уровнях модели взаимодействия открытых систем, определенной в ГОСТ 28906-91.

7.7. Для инцидентов ИБ, связанных со спам-рассылками, осуществляемыми в отношении клиентов, осуществляемых в рамках реализации методов «социального инжиниринга», рекомендуется рассмотрение следующих событий ИБ, значимых для цели поиска (выделения) и анализа содержательной (семантической) информации:

– исходные (базовые) события ИБ или их группа, являющиеся отправной точкой дальнейшего поиска и анализа, а также события ИБ или их группа, информация о которых потенциально может быть использована для выявления маркеров «скрытого» несанкционированного управления объектами информационной инфраструктуры, используемых для осуществления переводов денежных средств:

• события, связанные с осуществлением информационного взаимодействия с почтовыми серверами на прикладном уровне модели взаимодействия открытых систем, определенной в ГОСТ 28906-91;

• события, связанные с функционированием почтовых серверов, средств контентной фильтрации электронной почты;

– события ИБ или их группа, информация о которых потенциально может быть использована для определения технических способов и схем реализаций угроз ИБ, а также события ИБ или их группа, информация о которых потенциально может быть использована для проведения идентификации субъектов, реализующих угрозы ИБ:

• события, связанные с осуществлением информационного взаимодействия на аппаратном

(физическом), сетевом, транспортном уровнях модели взаимодействия открытых систем, определенной в ГОСТ 28906-91;

• события, связанные с осуществлением информационного взаимодействия с почтовыми серверами на прикладном уровне модели взаимодействия открытых систем, определенной в ГОСТ 28906-91;

• события, связанные с функционированием почтовых серверов, средств контентной фильтрации электронной почты.

7.8. Для инцидентов ИБ, связанных с реализацией атак типа «отказ в обслуживании» (DDOS-атаки), реализуемых применительно к информационной инфраструктуре клиентов, систем ДБО и систем фронт-офиса организации БС РФ, рекомендуется рассмотрение следующих событий ИБ, значимых для цели поиска (выделения) и анализа содержательной (семантической) информации:

– исходные (базовые) события ИБ или их группа, являющиеся отправной точкой дальнейшего поиска и анализа:

• события, связанные с осуществлением информационного взаимодействия на сетевом уровне модели взаимодействия открытых систем, определенной в ГОСТ 28906-91;

– события ИБ или их группа, информация о которых потенциально может быть использована для определения технических способов и схем реализаций угроз ИБ:

• события, связанные с осуществлением информационного взаимодействия на сетевом и транспортном уровне модели взаимодействия открытых систем, определенной в ГОСТ 28906-91;

– события ИБ или их группа, информация о которых потенциально может быть использована для проведения идентификации субъектов, реализующих угрозы ИБ:

• события, связанные с изменением состояния информационной инфраструктуры СВТ бот-сетей;

• события, связанные с антивирусной защитой СВТ бот-сетей;

• события, связанные с осуществлением информационного взаимодействия информационной инфраструктуры СВТ бот-сетей на сетевом и транспортном уровнях модели взаимодействия открытых систем, определенной в ГОСТ 28906-91;

– события ИБ или их группа, информация о которых потенциально может быть использована для выявления маркеров «скрытого» несанкционированного управления объектами информационной инфраструктуры, используемых для осуществления переводов денежных средств:

• события, связанные с изменением состояния информационной инфраструктуры СВТ бот-сетей.

7.9. Для инцидентов ИБ, связанных с деструктивным воздействием компьютерных вирусов на информационную инфраструктуру организации БС РФ и клиентов, рекомендуется рассмотрение следующих событий ИБ, значимых для цели поиска (выделения) и анализа содержательной (семантической) информации:

– исходные (базовые) события ИБ или их группа, являющиеся отправной точкой дальнейшего поиска и анализа:

• события, связанные с изменением состояния информационной инфраструктуры размещения целевых систем и информационной инфраструктуры клиентов;

• события, связанные с функционированием средств защиты от несанкционированного доступа;

• события, связанные с антивирусной защитой;

– события ИБ или их группа, информация о которых потенциально может быть использована для определения технических способов и схем реализаций угроз ИБ:

• события, связанные с изменением состояния информационной инфраструктуры размещения целевых систем и информационной инфраструктуры клиентов;

• события, связанные с функционированием средств защиты от несанкционированного доступа;

• события, связанные с осуществлением информационного взаимодействия на аппаратном (физическом), сетевом, транспортном и прикладном уровнях модели взаимодействия открытых систем, определенной в ГОСТ 28906-91;

– события ИБ или их группа, информация о которых потенциально может быть использована для проведения идентификации субъектов, реализующих угрозы ИБ:

• события, связанные с антивирусной защитой;

• события, связанные с осуществлением информационного взаимодействия на аппаратном (физическом), сетевом, транспортном уровнях модели взаимодействия открытых систем, определенной в ГОСТ 28906-91;

– события ИБ или их группа, информация о которых потенциально может быть использована для выявления маркеров «скрытого» несанкционированного управления объектами информационной инфраструктуры, используемых для осуществления переводов денежных средств:

• события, связанные с изменением состояния информационной инфраструктуры размещения целевых систем и информационной инфраструктуры клиентов;

• события, связанные с функционированием средств защиты от несанкционированного доступа;

• события, связанные с антивирусной защитой;

• события, связанные с осуществлением информационного взаимодействия на прикладном уровне модели взаимодействия открытых систем, определенной в ГОСТ 28906-91.

7.10. Для событий ИБ, связанных с идентификацией и аутентификацией субъектов доступа в целевых системах и информационной инфраструктуре размещения целевых систем, информационной инфраструктуры клиентов, аналитику может быть рекомендовано рассмотрение следующей информации:

– энергонезависимые технические данные, расположенные на запоминающих устройствах СВТ:

• информация конфигурационных файлов данных операционных систем и приложений целевых систем, информация системного реестра операционной системы Windows:

а) конфигурационная информация, определяющая размещение файлов протоколов (журналов) регистрации (log-файлов) и временных файлов;

б) конфигурационная информация о составе пользователей – субъектов доступа, включая информацию о составе учетных записей пользователей, статусах учетных записей пользователей;

• информация протоколов (журналов) регистрации (system events, application events, audit records) операционных систем и приложений целевых систем:

а) информация, связанная с выполнением операций идентификации и аутентификации;

б) информация, связанная с изменением аутентификационных данных субъектов доступа;

– энергозависимые технические данные операционных систем и данные, расположенные в оперативной памяти СВТ:

• информация о сетевых соединениях;

• информация об открытых сессиях доступа;

– протоколы (журналы) регистрации целевых систем, средств (систем) аутентификации, авторизации и разграничения доступа, СУБД:

• информация о действиях и операциях, связанных с неуспешными попытками доступа к целевым системам, информационной инфраструктуре размещения целевых систем, информационной инфраструктуре клиентов, СУБД;

• информация об идентификации и аутентификации субъектов доступа в целевых системах, информационной инфраструктуре размещения целевых систем, информационной инфраструктуре клиентов, СУБД;

• информация о неуспешных попытках выполнения идентификации и аутентификации субъектов доступа в целевых системах, информационной инфраструктуре размещения целевых систем, информационной инфраструктуре клиентов и СУБД, в том числе связанных с невозможностью получения данных от систем аутентификации;

• информация, связанная с изменением аутентификационных данных субъектов доступа;

• информация о составе субъектов доступа, включая информацию о составе учетных записей субъектов доступа, статусах учетных записей субъектов доступа.

7.11. Для событий ИБ, связанных с осуществлением доступа к целевым системам и информационной инфраструктуре размещения целевых систем, аналитику может быть рекомендовано рассмотрение следующей информации:

– энергонезависимые технические данные, расположенные на запоминающих устройствах СВТ:

• информация конфигурационных файлов данных операционных систем и приложений целевых систем, информация системного реестра операционной системы Windows:

а) информация, определяющая размещение файлов протоколов (журналов) регистрации (log-файлов) и временных файлов;

б) информация о составе субъектов доступа, включая информацию о составе учетных записей субъектов доступа, статусах учетных записей субъектов доступа, о включении учетных записей субъектов доступа в группы;

в) информация о правах доступа, предоставленных субъектам доступа и группам;

г) информация о статусах учетных записей субъектов доступа;

д) информация о пользовательских настройках, информация о домашней директории пользователя – субъекта доступа;

• информация протоколов (журналов) регистрации (system events, application events, audit records) операционных систем и приложений целевых систем:

а) информация, связанная с выполнением авторизации субъектов доступа;

б) информация об истории выполненных субъектами доступа команд (command history);

г) информация об использовании субъектами доступа файлов данных (recently accessed files);

д) информация об использовании субъектами доступа ресурсов сети Интернет (история web-браузера);

– энергозависимые технические данные операционных систем и данные, расположенные в оперативной памяти СВТ:

• информация об операциях, связанных с осуществлением доступа к файлам данных;

• информация о сетевых соединениях;

• информация о запущенных программных процессах;

• информация об открытых файлах данных;

• информация об открытых сессиях доступа;

– протоколы (журналы) регистрации целевых систем, средств (систем) аутентификации, авторизации и разграничения доступа, СУБД:

• информация об операциях, связанных с управлением доступом субъектов доступа к целе-

вым системам, информационной инфраструктуре размещения целевых систем, информационной инфраструктуре клиентов, СУБД:

а) информация о составе учетных записей субъектов доступа, статусах учетных записей субъектов доступа;

б) информация о действиях и операциях, связанных с изменением состава и значений атрибутов учетных записей;

в) информация о действиях и операциях, связанных с блокированием (разблокированием) учетных записей;

г) информация о действиях и операциях, связанных с предоставлением, блокированием и (или) прекращением предоставления логического доступа;

д) информация о действиях и операциях, связанных с изменением прав доступа;

е) информация о действиях и операциях, связанных с созданием, изменением, удалением роли, группы;

ж) информация о действиях и операциях, связанных с изменением прав доступа роли, группы;

з) информация о действиях и операциях, связанных с назначением ролей (изменением состава групп);

• информация о действиях и операциях, связанных с осуществлением доступа субъектов доступа к целевым системам, информационной инфраструктуре размещения целевых систем, информационной инфраструктуре клиентов, СУБД:

а) информация об авторизации, завершении и (или) прерывании (приостановке) осуществления доступа;

б) информация о действиях и операциях, выполненных субъектами доступа;

в) информация о неуспешных попытках доступа;

г) информация о выполненных субъектами доступа действий и операций, для которых не требуется выполнения предварительной идентификации и аутентификации;

д) информация о выполненных DML-операторах, операторе SELECT- и DDL-операторах;

• информация об изменении конфигурационных данных целевых систем, информационной инфраструктуры целевых систем, СУБД;

• информация об атрибутах выполненных операций в целевых системах, информационной инфраструктуры целевых систем, СУБД:

а) информация о содержании выполненной операции;

б) дата и время осуществления операции;

в) результат выполнения операции (успешная или неуспешная);

г) идентификационные данные субъекта доступа, выполнившего операцию;

д) идентификационные данные СВТ, которое использовалось для выполнения операции.

7.12. Для событий ИБ, связанных с осуществлением удаленного доступа к целевым системам и информационной инфраструктуре размещения целевых систем, аналитику может быть рекомендовано рассмотрение следующей информации:

– энергонезависимые технические данные, расположенные на запоминающих устройствах СВТ:

• информация операционных систем о действиях и операциях по удаленному доступу к объектам файловой системы (загрузка, скачивание, создание, удаление файлов, получение доступа к файлам);

– энергозависимые технические данные операционных систем и данные, расположенные в оперативной памяти СВТ:

• информация о сетевых конфигурациях;

• информация о сетевых соединениях;

• информация об открытых сессиях доступа;

– протоколы (журналы) регистрации телекоммуникационного оборудования, средств межсетевого экранирования, средств обнаружения и предотвращения атак и данные сетевого трафика на сеансовом и прикладном уровнях модели взаимодействия открытых систем, определенной в ГОСТ 28906-91:

• информация об установке и окончании сессии взаимодействия на сеансовом уровне;

• информация об использованных идентификаторах субъектов доступа;

• информация о выполняемых операциях и командах, результатах их выполнения;

• информация о возможных реализациях вторжений (атак), в том числе информация о типе реализуемой атаки (например, атака типа «переполнение буфера», SQL-инъекция), об использованной уязвимости, результативности реализации атаки.

7.13. Для событий ИБ, связанных с изменением информационной инфраструктуры размещения целевых систем, информационной инфраструктуры клиентов, аналитику может быть рекомендовано рассмотрение следующей информации:

– энергонезависимые технические данные, расположенные на запоминающих устройствах СВТ:

• информация о составе и атрибутах файлов данных, в том числе исполняемых файлов данных, файлов данных программного обеспечения, командных файлов данных и скриптов, файлов данных, потенциально содержащих мобильный код и исполняемые макросы, файлов документов;

• информация о реализации операций с использованием функций файловой системы (операционной системы), в том числе самокопирование, захват иных файлов данных, передача файлов данных;

• информация конфигурационных файлов данных операционных систем и приложений целевых систем, информация системного реестра операционной системы Windows:

а) информация о программных сервисах, запускаемых автоматически при загрузке операционной системы;

б) информация об установленном программном обеспечении, его обновлениях;

в) информация об обновлениях операционной системы;

г) конфигурационная информация, определяющая размещение файлов протоколов (журналов) регистрации (log-файлов) и временных файлов;

д) информация о запланированных задачах (scheduled jobs), включая информацию о наименовании запланированной задачи, составе выполняемых команд, программ и операций запланированной задачи, планируемых датах и времени выполнения запланированной задачи;

• информация о составе и атрибутах скрытых и удаленных исполняемых файлов данных;

• информация о составе, атрибутах и содержании временных файлов данных;

• информация о порождаемых исполняемыми файлами данных программных процессах;

• информация о составе и атрибутах скрытых исполняемых файлов данных и исполняемых файлов данных, расположенных в скрытых директориях файловых систем;

• информация о составе и атрибутах исполняемых файлов данных, расположенных в неиспользуемых областях в пределах логических модулей выделения файлового пространства (file slack space);

• информация о составе и атрибутах исполняемых файлов данных, расположенных в неиспользуемом пространстве файловой системы (free space);

• содержательная информация об атрибутах и содержании файлов данных:

а) дата и время создания файла;

б) дата и время последней модификации файла;

в) дата и время последнего доступа к файлу;

г) дата и время последнего изменения атрибутов файла, в том числе атрибутов, связанных с изменением прав доступа к файлу и владельца файла данных (inode change);

д) размер файла данных, место размещения в файловой системе;

е) формат или структура файла данных;

ж) наличие объектов, внедренных в файл данных;

з) используемые (реализуемые) исполняемым файлом данных программных интерфейсах (API);

и) значение вычисления хэш-функции файла данных;

к) сетевые соединения, инициируемые или принимаемые исполняемыми файлами данных;

л) дополнительные атрибуты файлов данных файловой системы NTFS (alternate data stream, ADS);

• информация протоколов (журналов) регистрации (system events, application events, audit records) операционных систем и приложений целевых систем:

а) информация о загрузке и завершении работы операционной системы;

б) информация об изменении конфигурационных данных операционных систем;

в) информация о загрузке, выгрузке и изменении функционирования драйверов физических и виртуальных устройств;

г) информация об изменении состава или обновлении программного обеспечения;

д) информация о подключении и отключении устройств, в том числе отчуждаемых и мобильных устройств;

е) информация о запускаемых программных процессах и сервисах;

ж) информация о составе и работе системных служб (запуск, остановка, возобновление, завершение, удаление, блокирование системных служб);

з) информация об ошибках программного обеспечения;

и) информация об изменении состава запланированных задачах (scheduled jobs), операциях по управлению расписанием запланированных задач;

– энергозависимые технические данные операционных систем и данные, расположенные в оперативной памяти СВТ:

• информация, полученная из неиспользуемых областей в пределах логических страниц или блоков выделения пространства оперативной памяти (memory slack space);

• информация, полученная из неиспользуемого пространства оперативной памяти (memory free space, garbage);

• информация о сетевых конфигурациях;

• информация о сетевых соединениях;

• информация о запущенных программных процессах;

• информация об открытых файлах данных;

• информация об открытых сессиях доступа;

• информация о системных дате и времени операционной системы, включая информацию о часовом поясе;

– данные, связанные с функционированием СУБД:

• информация о создании резервных копий баз данных и их восстановлении из резервных копий;

• информация об изменении конфигурационных данных СУБД и баз данных;

• информация об операциях, связанных с созданием, вызовом, загрузкой программных модулей и хранимых процедур и функций, в том числе внешних хранимых процедур (DDL-процедур).

7.14. Для событий ИБ, связанных с антивирусной защитой, аналитику может быть рекомендовано рассмотрение следующей информации:

– информация о выполненных операциях по установке и обновлению средств антивирусной защиты;

– информация о выполненных операциях по обновлению сигнатурных баз средств антивирусной защиты;

– информация о фактах обнаружения и удаления (в том числе неуспешных) компьютерных вирусов;

– информация о выполненных операциях по отключению антивирусных средств;

– информация о выполненных операциях по проверке отсутствия компьютерных вирусов;

– информация о сбоях в работе средств антивирусной защиты;

– информация о результатах выполнения проверок целостности программных средств антивирусной защиты;

– информация о случаях выявления использования технологии мобильного кода (Java, Java-Script, ActiveX, VBScript и иные аналогичные технологии).

7.15. Для событий ИБ, связанных с выполнением криптографических преобразований, аналитику может быть рекомендовано рассмотрение следующей информации:

– информация о выполненных операциях по криптографическому преобразованию информации при осуществлении переводов денежных средств;

– информация о выполненных операциях проверки электронной подписи в рамках осуществления переводов денежных средств.

7.16. Для событий ИБ, связанных с функционированием средств защиты от несанкционированного доступа, аналитику может быть рекомендовано рассмотрение следующей информации:

– информация о запуске программных процессов и сервисов;

– информация об установке, обновлении и(или) изменении состава программного обеспечения;

– информация о результатах выполнения доверенной загрузки операционных систем;

– информация о результатах выполнения операций по контролю состава, целостности программного обеспечения, контроля состава программного обеспечения, запускаемого при загрузке операционной системы.

7.17. Для событий ИБ, связанных с осуществлением информационного взаимодействия на всех уровнях модели взаимодействия открытых систем, определенной в ГОСТ 28906-91, аналитику может быть рекомендовано рассмотрение следующей информации:

– протоколы (журналы) регистрации телекоммуникационного оборудования, средств межсетевого экранирования, средств обнаружения и предотвращения атак и данные сетевого трафика:

• информация аппаратного (физического) и канального уровней по семиуровневой стандартной модели взаимодействия открытых систем, определенной в ГОСТ 28906-91:

а) MAC-адреса сетевых карт источника и получателя данных;

б) данные о протоколе канального уровня (EtherType value);

в) информация об изменениях состояния сетевого интерфейса на аппаратном (физическом) и канальном уровне, в том числе подключение к вычислительной сети, изменение параметров, отключение от вычислительной сети, физическое отсоединение от сети;

• информация сетевого уровня по семиуровневой стандартной модели взаимодействия открытых систем, определенной в ГОСТ 28906-91:

а) IP-адреса источника и получателя данных;

б) дата, время и результаты обработки сетевых пакетов;

в) идентификатор и информация о протоколе сетевого и транспортного уровня (IP protocol number, например, TCP, UDP, ICMP);

г) базовая информация используемого протокола (например, номер порта TCP или UDP, ICMP-тип и код);

д) информация о результатах выполнения операций адресации и маршрутизации (status information) и возникающих при этом ошибках (error information);

е) информация об адресах, портах и результатах выполнения NAT-преобразований;

ж) информация о результатах установления и отклонения PROXY-соединений;

з) информация о назначении IP-адресов DHCP и DNS-сервисов, в том числе дата и время обработки назначения (высвобождения) IP-адреса, MAC-адреса средств вычислительной техники, результаты назначения IP-адреса, информация о соответствии MAC-адресов и IP-адресов;

и) информация VPN-шлюзов об установлении взаимодействия на сетевом уровне, в том числе IP-адреса источника и получателя данных, дата и время обработки сетевых пакетов;

к) информация о создании, активации, деактивации, удалении правил фильтрации информационных потоков;

л) информация о результатах применения правил фильтрации информационных потоков;

• информация транспортного уровня по семиуровневой стандартной модели взаимодействия открытых систем, определенной в ГОСТ 28906-91:

а) информация об установке и окончании соединений по протоколам TCP, UDP, ICMP;

б) информация о номерах сетевых портов (ports) источника и получателя данных протоколов TCP и UDP, которые потенциально могут указывать на программное обеспечение, используемое для обмена данными;

в) информация о состоянии интерфейсов транспортного уровня взаимодействия (сокетов), в том числе создание сокета, переход в режим ожидания соединения, отправка и прием запроса на соединение, завершение соединения, удаление сокета;

г) информация о создании, активации, деактивации, удалении правил фильтрации информационных потоков;

д) информация о результатах применения правил фильтрации информационных потоков;

• информация сеансового и прикладного уровня по семиуровневой стандартной модели взаимодействия открытых систем, определенной в ГОСТ 28906-91:

а) данные, передаваемые по протоколу NetFlow;

б) информация об установке и окончании сессии взаимодействия на сеансовом уровне;

в) идентификатор и информация о протоколе прикладного уровня;

г) информация об использованных идентификаторах субъектов доступа;

д) информация о выполняемых операциях и командах, результатах их выполнения;

е) информация о возможных реализациях вторжений (атак), в том числе информация о типе реализуемой атаки (например, атака типа «переполнение буфера», SQL-инъекция), об использованной уязвимости, результативности реализации атаки;

ж) информация о создании, активации, деактивации, удалении правил фильтрации информационных потоков;

з) информация о результатах применения правил фильтрации информационных потоков;

и) информация о создании, изменении, удалении доверительных отношений между доменами;

– протоколы (журналы) регистрации и данные почтовых серверов, средств контентной фильтрации электронной почты:

• информация «заголовков» почтовых сообщений:

а) информация о почтовых адресах отправителя и получателя почтового сообщения;

б) информация о дате и времени отправления почтовых сообщений;

в) информация о «теме» почтового сообщения;

г) информация об идентификационных номерах почтовых сообщений (message ID);

д) информация о типе почтового клиента, использованного для формирования почтового клиента;

е) информация о «степени важности» почтового сообщения;

ж) информация о маршрутизации почтового сообщения (перечень транзитных почтовых серверов прохождения почтового сообщения, дата и время приема почтового сообщения указанными почтовыми серверами);

• информация «тела» почтового сообщения:

а) содержание почтового сообщения;

б) информация о типе содержимого почтового сообщения (например, простой текст, наличие графики, наличие прикрепленных файлов);

в) информация о наличии прикрепленных файлов и содержание прикрепленных файлов;

г) информация о наличии и содержании гиперссылок;

– протоколы (журналы) регистрации и данных web-серверов, средств контентной фильтрации web-протоколов:

• информация о дате и времени получения запроса, результате выполнения запроса (status code);

• информация об IP-адресе инициатора запроса;

• информация о CBT, с использованием которого сформирован запрос:

а) информация о web-браузере, сформировавшем запрос;

б) информация об операционной системе средства вычислительной техники, использованного для формирования запроса;

• информация о типе запроса (получение данных, запись данных);

• информация о ресурсе доступа, в отношении которого выполнен запрос.

7.18. Особое внимание при анализе аналитику рекомендуется уделять следующей содержательной (семантической) информации.

Инциденты ИБ, связанные с НСД к объектам информационной инфраструктуры клиентов или информационной инфраструктуры целевых систем:

– информация о попытках подбора пароля, заключающаяся в наличии существенного количества попыток доступа с использованием «привилегированных» учетных записей, в том числе «встроенных» учетных записей (например, root, Administrator), результатом которых может являться успешная авторизация;

– информация о попытках осуществления доступа в нетипичное время (например, ночью). При

этом следует учитывать различия в возможных часовых поясах нахождения аналитика и места сбора технических данных;

– информация о нетипичном поведении субъектов доступа при осуществлении доступа (в том числе наличие существенного количества сбоев авторизации, слишком ранняя или слишком поздняя попытка доступа и авторизации, нехарактерная для данного пользователя активность при осуществлении доступа);

– информация о попытках осуществления доступа субъектами доступа к системам и ресурсам, которые не требуются ему для выполнения служебных обязанностей;

– информация о существенном изменении состава внешних IP/DNS-адресов либо наличии постоянного сетевого трафика на IP/DNS-адреса, находящиеся вне территории РФ, что может свидетельствовать о заражении средства вычислительной техники компьютерными вирусами;

– информация о попытках установления входящих соединений с IP-адресами, находящимися вне территории РФ;

– информация о попытках установления входящих соединений в обход эксплуатируемого VPN-шлюза;

– информация о доступе к протоколам (журналам), содержащим информацию о событиях ИБ.

Инциденты ИБ, связанные с реализацией атак типа «отказ в обслуживании» (DDOS-атаки), реализуемые применительно к информационной инфраструктуре клиентов, систем ДБО и систем фронт-офиса организации БС РФ:

– информация о предварительных признаках DDOS-атак в виде кратковременных, нетипичных «всплесков» сетевого трафика, которые могут свидетельствовать о проведении злоумышленниками тестирования устойчивости информационной инфраструктуры организации БС РФ к DDOS-атакам;

– сравнительная информация о составе IP-адресов в период осуществления DDOS-атаки и IP-адресов за определенный период до реализации DDOS-атаки, позволяющая идентифицировать реальные IP-адреса лиц, осуществляющие атаки;

– информация о наличии угроз (вымогательств), связанных с предполагаемым началом DDOS-атаки. Такие угрозы могут попадать в организацию БС РФ через общедоступные (информационные) почтовые ящики, официальных представителей (пресс-службы) организации БС РФ, а также через работников организации БС РФ, адреса которых есть у злоумышленника.

Инциденты ИБ, связанные с деструктивным воздействием компьютерных вирусов на информационную инфраструктуру организации БС РФ и клиентов:

– информация о дате и времени появления компьютерных вирусов на СВТ организации БС РФ;

– информация о выявлении антивирусными средствами компьютерных вирусов, о наличии «в карантине» антивирусного средства зараженных файлов за интересующий период времени и (или) диапазон дат;

– информация о классификации производителем антивирусного средства компьютерных вирусов и исходном местоположении выявленных компонентов компьютерных вирусов на СВТ организации БС РФ;

– информация о наличии постоянного и (или) периодического исходящего или входящего сетевого трафика небольшого объема на сетевые адреса за пределами РФ либо сетевые адреса, находящиеся в РФ, но не принадлежащие списку IP-адресов, с которыми организация ведет разрешенный обмен данными;

– информация о нетипичных маршрутах прохождения сетевого трафика и нетипичных маршрутных таблицах сетевого оборудования;

– информация о наличии посторонних программных процессов, похожих на системные программные процессы, но запущенные либо из нетипичного места (временные папки, папки перемещаемых профилей), либо программных процессов, имеющих схожее название с системными;

– информация о наличии файлов и папок, похожих на «системные» файлы и папки, но находящихся в отличном от стандартного размещения местоположении в файловой системе (например, папка Windows Update в корне папки Windows);

– информация о наличии нехарактерного для организации БС РФ программного обеспечения, запускаемого при запуске операционной системы СВТ, в том числе в папках автозагрузки, в службах, в системных драйверах, в системном реестре операционной системы Windows, в планировщике задач, в иных специфических местах, определяемых типом операционной системы;

– информация о наличии в протоколах (журналах) регистрации операционных систем или специализированного программного обеспечения данных о подключении устройств;

– информация о наличии в протоколах (журналах) регистрации серверов электронной почты входящих электронных сообщений с адресов электронной почты, имеющих схожее написание с доменами государственных учреждений, либо с доменов, переписка с которыми не характерна для деятельности организации БС РФ.

7.19. Для проведения анализа содержательной (семантической) информации аналитику могут быть рекомендованы следующие общие стратегии.

Стратегия анализа в определенном временном диапазоне, которая может быть использована в

случае наличия у аналитика сведений о дате и времени исходного (базового) интересующего события ИБ или их группы. Аналитику могут быть рекомендованы следующие методы анализа:

– анализ содержательной информации об атрибутах файлов данных с целью определения состава файлов данных и последующего анализа содержания файлов данных, созданных и (или) модифицированных за временной диапазон, связанный с инцидентом ИБ;

– анализ состава и содержания протоколов (журналов) регистрации за временной диапазон, связанный с инцидентом ИБ.

Стратегия анализа умышленно скрытых данных, которая предусматривает:

– проведение сравнительного анализа и расхождений содержания заголовков файлов данных (file header), расширений и структур файлов данных;

– анализ структуры и содержания зашифрованных файлов данных, файлов данных, защищенных паролями, в том числе архивов, файлов данных, содержимое которых сформировано с использованием методов «стеганографии»;

– анализ информации из скрытых областей накопителей на жестких магнитных дисках (host-protected area HPA):

– анализ внедренных объектов в файлы данных (например, в файлы документов);

– анализ возможного размещения файлов данных в нестандартных местах файловой системы. Стратегия сравнительного (корреляционного) анализа файлов данных и приложений, которая предусматривает:

– сопоставление состава файлов данных с установленными приложениями;

– сравнительный анализ состава и целостности исполняемых файлов данных на основе вычисления значений хэш-функций и эталонных значений;

– анализ возможной связи между файлами данных и (или) приложениями, например, соотнесение:

• данных журналов (протоколов) использования сети Интернет с кеш-файлами:

• файлов данных и файлов, содержащихся во вложении электронных почтовых сообщений;

– идентификация неизвестных типов файлов данных.

7.20. С целью идентификации субъектов, реализующих угрозы ИБ, аналитику может быть рекомендовано:

– определение владельца и места регистрации IP/DNS-адреса, с которого зафиксирована реализация угрозы ИБ или который был использован для реализации угрозы ИБ;

– проведение анализа атрибутов подозрительных или вредоносных файлов данных;

– проведение анализа временных параметров реализации угрозы ИБ (в том числе время наибольшей активности);

– проведение анализа временных параметров создания вредоносного кода и его отдельных компонентов;

– проведение анализа программного кода, использованного для реализации угрозы ИБ (например, вредоносного кода в файле данных, вредоносного скрипта, содержания «тела» почтового сообщения);

– проведение лингвистического (стилометрического) анализа текстов, сопровождающих реализацию угрозы ИБ (например, требование выкупа или шантажа);

– проведение анализа (пути) до потенциального нарушителя на следующих уровнях модели взаимодействия открытых систем, определенной в ГОСТ 28906-91:

• сетевом (трассировка или traceback);

• прикладном (например, путем анализа заголовков почтовых сообщений);

• уровне маршрутизации (путем анализа таблиц маршрутизации);

– проведение анализа получателей несанкционированных переводов денежных средств или денежных средств, в отношении которых совершено покушение на хищение.

При проведении идентификации субъектов, реализующих угрозы ИБ, аналитик должен учитывать наличие следующих особенностей:

– потенциальная возможность использования для реализации угроз ИБ промежуточных узлов (прокси-серверов или abuse-устойчивый хостинг), которые могут находиться в различных юрисдикциях;

– потенциальная возможность целенаправленного изменения нарушителями ИБ служебных заголовков в трафике на сетевом или прикладном уровне (например, в сообщениях почтовых серверов или сервисов) для цели сокрытия нарушителями своего реального местоположения;

– отсутствие в большинстве современных сетевых и прикладных протоколов способов достоверного определения источника отправления данных;

– отсутствие реализации проверки идентификационных данных при регистрации IP/DNS-адресов;

– использование подставных лиц для выполнения отдельных операций в рамках реализации угрозы (например, в качестве получателей переводов денежных средств).

7.21. Для обеспечения возможности проведения выделения и анализа содержательной (семантической) информации организации БС РФ рекомендуется обеспечить в распоряжении аналитика следующих технических средств и инструментов:

– технические средства и инструменты анализа данных файловых систем, позволяющие:

• проводить поиск, выделение и анализ содержательной (семантической) информации в составе подозрительных файлов данных, удаленных файлов данных, скрытых директориях файловых систем, в неиспользуемых областях в пределах логических модулей выделения файлового пространства (file slack space), в неиспользуемом пространстве файловой системы (free space);

• устанавливать типы обрабатываемых файлов данных по содержанию заголовков файлов данных (file header) и их структуре;

• просматривать содержимое файлов данных разных форматов;

• осуществлять извлечение файлов данных из архивов;

• просматривать структуру директорий файловой системы, в том числе в графическом виде;

• проводить контроль состава и целостности исполняемых файлов данных на основе вычисления значений хэш-функций и эталонных значений, содержащихся в соответствующих справочниках, в том числе разрабатываемых организацией БС РФ. В качестве справочных данных организацией БС РФ может использоваться информация о вычисленных эталонных значениях хэш-функций, размещенная в справочнике NIST's National Software Reference Library (NSRL) [2];

• осуществлять полнотекстовый поиск по «ключевым словам» и поиск по «шаблонам» в содержимом файлов данных;

• осуществлять поиск и анализ информации в атрибутах файлов данных;

– технические средства и инструменты анализа данных оперативной памяти СВТ, позволяющие:

• просматривать содержимое, осуществлять поиск на основе текстовых и цифровых «шаблонов», ключевых слов и проводить анализ больших массивов неструктурированной информации (hex editors);

– технические средства и инструменты анализа данных протоколов (журналов) сетевого оборудования и данных сетевого трафика, позволяющие:

• осуществлять централизованный сбор, хранение и анализ данных протоколов (журналов) сетевого оборудования;

• осуществлять реконструкцию действий и событий для отдельных сессий сетевого взаимодействия и (или) всех сессий сетевого взаимодействия за определенный временной период;

• осуществлять визуализацию сетевого взаимодействия между СВТ (хостами) и иными элементами информационной инфраструктуры целевых систем;

• осуществлять построение шаблонов и профилей «типовой» сетевой активности и выявлять существенные отклонения сетевой активности от построенных шаблонов и профилей;

• осуществлять поиск в данных сетевого трафика на основе текстовых и цифровых «шаблонов», ключевых слов, аномалий.

Рекомендации по составу технических средств выделения из технических данных содержательной (семантической) информации и ее анализа приведены в приложении В к настоящему стандарту.

7.22. При проведении выделения и анализа содержательной (семантической) информации аналитик должен учитывать наличие следующих возможных технических ограничений:

– хранение содержимого файлов данных в зашифрованном виде;

– парольная защита архивов файлов данных;

– сокрытие файлов содержимого файлов данных с использованием методов «стеганографии» и «обфускации»;

– использование вредоносного кода в содержимом архивных файлов, реализующего атаку типа «бомба разархивирования», предполагающую выполнение множественной повторяющейся операции разархивирования;

– использование вредоносного кода, реализующего выполнение множественной повторяющейся операции записи посторонних данных (шума) в оперативную память;

– использование вредоносного кода, обнаруживающего факт его анализа и пытающегося реализовать деструктивное воздействие на СВТ по факту своего обнаружения (например, перезаписать или уничтожить MBR-запись или зашифровать системные файлы на жестком магнитном диске);

– использование уникальных проприетарных форматов файлов данных;

– отсутствие должной синхронизации системного времени объектов информационной инфраструктуры – источников технических данных;

– использование накопителей на жестких магнитных дисках совместно с флеш-памятью, на которой сохранен пароль, необходимый для осуществления доступа к данным накопителя, в том числе в случаях, когда накопитель был извлечен из СВТ;

– шифрование или маскирование сетевого трафика;

– использование нетиповых номеров портов (ports) в рамках сетевого взаимодействия;

– сокрытие злоумышленником IP-адресов (spoofed IP addresses);

– регулярная смена злоумышленником IP/DNS-адресов;

– использование специальных алгоритмов генерации доменных имен;

– использование промежуточных узлов (в том числе нетипичных, например, принтеров), осложняющих идентификацию субъектов, реализующих угрозы ИБ. При этом необходимо учитывать, что угроза может быть реализована через узлы-посредники, владельцы которых не связаны с реализацией угрозы ИБ;

– сокрытие (инкапсуляция) вредоносной активности в разрешенных протоколах информационного взаимодействия (например, в DNS или HTTP/HTTPS).

7.23. Результаты выполнения аналитиком процедур и сервисных команд по выделению и анализу содержательной (семантической) информации должны быть документированы. Организации БС РФ рекомендуется формализовать правила документирования результатов выделения и анализа содержательной (семантической) информации. В правилах рекомендуется определить необходимость документирования:

– описания инцидента ИБ и его классификацию, выполненную с учетом содержания пункта 6.1 настоящего стандарта;

– описания состава собранных (используемых) технических данных;

– описания цели проведенного анализа собранных технических данных из числа определенных в пункте 7.1 настоящего стандарта;

– описания собранной первичной содержательной (семантической) информации, потенциально связанной с исходными (базовыми) событиями ИБ или их группой;

– описания использованных технических средств и инструментов, выполненных процедур и сервисных команд, связанных с обработкой технических данных. При этом описание должно обеспечивать возможность повторного выполнения указанных процедур и сервисных команд с исходными техническими данными;

– даты и времени выполнения процедур и сервисных команд по выделению и анализу содержательной (семантической) информации;

– содержания выделенной семантической информации;

– результатов анализа с максимально возможно подробным описанием:

• технических способов и схем реализаций угроз ИБ;

• результатов идентификации субъектов, реализующих угрозы ИБ;

• результатов выявления маркеров «скрытого» несанкционированного управления объектами информационной инфраструктуры;

– рекомендаций по сбору дополнительных технических данных с объектов информационной инфраструктуры, не принадлежащей организации БС РФ, например, протоколов (журналов) регистрации провайдеров сети Интернет или мобильных операторов связи;

– описания возможных вариантов интерпретации результатов анализа в случае отсутствия у аналитика однозначного вывода относительно инцидента ИБ;

– подробных выводов и рекомендаций, направленных на:

• совершенствование обеспечения ИБ организации БС РФ;

• устранение последствий инцидентов ИБ;

• устранение выявленных уязвимостей ИБ;

• инициирование взаимодействия с правоохранительными органами и (или) FinCert Банка России, а также иными организациями, проводящими мероприятия по реагированию на инциденты ИБ.

7.24. При определении содержания и детализации документов, содержащих результаты выполнения аналитиком процедур и сервисных команд по выделению и анализу содержательной (семантической) информации, организации БС РФ рекомендуется учитывать состав целевых получателей информации. Организации БС РФ рекомендуется рассматривать следующих потенциальных целевых получателей информации:

– руководство организации БС РФ, которому целесообразно обеспечить предоставление сводных аналитических отчетов обо всех выявленных инцидентах ИБ без указания детальных технических данных;

– технические подразделения организации БС РФ, служба ИБ, правоохранительные органы, FinCert Банка России, которым целесообразно обеспечить предоставление максимально подробных отчетов, содержащих подробное описание технических аспектов, связанных с инцидентом ИБ;

– подразделения по связям с общественностью или подразделения по работе с клиентами организации БС РФ, которым целесообразно обеспечить предоставление сводной информации без указания детальных технических данных, но направленной на повышение осведомленности в части возможных причин инцидента ИБ, которые могут быть интересны средствам массовой информации или клиентам организации БС РФ.

8. Рекомендации к распространению (передаче) выделенной и оформленной содержательной (семантической) информации

8.1. С целью получения методической и практической помощи в рамках выполнения процедур реагирования на инциденты ИБ организации БС РФ рекомендуется:

– обратиться в МВД России либо его территориальное подразделение с заявлением об оказании

содействия в реализации процедур реагирования на инцидент ИБ. Для подачи заявления в МВД России следует подготовить пакет следующих документов:

• заявление в свободной форме, к которому прилагается обзорная информация об инциденте ИБ – профиль инцидента ИБ, сформированный в соответствии с пунктом 6.1 настоящего стандарта. Заявление юридического лица пишется руководителем или уполномоченным лицом, действующим на основании соответствующей доверенности;

• выписка по расчетному или лицевому счету, подвергшемуся фактическому несанкционированному списанию денежных средств;

• для юридического лица – комплект правоустанавливающих документов юридического лица;

– обратиться в FinCert Банка России (контактные данные указаны на официальном сайте Банка России).

8.2. Организации БС РФ следует обеспечить возможность предоставления по запросам МВД России и (или) FinCert Банка России:

– документов, содержащих результаты выполнения аналитиком процедур и сервисных команд по выделению и анализу содержательной (семантической) информации, сформированных в соответствии с положениями пункта 7.13 настоящего стандарта;

– эталонных копий собранных исходных технических данных, сформированных в соответствии с положениями раздела 6 настоящего стандарта.

8.3. Организации БС РФ рекомендуется использование сервисов FinCert Банка России с целью:

– получения актуальной аналитической информации технического характера о выявленных в БС РФ инцидентах ИБ;

– использования полученной аналитической информации для цели своевременного выявления маркеров «скрытого» несанкционированного управления объектами информационной инфраструктуры в рамках процедур анализа содержательной (семантической) информации, проводимых в соответствии с положениями раздела 7 настоящего стандарта.

9. Рекомендации по распределению зон ответственности подразделений организации БС РФ в рамках процесса обработки технических данных

9.1. В рамках реализации процессов обработки технических данных рекомендуется участие следующих подразделений организации БС РФ:

– подразделение информатизации в части:

• обеспечения наличия технических данных путем должной настройки объектов информационной инфраструктуры для ведения протоколов (журналов) регистрации;

• обеспечения хранения протоколов (журналов) регистрации в течение как минимум трех лет;

• обеспечения необходимых технических средств для сбора и обработки технических данных;

• участия при необходимости в сборе технических данных;

• участия при необходимости в выделении и анализе содержательной (семантической) информации;

• предоставления содействия и информации, необходимых для проведения полноценного сбора технических данных, выделения и анализа содержательной (семантической) информации;

– служба ИБ в части:

• организации и проведения сбора технических данных;

• организации и проведения выделения и анализа содержательной (семантической) информации;

• разработки планов (регламентов) сбора технических данных, реализуемого в случае выявления инцидентов ИБ;

• формирования предложений по привлечению сторонних специалистов, а также по взаимодействию с правоохранительными органами, обращению в МВД России, FinCert Банка России;

• обеспечения и координации взаимодействия с правоохранительными органами и FinCert Банка России;

• обеспечения взаимодействия с клиентами организации БС РФ для получения технических данных, собранных клиентами;

• контроля обеспечения наличия технических данных;

– юридическая служба – в части привлечения представителей, которых целесообразно обеспечить при документировании результатов выделения и анализа содержательной (семантической) информации, предполагаемых к передаче в правоохранительные органы;

– подразделение, ответственное за операционную деятельность, обслуживание банковских карт – в части участия при необходимости в анализе содержательной (семантической) информации при выявлении инцидентов ИБ, связанных с переводами денежных средств, а также принятии решений о возможности отключения и (или) выведения из штатного режима объектов информационной инфраструктуры целевых систем;

– подразделение внутренней (физической) безопасности – в части сопровождения при необходимости работников организации БС РФ при сборе технических данных с информационной инфраструктуры клиентов;

– подразделение по связям с общественностью – в части обеспечения взаимодействия со средствами массовой информации.

9.2. Ответственных за выполнение ролей в рамках реализации процессов обработки технических данных рекомендуется включать в группу реагирования на инциденты ИБ, создаваемую в соответствии с РС БР ИББС-2.5.

9.3. Организации БС РФ рекомендуется выделение и назначение работникам службы ИБ отдельной функциональной роли (или выделение отдельного функционального подразделения), связанной с выполнением функций, определенных в пункте 9.1 настоящего раздела.

10. Рекомендации по взаимодействию с клиентами организации БС РФ в рамках процесса обработки технических данных

10.1. В случаях, когда в результате реализации инцидента ИБ пострадали клиенты – физические лица, организации БС РФ не рекомендуется определять для них существенный объем выполняемых процедур, связанных с обработкой технических данных.

10.2. Рекомендуемым решением является доведение до клиента – физического лица плана (регламента) действий, содержащего:

– условия возникновения необходимости выполнения плана (регламента), в том числе:

• спам-рассылки, реализуемые в рамках реализации методов «социального инжиниринга»;

• деструктивное воздействие компьютерных вирусов;

• обнаружение сайтов-двойников организации БС РФ («фишинговых» сайтов) в информационно-телекоммуникационной сети Интернет;

• несанкционированный перевод денежных средств;

– описание следующего порядка действий:

• фиксация и описание СВТ (настольные компьютеры, ноутбуки), используемого клиентом для осуществления доступа к системам ДБО, осуществляемые с учетом содержания пункта 6.6 настоящего стандарта;

• отключение СВТ, используемого клиентом для осуществления доступа к системам ДБО, путем прерывания питания[20] с последующим возможным извлечением запоминающих устройств;

• передачей запоминающего устройства в адрес организации БС РФ с обеспечением их безопасной упаковки, хранения и транспортировки, осуществляемых с учетом содержания пункта 6.7 настоящего стандарта.

10.3. Сбор технических данных с объектов информационной инфраструктуры клиентов – юридических лиц может осуществляться самостоятельно клиентами организации БС РФ. В этом случае организации БС РФ рекомендуется разработать детальный план (регламент) действий клиентов – юридических лиц по сбору и передаче организации БС РФ технических данных и обеспечить возможность доступа клиентов к содержанию указанного плана.

Выделение из технических данных, собранных клиентами, семантической (содержательной) информации и ее анализ рекомендуется выполнять организации БС РФ.

10.4. Выполнение клиентами – юридическими лицами сбора технических данных должно обеспечивать:

– реализацию принципов обработки технических данных, определенных в пункте 5.2 настоящего стандарта;

– реализацию рекомендаций по сбору технических данных, определенных в разделе 6 настоящего стандарта, в части сбора технических данных с информационной инфраструктуры клиентов.

В плане (регламенте) действий клиентов – юридических лиц по сбору и передаче организации БС РФ технических данных рекомендуется включать:

– перечень собираемых технических данных;

– приоритеты (последовательность) сбора технических данных;

– описание правил документирования выполненных процедур и сервисных команд при сборе технических данных;

– описание правил документирования места сбора технических данных;

– детальные инструкции по использованию технических средств, описание процедур и сервисных команд, необходимых для сбора технических данных;

– описание процедур и сервисных команд, в том числе технических, проверки (контроля) целостности собранных данных;

– требования к количеству создаваемых копий собираемых технических данных;

– описание правил маркирования безопасной упаковки, хранения и передачи в адрес организации БС РФ носителей собранных технических данных.

10.5. Для всех категорий клиентов организации БС РФ рекомендуется регламентировать и обеспечить возможность применения:

– формы обращения клиента с целью передачи носителей собранных технических данных;

– правил и формы актирования факта передачи носителей собранных технических данных;

– контактной информации для возможной передачи носителей собранных технических данных;

[20] Прерывание питания осуществляется с учетом описанных в разделе 6 особенностей данной операции.

– требований к составу передаваемой документации совместно с носителями технических данных;

– условий принятия организацией БС РФ собранных технических данных.

10.6. Сбор технических данных с информационной инфраструктуры клиентов работниками организации БС РФ следует осуществлять только при наличии уверенности организации БС РФ в их безопасности.

11. Рекомендации к компетенции персонала организации БС РФ и (или) иных внешних организаций, задействованных в процессах обработки технических данных

11.1. Организации БС РФ рекомендуется обеспечить наличие должной компетенции работников и (или) привлеченных специалистов для выполнения деятельности по сбору технических данных, поиску (выделению) содержательной (семантической) информации и анализу. Работники организации БС РФ, задействованные в сборе и обработке технических данных, должны:

– получить необходимые знания своих функций, прав и обязанностей, связанных со сбором и обработкой технических данных в рамках реагирования на инциденты ИБ;

– получить необходимые технические знания в части:

• возможного состава собираемых технических данных;

• условий возникновения необходимости сбора технических данных;

• возможного состава объектов информационной инфраструктуры организации БС РФ, являющихся объектами сбора технических данных;

• реализации технологических и технических процедур обработки технических данных в рамках реагирования на инциденты ИБ, использования необходимых технических средств и инструментов;

• установленных ограничений на выполнение отдельных процедур и сервисных команд, способных повредить и (или) уничтожить собираемые технические данные;

– получить необходимые знания в части состава и содержания принципов и процедур сбора и обработки технических данных, направленных на обеспечение относимости собранных и обрабатываемых технических данных к конкретному инциденту ИБ;

– получить необходимые знания в части состава и содержания принципов и процедур сбора и обработки технических данных, направленных на обеспечение сохранности (нераспространение) информации, защищаемой в соответствии с требованиями законодательства РФ, в том числе содержащей банковскую тайну и персональные данные.

Отдельное внимание организации БС РФ должно быть уделено вопросам регламентации и доведения до соответствующих работников организации БС РФ правил сбора технических данных с объектов информационной инфраструктуры, критичных для обеспечения непрерывности деятельности организации БС РФ, в том числе условиям возможного отключения и (или) выведения из штатного режима функционирования указанных объектов.

11.2. Организации БС РФ рекомендуется обеспечить наличие следующих знаний и компетенции аналитиков, выполняющих поиск (выделение) и анализ содержательной (семантической) информации:

– глубокое знание и понимание способов организации хранения технических данных в файловых системах для разных типов носителей информации (разделение на логические тома, логическое форматирование файловых систем, способов организации хранения файлов и директорий), которые потенциально могут быть источниками значимой (семантической) информации. К таким носителям информации могут быть отнесены:

• накопители на жестких магнитных дисках;

• накопители на гибких магнитных дисках (флоппи-диски);

• носители информации портативных компьютеров (планшетов), мобильных телефонов;

• CD-диски, DVD-диски;

• флеш-карты;

• оптические накопители;

• карты памяти (в том числе SD, PC Card, CF, MMC, Memory Stick).

Для получения дополнительной информации о составе возможных носителей информации и соответствующих файловых системах возможно использование рекомендаций, определенных в разделах 4.1.1 «File Storage Media» и 4.1.2 «FileSystems» NIST 800-86 Guide to Integrating Forensic Techniques into Incident Response [3].

– глубокое знание и понимание способов организации хранения как минимум в следующих файловых системах:

• операционные системы Windows и их файловые системы: FAT16, FAT32, NTFS;

• операционные системы Unix, Linux и их файловые системы: Unix File System (UFS), Second Extended Filesystem (ext2fs), Third Extended Filesystem (ext3fs), ReiserFS;

• операционная система MacOs и ее файловая система: Hierarchical File System (HFS), HFS Plus;

• CD-диски: Compact Disc File System (CDFS), ISO 9660, Joliet;

• DVD-диски: Universal Disc Format (UDF);

– глубокое понимание сетевых протоколов передачи данных TCP/IP и принципов их инкапсуляции:

• протоколов прикладного уровня, в том числе протоколов DNS, FTP, HTTP, SMTP, POP3, IMAP, SNMP;

• протоколов транспортного уровня, в том числе протоколов TCP, UDP, ICMP;

• протоколов сетевого уровня, в том числе протоколов IPv4, IPv6, IPSec;

• протоколов маршрутизации, в том числе протоколов RIP, OSPF, BGP;

• протоколов канального и физического уровня, в том числе протокола Ethernet и семейства протоколов 802.11;

• знание и понимание угроз ИБ, связанных с использованием вычислительных сетей, способов и техник реализации сетевых атак;

– знание и понимание организации вычислительных сетей (сетевой топологии) организации БС РФ, в том числе знание и понимание:

• сетевой архитектуры организации БС РФ;

• используемого организацией БС РФ сетевого и телекоммуникационного оборудования;

• IP-адресов ключевых (критических) программных сервисов, в первую очередь используемых для осуществления переводов денежных средств;

• номера используемых сетевых портов (ports) ключевых (критических) программных сервисов, в первую очередь используемых для осуществления переводов денежных средств;

– глубокое знание и понимание возможного содержания данных операционных систем, эксплуатируемых в пределах информационной инфраструктуры организации БС РФ:

• порядка загрузки операционных систем Windows, Linux и мобильных операционных систем;

• состава и возможного содержания конфигурационных файлов данных операционных систем;

• состава и возможного содержания протоколов (журналов) регистрации операционных систем;

• структуры и информации реестра операционной системы Windows;

• состава и возможного содержания информации, содержащейся в неиспользуемых областях в пределах логических страниц или блоков выделения пространства оперативной памяти (memory slack space);

• состав и возможное содержание информации, расположенной в неиспользуемом пространстве оперативной памяти (memory free space, garbage);

• состав и возможное содержание информации о сетевых конфигурациях, сетевых соединениях, запущенных программных процессах, открытых сессиях доступа;

– знание и понимание организации и правил эксплуатации информационной инфраструктуры организации БС РФ:

• состава СВТ и серверного оборудования;

• состава, правил размещения, возможного содержания протоколов (журналов) регистрации операционных систем, системного программного обеспечения, СУБД, почтовых серверов, web-серверов;

• состава, правил размещения, возможного содержания протоколов (журналов) регистрации средств защиты информации;

• состава, правил размещения, возможного содержания протоколов (журналов) регистрации программного обеспечения целевых систем.

11.3. Организации БС РФ как минимум следует обеспечить наличие должной компетенции работников и (или) привлеченных специалистов для выполнения деятельности по обеспечению наличия, хранения и сбора технических данных. В случае существенных инцидентов ИБ и отсутствия должной компетенции работников организации БС РФ к проведению необходимого выделения и анализа содержательной (семантической) информации организации БС РФ может быть рекомендовано обращение в FinCert Банка России. Соответствующий запрос с описанием инцидента ИБ – профиля инцидента ИБ, сформированного в соответствии с пунктом 6.1 настоящего стандарта, следует направить на электронный адрес fincert@cbr.ru.

12. Рекомендации по обеспечению наличия технических данных на этапах создания и эксплуатации информационной инфраструктуры

12.1. Для обеспечения наличия и сохранности технических данных для цели реагирования на инциденты ИБ организации БС РФ рекомендуется:

– установить ограничения и организовать контроль использования административных учетных записей для объектов информационной инфраструктуры, являющихся источниками технических данных;

– установить ограничения на совмещение одним лицом полномочий по использованию административных учетных записей разных объектов информационной инфраструктуры, являющихся источниками технических данных, в том числе установить ограничения на выполнение одним лицом функций администратора операционных систем, СУБД, целевых систем;

– принятие мер по мониторингу сообщений о выявленных уязвимостях объектов информационной инфраструктуры, являющихся источниками технических данных, и по реагированию на них в соответствии с РС БР ИББС-2.6, направленных на обеспечение невозможности использования уязвимостей для несанкционированного отключения

протоколирования и повреждения технических данных, сокрытия нарушителем своих действий;

– принятие мер по контролю фактического состава технических средств и систем – источников технических данных путем применения средств инвентаризации и оценки защищенности целевых систем;

– протоколирование всех действий с данными протоколов (журналов) регистрации, в том числе действий по отключению ведения и (или) очистке протоколов (журналов);

– принятие организационных мер по ограничению использования «непротоколируемых» административных учетных записей, например, путем разделения административного пароля на две части для цели реализации принципа «двойного контроля»;

– обеспечение постоянного формирования и контроля формирования технических данных – протоколов (журналов) регистрации, являющихся потенциальной содержательной (семантической) информацией, состав которой определен в пунктах 7.10-7.17 настоящего стандарта. Обеспечение ведения протоколов (журналов) регистрации реализуется путем соответствующего выбора, настройки и (или) создания следующих источников технических данных:

- операционные системы;
- целевые системы;
- средства (системы) аутентификации, авторизации и разграничения доступа;
- средства антивирусной защиты информационной инфраструктуры;
- средства криптографической защиты информации;
- средства защиты от несанкционированного доступа;
- маршрутизаторы и средства межсетевого экранирования, в том числе средства межсетевого экранирования прикладного уровня;
- DHCP- и DNS-сервисы;
- средства обнаружения вторжений и сетевых атак в информационную инфраструктуру;
- средства, используемые для предоставления удаленного доступа (VPN-шлюзы);
- почтовые серверы и средства контентной фильтрации электронной почты;
- web-серверы и средства контентной фильтрации web-протоколов;
- СУБД;

– обеспечить периодическое тестирование ведения протоколов (журналов) регистрации, например, путем периодического проведения тестирования на проникновение с имитацией возможных действий нарушителя по реализации инцидентов ИБ;

– обеспечивать адаптацию содержания протоколов (журналов) регистрации, состава источников технических данных, формирующих протоколы (журналы) регистрации, с учетом появления новых инцидентов ИБ, опыта организации БС РФ по реагированию на них.

12.2. Организации БС РФ рекомендуется учитывать, что разные технические средства и системы – источники технических данных могут формировать разный состав сведений об одном и том же инциденте ИБ. К примеру, целевая система может регистрировать факт выполнения несанкционированной операции, но не идентифицировать источник сообщения, инициировавшего операцию, на сетевом уровне взаимодействия. Средства защиты сетевого уровня могут регистрировать факт поступления сообщения и его источник, но не регистрировать операцию, инициированную сообщением. Таким образом, рекомендуется обеспечивать формирование, сбор и сопоставление всех возможных технических данных об инциденте ИБ с максимально возможной избыточностью.

12.3. Организации БС РФ рекомендуется обеспечить применение для всех целевых систем унифицированного состава технических средств и систем – источников технических данных, а также реализовать систему централизованного сбора и хранения протоколов (журналов) регистрации (например, SIEM систему).

При реализации системы централизованного сбора и хранения протоколов (журналов) регистрации рекомендуется обеспечить:

– централизованный сбор и хранение технических данных протоколов (журналов) регистрации, формируемых источниками технических данных, указанных в пункте 12.1 настоящего стандарта;

– реализация сбора технических данных путем комбинации следующих способов:

- путем периодического автоматического копирования протоколов (журналов) регистрации;
- путем получения данных, передаваемых с помощью протоколов аудита и диагностики (в том числе SYSLOG, SNMP);
- путем периодического сбора данных о фактическом составе технических средств и систем – источников технических данных путем использования средств инвентаризации и оценки защищенности, протоколов удаленного администрирования (системного сканирования);
- путем копирования сетевого трафика;

– контроль работоспособности технических средств, применяемых для сбора протоколов (журналов) регистрации;

– хранение собранных технических данных, в том числе архивное хранение, обеспечивающее:

- контроль и протоколирование доступа к собранным техническим данным;

• реализацию защитных мер, направленных на обеспечение конфиденциальности, целостности и доступности собранных технических данных;

• обеспечение запрета единоличного изменения и (или) удаления собранных технических данных;

• возможность установления сроков оперативного хранения технических данных;

• архивное хранение по истечении срока оперативного хранения, реализуемое при необходимости внешними системами архивного хранения;

• возможность доступа к архивным данным о событиях информационной безопасности для цели анализа в течение трех лет;

– реализацию защиты собранных технических данных от несанкционированного доступа, двустороннюю аутентификацию при использовании общедоступных вычислительных сетей, в том числе информационно-телекоммуникационной сети Интернет, для цели передачи указанных данных;

– гарантированную доставку данных о событиях информационной безопасности;

– приведение однотипных технических данных, формируемых разными источниками технических данных, к унифицированному формату;

– возможность объединения и корреляции технических данных, сформированных разными источниками технических данных, в пределах одного общего инцидента ИБ;

– приведение (синхронизация) временных меток записей электронных журналов событий ИБ к единому часовому поясу и единому эталонному времени, для чего рекомендуется:

• использование в качестве основного сигнала точного времени спутниковой системы «ГЛОНАСС»[21];

• использование в информационной инфраструктуре специального оборудования, содержащего в своем составе приемники сигналов спутниковой системы «ГЛОНАСС» – сервер времени информационной инфраструктуры (Time Server);

• осуществление синхронизации системного времени технических средств, являющихся источниками технических данных, с сервером времени информационной инфраструктуры с одновременным документированием выполнения этой операции;

• осуществление синхронизации системного времени видеорегистраторов, установленных в корпусах технических средств, являющихся источниками технических данных, систем видеонаблюдения и систем контроля доступа, с одновременным документированием выполнения этой операции.

[21] Допустимо использование интернет-сервисов точного времени, погрешность которых должна быть достаточной для целей выявления и анализа событий ИБ.