С. А. Толстая
Банк России

СИСТЕМОТЕХНИКА КОНТРОЛЬНЫХ МЕРОПРИЯТИЙ ОБЕСПЕЧЕНИЯ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ БАНКОВСКОЙ ОРГАНИЗАЦИИ

Процессы контроля обеспечения информационной безопасности (ИБ), реализованные в организации банковской системы Российской Федерации (далее — Организация), позволяют за счет своевременного и адекватного принятия мер избежать деградации системы обеспечения информационной безопасности (СОИБ) и обеспечить требуемый уровень ИБ Организации в течение длительного времени.

Целью контроля обеспечения ИБ Организации является обеспечение достаточной уверенности в том, что СОИБ функционирует эффективно, надлежащим образом (в соответствии с политикой ИБ или другим нормативным документам), адекватно существующим угрозам ИБ, а также внутренним и внешним условиям функционирования Организации.

Основные требования к контролю обеспечения ИБ можно сформулировать следующим образом:

· контроль должен проводиться регулярно, при этом периодичность контроля ИБ зависит от скорости снижения эффективности механизмов защиты (деградации свойств ИБ контролируемого объекта);

· процессы (процедуры) контроля ИБ должны быть определены во внутренних документах Организации и регламентированы (осуществляться в соответствии с регламентами, инструкциями, руководствами);

· должен быть соблюден принцип разделения полномочий между лицами, чья деятельность подлежит контролю, и лицами, осуществляющими контроль;

· результаты контроля ИБ должны быть объективными, достоверными, повторяемыми и точными (под объективностью понимается отсутствие предвзятости и субъективного отношения, под достоверностью понимается соответствие действительности, под точностью понимается соблюдение строгости в измерениях и максимальная близость к реальным данным);

· результаты выполнения процедур контроля ИБ должны документироваться, то есть подтверждаться документами, содержащими свидетельства и (или) результаты их выполнения;

· необходимо обеспечить доверие к результатам контроля.

Одновременное выполнение этих требований возможно только при реализации комплекса мероприятий контроля, объединенных в систему контрольных мероприятий в области обеспечения ИБ (далее — система контроля ИБ).

Для определения основных характеристик системы контроля ИБ Организации можно использовать комплекс документов Банка России «Обеспечение информационной безопасности организаций банковской системы Российской федерации» и основные положения базового стандарта комплекса СТО БР ИББС-1.0 «Обеспечение информационной безопасности организаций банковской системы Российской федерации. Общие положения» (далее — Стандарт).

В соответствии со Стандартом, СОИБ Организации представляет собой совокупность системы ИБ (СИБ) и системы менеджмента ИБ (СМИБ), где СИБ — это совокупность защитных мер, реализующих обеспечение ИБ Организации; СМИБ — это совокупность процессов менеджмента ИБ, включая ресурсное и административное (организационное) обеспечение этих процессов.

Согласно Стандарту, для обеспечения и поддержания ИБ в Организации необходима реализация четырех групп процессов, составляющих СМИБ Организации: планирование СОИБ Организации (планирование); реализация СОИБ Организации (реализация); мониторинг и анализ СОИБ Организации (проверка); поддержка и улучшение СОИБ Организации (совершенствование).

Группы процессов СМИБ Организации следует организовывать в виде циклической модели Деминга «…— планирование — реализация — проверка — совершенствование — планирование —…».

Контроль обеспечения ИБ Организации — деятельность в рамках группы процессов «проверка» СОИБ Организации, осуществляемая органами управления, подразделениями и служащими Организации и заключающаяся в проверке и оценке обеспечения ИБ Организации. Проверка и оценка обеспечения ИБ Организаций проводится путем выполнения следующих процессов: мониторинга ИБ; самооценки ИБ; внешнего аудита ИБ; анализа функционирования СОИБ; анализа СОИБ со стороны руководства.

Таким образом, *система контроля ИБ — это множество процессов контроля (в рамках группы процессов «проверка» СОИБ), находящихся в отношениях и связях друг с другом и взаимодействующих между собой для достижения общей цели контроля обеспечения ИБ Организации.*

Под *мониторингом информационной безопасности* Организации (мониторинг ИБ) понимается постоянное наблюдение за объектами и субъектами, влияющими на обеспечение информационной безопасности в Организации, а также сбор, анализ и обобщение указанных наблюдений. В понятие мониторинга ИБ заложена непрерывность процесса во времени — непрерывное наблюдение и регистрация событий, влияющих на ИБ. Эти события подвергаются анализу, на основе которого делается вывод о наличии или отсутствии инцидента ИБ. Под инцидентом ИБ понимается **с**обытие, вызывающее действительное, предпринимаемое или вероятное нарушение информационной безопасности **Организации.** Нарушение может вызываться либо ошибкой людей, либо неправильным функционированием технических средств, либо природными факторами, либо преднамеренными злоумышленными действиями, приводящими к нарушению конфиденциальности, целостности или доступности.

Основными целями мониторинга ИБ являются:

· выявление и анализ действий и событий, влияющих на обеспечение ИБ (выявление нештатных (в том числе злоумышленных) действий, выявление нарушений требований безопасности (инцидентам ИБ) и предоставление данных как по уже свершившимся, так и по потенциально возможным инцидентам ИБ);

· контроль за соблюдением требований ИБ, зафиксированных в политиках ИБ и других внутренних нормативных документах по обеспечению ИБ Организации;

· оперативное предоставление исходных данных для оценки и анализа рисков ИБ, для формирования корректирующих воздействий, минимизирующих риски ИБ или сводящих их к уровню допустимых, а также для предотвращения ошибок пользователей или минимизации их последствий.

Выполнение деятельности в рамках процесса «мониторинг ИБ» обеспечивает прозрачность используемых технологий (банковских технологических процессов), а также гарантирует их наблюдаемость в течение всего времени функционирования, что, как следствие, повышает уровень доверия бизнеса к данным технологиям.

Мониторинг ИБ способствует повышению чувства ответственности сотрудников Организации за свои действия, а, кроме того, знания потенциального нарушителя о наличии механизмов мониторинга во многих случаях выступают эффективным сдерживающим фактором нарушений ИБ.

Основными задачами деятельности в рамках процесса «мониторинг ИБ» являются:

· контроль и регистрация изменений в информационной сфере Организации, анализ соответствующих журналов регистрации;

· обнаружение и регистрация ошибок процедур генерации, хранения, обработки, передачи и использования информационных активов, анализ соответствующих журналов регистрации;

· наблюдение за информационной сферой Организации в целях выявления и регистрации инцидентов ИБ (успешных и безуспешных нарушений требований ИБ (политик ИБ)), анализ соответствующих журналов регистрации;

· определение действий, предпринимаемых в ответ на возникший инцидент ИБ, регистрация этих действий;

· регистрации других действий и событий, влияющих на обеспечение ИБ (например, действий и событий в системах, наиболее критичных с точки зрения функционирования бизнеса и подверженных высокой степени риска, это должно быть зафиксировано в соответствующих документах Организации), анализ соответствующих журналов регистрации;

· наблюдение за функционированием защитных мер, регистрация соответствующих событий, анализ журналов регистрации.

Для выполнения задач мониторинга ИБ могут использоваться как специализированные (например, программные) средства, так и штатные (входящие в коммерческие продукты и системы) средства регистрации действий пользователей, процессов и т. п.

Мониторинг ИБ проводится персоналом Организации, ответственным за ИБ.

Деятельность в рамках процесса «мониторинг ИБ» осуществляется с помощью следующих методов и механизмов:

· средства контроля топологии архитектуры и настроек оборудования автоматизированных банковских систем и средств защиты;

· инструментальные средства контроля реализации требований политик ИБ (для разных систем и разных технологических процессов), средства анализа журналов регистрации, системы агрегирования событий безопасности;

· сканеры защищенности;

· системы обнаружения вторжений;

· административный контроль выполнения требований ИБ, зафиксированных в политиках ИБ и других внутренних нормативных документах по обеспечению ИБ Организации, в том числе контроль соблюдения сотрудниками инструкций и регламентов;

· административный контроль исполнения поручений, планов работ и других распорядительных документов;

· контроль распространения документов и их использования;

· контроль документирования процедур (выполняемых действий).

***Самооценка информационной безопасности* Организации (самооценка ИБ)**: систематический и документируемый процесс получения свидетельств самооценки в деятельности Организации по обеспечению ИБ и определения степени выполнения в Организации установленных критериев самооценки ИБ. Самооценка ИБ выполняется самостоятельно сотрудниками Организации.

Основной целью самооценки ИБ является определение уровня соответствия защитных мер, процессов и процедур СОИБ (в зависимости от критериев самооценки) законодательству РФ, нормативным правовым актам Банка России, положениям стандартов (СТО БР ИББС-1.0, 27001), внутренним нормативным документам Организации, содержащим требования по ИБ (политики ИБ, положения, инструкции, регламенты и т. д.), потребностям Организации, контрактным требованиям Организации, условиям ведения бизнеса.

Кроме того, целями деятельности в рамках процесса «самооценка ИБ» могут быть подготовка к проведению внешнего аудита, разработка политик безопасности и других организационно-распорядительных документов по ИБ.

Основной задачей деятельности в рамках процесса «самооценка ИБ» является установление степени выполнения в Организации установленных критериев самооценки ИБ.

Самооценка ИБ проводится собственными силами и по инициативе руководства Организации.

Внешний аудит информационной безопасности Организации: систематический, независимый и документируемый процесс получения свидетельств аудита деятельности Организации по обеспечению

ИБ и установления степени выполнения в Организации установленных критериев аудита ИБ, проводимый внешней по отношению к проверяемой независимой проверяющей организацией.

Основной целью внешнего аудита ИБ является определение уровня ИБ Организации внешней независимой проверяющей организацией. Внешний аудит ИБ проводится как для собственных целей самой Организации, так и с целями повышения доверия к ней со стороны других организаций.

Основной задачей деятельности в рамках процесса «внешний аудит ИБ» является установление степени выполнения в Организации установленных критериев аудита ИБ.

Выполнение деятельности в рамках процесса «*анализ функционирования СОИБ*» позволяет:

· оценивать адекватность существующих механизмов защиты путем анализа инцидентов ИБ и выявления закономерностей в их появлении;

· определять, должным ли образом решаются задачи по обеспечению ИБ, возложенные на отдельных сотрудников и предусмотренные информационными технологиями, и спланировать корректирующие действия;

· определять неправильное или неэффективное использование ресурсов;

Выполнение деятельности в рамках процесса «анализ СОИБ со стороны руководства» позволяет принять обоснованные решения относительно использования мер защиты, адекватных с точки зрения соотношения их стоимости и возможности осуществления угроз ИБ.

Основные цели проведения анализа функционирования СОИБ могут быть сформулированы следующим образом:

· оценка эффективности СОИБ;

· оценка следования принципам ИБ и выполнения требований ИБ, закрепленным в политике ИБ Организации, а также в иных внутренних документах Организации;

· оценка соответствия СОИБ требованиям законодательства Российской Федерации и стандартов Банка России;

· определение и анализ проблем функционирования СОИБ;

· определение необходимости тактических улучшений СОИБ.

Основными задачами деятельности в рамках процесса «анализ функционирования СОИБ» являются:

· анализ результатов мониторинга ИБ, самооценки ИБ и внешнего аудита ИБ и подготовка на основе этого анализа данных для разработки плана мероприятий по устранению недостатков;

· оценка адекватности модели нарушителей и модели угроз Организации существующим нарушителям и угрозам ИБ;

· анализ отсутствия разрывов в технологических процессах обеспечения ИБ, а также несогласованности в использовании защитных мер;

· анализ рисков ИБ, сравнение с уровнем допустимых рисков;

· проверка адекватности используемых защитных мер результатам оценки рисков;

· оценка уровня остаточного риска при изменениях внутри организации и во внешней среде;

· оценка соответствия СОИБ требованиям внутренних документов Организации (в том числе политике ИБ);

· анализ соответствия комплекса внутренних документов, регламентирующих деятельность по обеспечению ИБ в Организации, требованиям законодательства Российской Федерации, требованиям стандартов Банка России, контрактным требованиям организации, угрозам ИБ и уязвимостям технологических процессов;

· анализ соответствия внутренних документов нижних уровней иерархии, регламентирующих деятельность по обеспечению ИБ в Организации, требованиям политик ИБ Организации;

· определение направлений тактических улучшений СОИБ;

· подготовка данных для анализа СОИБ руководством.

Анализ функционирования СОИБ проводится персоналом Организации, ответственным за обеспечение ИБ.

Основными целями процесса «*анализ СОИБ со стороны руководства*» являются:

· определение и анализ проблем функционирования СОИБ;

· определение необходимости стратегических улучшений СОИБ.

Основными задачами деятельности в рамках процесса «анализ СОИБ со стороны руководства» являются:

· анализ результатов мониторинга ИБ, самооценки ИБ, внешнего аудита ИБ, анализа функционирования СОИБ;

· пересмотр (при необходимости) уровня приемлемого риска;

· анализ уровня остаточного риска;

· анализ предложений заинтересованных сторон;

· определение направлений стратегических улучшений СОИБ.

Взаимосвязь процессов, входящих в систему контроля ИБ, иллюстрирует структурная схема, показанная на рис. 1.

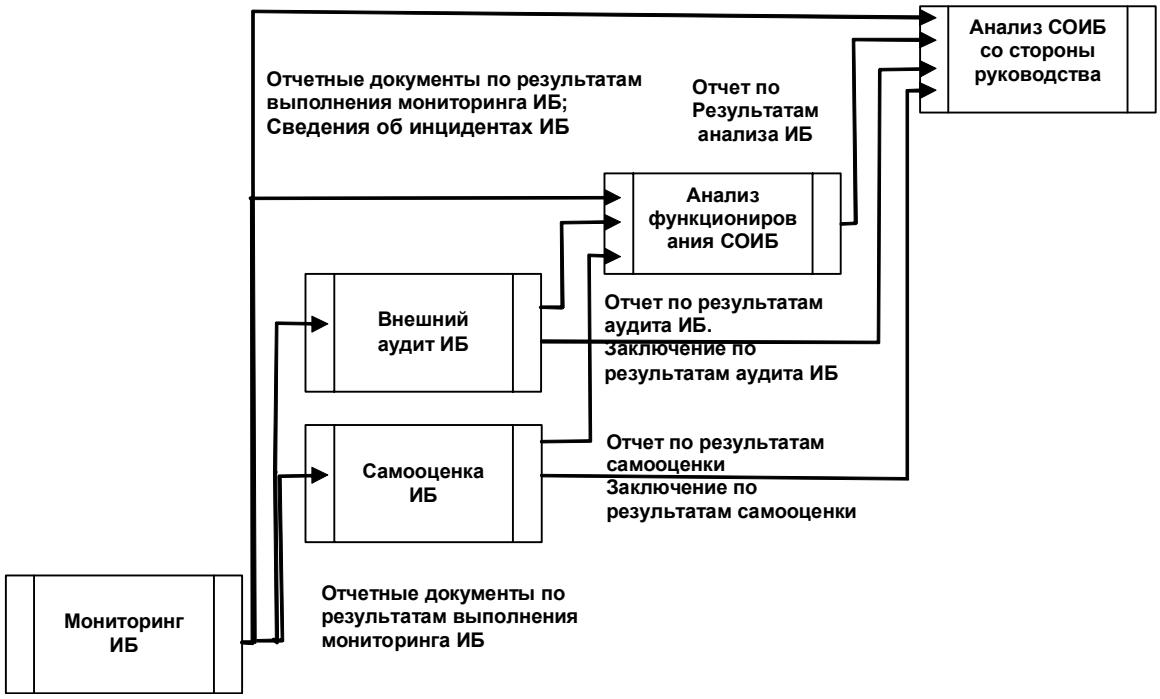

Рис. 1. Структурная схема системы контроля ИБ

Мониторинг ИБ осуществляется непрерывно. На основании проводимого мониторинга ИБ формируется оперативная оценка состояния СОИБ. Отчетные материалы по результатам мониторинга ИБ, в частности сведения о событиях и инцидентах ИБ, используются при проведении самооценки ИБ, внешнего аудита ИБ, анализа функционирования СОИБ, в том числе со стороны руководства.

Периодичность проведения самооценки ИБ и внешнего аудита ИБ зависит от скорости снижения эффективности защитных мер и процессов СОИБ и устанавливается во внутренних документах Организации. Результаты проведения самооценки ИБ и внешнего аудита ИБ используются при анализе функционирования СОИБ и анализе СОИБ со стороны руководства.

Анализ функционирования СОИБ по результатам мониторинга ИБ проводится постоянно. Кроме того, анализ функционирования СОИБ по результатам самооценки ИБ и внешнего аудита ИБ проводится после указанных мероприятий.

По результатам всех контрольных мероприятий формируются отчеты руководству, которые используются при проведении анализа СОИБ руководством. При этом форма и содержание указанных отчетов зависит от уровня руководителя (руководитель службы ИБ, руководитель, курирующий вопросы ИБ, высшее руководство Организации). Результаты всех контрольных мероприятий анализируются руководством Организации и используются для подготовки планов мероприятий по совершенствованию СОИБ.

Результаты контроля обеспечения ИБ используются для определения качественных или количественных показателей, позволяющих оценить эффективность СОИБ Организации, и являются основой для выполнения деятельности по совершенствованию СОИБ. Для того чтобы можно было доверять результатам контроля, они должны быть объективными, достоверными, повторяемыми и точными. Чтобы обеспечить доверие к результатам контроля, необходимо установить единую и формализовать систему контрольных мероприятий, определить цели, задачи, методы организации и требования к процессам контроля обеспечения ИБ, а также форму и содержание результатов.

Дальнейшее схемотехническое описание системы контроля ИБ Организации должно быть направлено на описание каждого процесса, входящего в систему. Для этого необходимо определить: цели и задач деятельности в рамках процесса; требования к деятельности в рамках процесса; входные и выходные данные для процесса; необходимые ресурсы; требования по управлению процессом.