РЕКОМЕНДАЦИИ В ОБЛАСТИ
СТАНДАРТИЗАЦИИ
БАНКА РОССИИ

РС БР ИББС-2.0-2007

ОБЕСПЕЧЕНИЕ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ ОРГАНИЗАЦИЙ БАНКОВСКОЙ СИСТЕМЫ РОССИЙСКОЙ ФЕДЕРАЦИИ

МЕТОДИЧЕСКИЕ РЕКОМЕНДАЦИИ ПО ДОКУМЕНТАЦИИ В ОБЛАСТИ ОБЕСПЕЧЕНИЯ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ В СООТВЕТСТВИИ С ТРЕБОВАНИЯМИ СТО БР ИББС-1.0

Дата введения: 2007-05-01

Москва
2007

Предисловие

1. ПРИНЯТЫ И ВВЕДЕНЫ в действие Распоряжением Банка России от 28 апреля 2007 года № Р-348.

2. ВВЕДЕНЫ ВПЕРВЫЕ.

Содержание

Введение

Адекватный потребностям бизнеса уровень информационной безопасности (ИБ) может быть обеспечен только на основе комплексного подхода, предполагающего планомерное использование правовых, организационных, программно-технических и других мер обеспечения ИБ на единой концептуальной и методической основе.

Для обеспечения согласованности, целенаправленности, планомерности деятельности по обеспечению ИБ эта деятельность должна быть документирована.

Документы по обеспечению ИБ позволяют определить и довести до каждого работника правила и требования по обеспечению ИБ, которыми он должен руководствоваться в своей производственной деятельности, а также определить порядок контроля за их соблюдением.

РЕКОМЕНДАЦИИ В ОБЛАСТИ СТАНДАРТИЗАЦИИ БАНКА РОССИИ

ОБЕСПЕЧЕНИЕ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ ОРГАНИЗАЦИЙ БАНКОВСКОЙ СИСТЕМЫ РОССИЙСКОЙ ФЕДЕРАЦИИ

МЕТОДИЧЕСКИЕ РЕКОМЕНДАЦИИ ПО ДОКУМЕНТАЦИИ В ОБЛАСТИ ОБЕСПЕЧЕНИЯ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ В СООТВЕТСТВИИ С ТРЕБОВАНИЯМИ СТО БР ИББС-1.0

Дата введения: 2007-05-01

1. Область применения

Настоящий документ распространяется на организации банковской системы (БС) Российской Федерации (РФ) и устанавливает рекомендации к структуре, составу, назначению и содержанию внутренних документов по обеспечению информационной безопасности организаций БС РФ в соответствии с требованиями стандарта Банка России СТО БР ИББС-1.0 “Обеспечение информационной безопасности организаций банковской системы Российской Федерации. Общие положения” (далее — СТО БР ИББС-1.0).

Настоящие рекомендации в области стандартизации рекомендованы для применения путем включения ссылок на них и(или) прямого использования устанавливаемых в них положений во внутренних документах организации БС РФ.

Рекомендации в области стандартизации применяются на добровольной основе, если только в отношении конкретных положений обязательность не установлена действующим законодательством Российской Федерации, нормативным актом Банка России или условиями договоров организации БС РФ со сторонними организациями.

2. Нормативные ссылки

В настоящих рекомендациях использованы нормативные ссылки на следующие стандарты:

ГОСТ Р 1.4-2004 Стандартизация в Российской Федерации. Стандарты организаций. Общие положения

СТО БР ИББС-1.0

3. Структура документов по обеспечению информационной безопасности

3.1. Деятельность организации БС РФ по обеспечению ИБ осуществляется на основе следующих документов:

- действующих законодательных актов и нормативных документов Российской Федерации по обеспечению ИБ;
- нормативных актов Банка России;
- внутренних документов организации БС РФ по обеспечению ИБ.

3.2. В состав внутренних документов организаций БС РФ по обеспечению ИБ рекомендуется включать следующие виды документов (документированной информации), организованных в виде приведенной на рисунке 1 иерархической структуры:

— документы, содержащие положения корпоративной политики ИБ организации БС РФ (документы первого уровня), определяют высокоуровневые цели, содержание и основные направления деятельности по обеспечению ИБ, предназначенные для организации в целом;
— документы, содержащие положения частных политик (документы второго уровня), детализируют положения корпоративной политики ИБ применительно к одной или нескольким областям ИБ, видам и технологиям деятельности организации БС РФ;
— документы, содержащие положения ИБ, применяемые к процедурам (порядку выполнения действий или операций) обеспечения ИБ (документы третьего уровня), содержат правила и параметры, устанавливающие способ осуществления и выполнения конкретных действий, связанных с ИБ, в рамках технологических процессов, используемых в организации БС РФ, либо ограничения по выполнению отдельных действий, связанных с реализацией защитных мер, в используемых технологических процессах (технические задания, регламенты, порядки, инструкции);
— документы, содержащие свидетельства выполненной деятельности по обеспечению ИБ (документы четвертого уровня), отражают достигнутые результаты (промежуточные и окончательные), относящиеся к обеспечению ИБ организации БС РФ.

Рисунок 1. Структура внутренних документов организации БС РФ по обеспечению ИБ

3.3. Рекомендуется, чтобы положения документов по обеспечению ИБ организации БС РФ:
— носили не рекомендательный, а обязательный характер;
— были выполнимыми и контролируемыми. Не рекомендуется включать в состав этих документов положения, контроль реализации которых затруднен или невозможен;
— были адекватны требованиям и условиям ведения деятельности (включая угрозы и риски ИБ), в том числе в условиях их изменчивости;
— не противоречили друг другу.

3.4. В состав документов организации БС РФ рекомендуется включить документ (классификатор), содержащий перечень и назначение всех документов организации БС РФ (для каждого из вышеопределенных уровней иерархической структуры), регламентирующих деятельность по обеспечению ИБ организации БС РФ. Указанный классификатор может быть полезен при осуществлении менеджмента документов организации БС РФ, для повышения степени осведомленности сотрудников организации БС РФ, а также при выполнении аудита информационной безопасности организации БС РФ.

3.5. При наличии у организации БС РФ сети филиалов (территориальных учреждений) в каждом из филиалов (территориальном учреждении) рекомендуется иметь единый для организации БС РФ, утвержденный комплект документов по обеспечению ИБ. В случае возникновения

необходимости учета специфики конкретных филиалов в них должны быть разработаны собственные документы, учитывающие эту специфику. Рекомендуется, чтобы документы по обеспечению ИБ филиала (территориального учреждения) организации БС РФ базировались на положениях документов по обеспечению ИБ, принятых головной организацией (центральным аппаратом) организации БС РФ, и не противоречили им.

3.6. Пример требований международного стандарта [1] к структуре (иерархии) и содержанию внутренних документов ИБ организации приведен в приложении А.

4. Состав внутренних документов по обеспечению информационной безопасности

4.1. Документы первого уровня

4.1.1. Корпоративная политика ИБ определяет на высоком (общем) уровне цели и задачи обеспечения ИБ организации БС РФ, включая способы контроля реализации требований политики ИБ организации БС РФ. Корпоративная политика ИБ организации БС РФ определяет содержание, назначение и требования к деятельности по обеспечению ИБ организации БС РФ без указания специфических деталей.

4.1.2. В корпоративной политике ИБ организации БС РФ рекомендуется определять высокоуровневые правила и требования к деятельности по управлению рисками, в том числе по анализу и выработке позиций в отношении рисков.

4.1.3. Корпоративная политика ИБ организации БС РФ[1] может быть представлена как в виде комплекта документов, так и в виде единого обобщающего документа.

4.1.4. В корпоративную политику ИБ организации БС РФ рекомендуется включать следующие положения:

- определение ИБ в терминах деятельности данной организации БС РФ, области действия политики, целей, задач и принципов обеспечения ИБ организации БС РФ;
- изложение намерения обеспечения ИБ, направленного на достижение указанных целей и на реализацию принципов обеспечения ИБ;
- общие сведения об активах, подлежащих защите, их классификацию;
- модели угроз и нарушителей (внутреннего и внешнего) в соответствии с требованиями раздела 7 СТО БР ИББС-1.0, на противодействие которым ориентирована корпоративная политика ИБ;
- высокоуровневое изложение правил и требований в области ИБ, представляющих особую важность для организации БС РФ, например:
- обеспечение соответствия законодательным актам, нормативным документам Российской Федерации в области обеспечения ИБ и нормативным актам Банка России;
- требования к управлению ИБ;
- требования по предотвращению и обнаружению компьютерных вирусов и другого вредоносного программного обеспечения;
- требования по управлению непрерывностью бизнеса;
- санкции и последствия нарушений политики безопасности;
- определение общих ролей и обязанностей, связанных с обеспечением ИБ, включая информирование об инцидентах ИБ;
- перечень частных политик ИБ, развивающих и детализирующих положения корпоративной политики ИБ, а также указание подразделений организации БС РФ, ответственных за их соблюдение и/или реализацию;
- положения по контролю реализации корпоративной политики информационной безопасности организации БС РФ;
- ответственность за реализацию и поддержку документа;
- условия пересмотра (выпуска новой редакции) документа.

4.1.5. К разработке и согласованию корпоративной политики ИБ рекомендуется привлекать представителей следующих служб организации БС РФ, связанных с ее информационной сферой:

- руководство организации БС РФ;
- профильные подразделения;
- служба информатизации;
- служба безопасности (информационной безопасности).

---

[1] В названии политики ИБ должно быть указано название организации, которой принадлежит политика.

4.1.6. Корпоративная политика ИБ должна быть утверждена руководителем организации БС РФ (например, председателем, генеральным директором, президентом, руководителем филиала).

4.2. Документы второго уровня

4.2.1. Второй уровень документов по обеспечению ИБ составляют документы, определяющие правила, требования и принципы, используемые применительно к отдельным областям ИБ, видам и технологиям деятельности организации БС РФ.

Кроме того, в состав документов данного уровня рекомендуется включить планы работ по обеспечению ИБ организации БС РФ и стандарты технологий обеспечения ИБ организации БС РФ.

4.2.2. Не рекомендуется повторение одинаковых правил в различных частных политиках. Включение в частную политику правила, содержащегося в другой (существующей) политике, целесообразно осуществлять посредством соответствующей ссылки. Например, для того чтобы в "Политику обеспечения ИБ информационных банковских технологических процессов" включить требования по антивирусной защите, следует сделать ссылку на "Политику антивирусной защиты" (при ее наличии).

4.2.3. Частные политики формируются на основании принципов, требований и задач, определенных в корпоративной политике ИБ организации БС РФ, с учетом детализации, уточнения и дополнительной классификации активов и угроз, определения владельцев активов, анализа, оценки рисков и возможных последствий реализаций угроз в границах области действия регламентируемой области или технологии.

4.2.4. В частные политики ИБ организации БС РФ рекомендуется включать положения, определяющие:

- цели и задачи ИБ, на обеспечение которых направлена частная политика;
- область действия политики, определение объектов (активов) защиты, уязвимостей, угроз и оценка рисков, связанных с объектами защиты;
- сведения о виде деятельности, на обеспечение ИБ которой направлено действие положений частной политики, о совокупности банковских технологий, применяемых в рамках выполнения данного вида деятельности, и об основных технологических процессах, реализующих указанные технологии;
- определение субъектов (ролей), на которых распространяется действие документа. В качестве субъектов (ролей) могут рассматриваться как структурные подразделения организации БС РФ, так и отдельные исполнители;
- содержательную часть документа (требования и правила);
- обязанности по обеспечению ИБ в рамках области действия частной политики ИБ, описание функций субъектов (ролей) над управляемыми объектами в рамках регламентируемых технологических процессов;
- состав ссылочных документов[1];
- положения по контролю реализации частной политики ИБ;
- ответственность за реализацию и поддержку документа;
- условия пересмотра документа.

4.2.5. В состав планов работ по обеспечению ИБ организации БС РФ рекомендуется включать, но не ограничиваться ими:

- планы по реализации и внедрению процедур, требований и мер обеспечения ИБ;
- планы мероприятий на случаи возможных инцидентов ИБ;
- планы мероприятий по обеспечению деятельности в рамках управления ИБ;
- планы мероприятий по управлению документами, связанными с обеспечением ИБ;
- планы работ по обслуживанию аппаратных средств и программных систем, используемых для обеспечения ИБ;
- планы мероприятий по обучению и повышению осведомленности служащих организации БС РФ.

4.2.6. В планах работ по обеспечению ИБ рекомендуется описывать перечень, порядок, объем (в той или иной форме), сроки выполнения мероприятий по реализации задач обеспечения ИБ организации БС РФ, а также указывать руководителей, исполнителей и ответственность за выполнение этих мероприятий.

---

[1] К ссылочным документам относятся документы, ознакомление с которыми обязательно для адекватного понимания текста политики ИБ. Например, если в тексте политики говорится о требованиях к конфиденциальной информации, то в ссылочных документах должен быть указан документ, определяющий перечень сведений, которые относятся к конфиденциальной информации.

4.2.7. Планы по обеспечению ИБ как минимум должны определять:
— последовательность выполнения мероприятий в рамках деятельности по обеспечению ИБ;
— сроки начала и окончания запланированных мероприятий;
— субъектов (лиц или структурные подразделения), ответственных за выполнение каждого указанного мероприятия.

4.2.8. Стандарты технологий обеспечения ИБ организации БС РФ устанавливают требования и характеристики, предназначенные для всеобщего и многократного использования, касающиеся обеспечения ИБ организации БС РФ. Стандарты технологий обеспечения ИБ организации БС РФ могут разрабатываться как в отношении специализированных технологий обеспечения ИБ, так и в отношении технологий, реализуемых банковскими информационными системами.

4.2.9. Структуру и содержание стандартов технологий обеспечения ИБ организации БС РФ рекомендуется разрабатывать на основе требований ГОСТ Р 1.4-2004.

4.2.10. К разработке и согласованию частных политик обеспечения ИБ рекомендуется привлекать представителей:
— руководства организации БС РФ и профильных подразделений;
— служб информатизации и безопасности.

4.2.11. Документы второго уровня могут быть утверждены руководителем организации БС РФ (профильного подразделения организации БС РФ), его заместителем по вопросам ИБ или иными должностными лицами, в компетенцию которых входят вопросы, отраженные в этих документах.

Примеры состава частных политик ИБ и состава планов ИБ, основанные на положениях СТО БР ИББС-1.0 и согласованные с положениями международного стандарта [2], приведены в приложении Б.

4.3. Документы третьего уровня

4.3.1. Третий уровень документов по обеспечению ИБ составляют документы, содержащие требования к процедурам обеспечения ИБ, выполняемым работниками в рамках технологических процессов, реализующих технологии, требования ИБ к которым определены в частных политиках организации БС РФ.

4.3.2. В документах, содержащих требования ИБ к процедурам, выполняемым как структурными подразделениями организации БС РФ, так и ее работниками, рекомендуется давать детализированные описания порядка выполняемых действий и(или) вводимых ограничений, что должно позволить четко определить правила выполнения задач обеспечения ИБ на каждом рабочем месте, для каждой роли ИБ, а также установить конкретную ответственность за выполнение предписанных требований.

4.3.3. К документам, содержащим требования ИБ к процедурам, относятся, например:
— инструкции по обеспечению ИБ, в том числе и должностные;
— руководства по обеспечению ИБ, например, по классификации активов;
— методические указания по обеспечению ИБ;
— документы, содержащие требования к конфигурациям.

4.3.4. Инструкции, руководства, методические указания по обеспечению ИБ содержат свод правил, устанавливающих порядок и способ выполнения отдельных операций по обеспечению ИБ.

4.3.5. К инструкциям, руководствам, методическим указаниям по обеспечению ИБ предъявляются повышенные требования четкости и ясности изложения текста. Документы этого уровня, в отличие от документов вышестоящего уровня, описывают конкретные приемы и порядок действий сотрудников для решения определенных им (например, ролью) задач либо конкретные ограничения.

4.3.6. Рекомендуется, чтобы инструкции, руководства, методические указания по обеспечению ИБ содержали:
— определение субъекта (субъектов), деятельность которых регламентируется инструкцией, и/или наименование деятельности, которая описывается инструкцией;
— ресурсы, необходимые для выполнения деятельности;
— детальное описание выполняемых операций, включая накладываемые ограничения, и результат выполнения операций;
— обязанности субъекта (субъектов) в рамках выполнения регламентируемой деятельности;
— права и ответственность субъекта (субъектов).

4.3.7. Документы, содержащие требования к конфигурациям, определяют конкретные значения параметров систем и их компонентов, а также способы их настройки, позволяющие обеспечить требуемый уровень ИБ.

4.3.8. Документы, содержащие процедурные требования ИБ, могут быть утверждены лицами, ответственными за реализацию соответствующих видов деятельности по обеспечению ИБ.

4.4. Документы четвертого уровня

4.4.1. Четвертый уровень документов по обеспечению ИБ составляют документы, содержащие записи о результатах реализации деятельности по обеспечению ИБ, регламентированной документами верхних уровней иерархии согласно структуре документов, представленной на рисунке 1. Свидетельства выполненной деятельности совместно с документами более высоких уровней иерархии могут служить документированным доказательством реализации требований ИБ при проведении внутреннего контроля и внешнего аудита ИБ организации БС РФ.

4.4.2. К этой группе документов относятся, например:

— реестры и описи (например, опись информационных активов организации БС РФ);
— регистрационные журналы, в том числе журналы регистрации инцидентов;
— протоколы (например, протокол проведения испытаний);
— листы ознакомления;
— обязательства (например, обязательства о неразглашении);
— акты;
— договоры;
— отчеты.

4.4.3. Наличие документов организации БС РФ, содержащих свидетельства выполненной деятельности по обеспечению ИБ, определяется требованиями, зафиксированными во внутренних документах по обеспечению ИБ верхних уровней иерархии.

4.4.4. Документы, содержащие свидетельства выполненной деятельности по обеспечению ИБ, могут быть представлены как в электронной форме, так и на бумажном носителе.

4.4.5. Рекомендуется по возможности дублировать документы, содержащие свидетельства выполненной деятельности по обеспечению ИБ, представленные в электронной форме, на бумажный носитель.

4.4.6. Должно обеспечиваться архивное хранение документов, содержащих свидетельства выполненной деятельности по обеспечению ИБ. Время хранения может определяться как требованиями законодательных актов Российской Федерации и требованиями Банка России, так и требованиями самой организации БС РФ.

5. Менеджмент документов по обеспечению информационной безопасности

5.1. Менеджмент документов по обеспечению ИБ направлен на обеспечение разработки, учета, использования, хранения, проверки, обновления (поддержания актуального состояния) и изменения документов по обеспечению ИБ организации БС РФ.

5.2. При осуществлении менеджмента документов по обеспечению ИБ рекомендуется предусмотреть документированные виды деятельности, с тем чтобы:

— обеспечить адекватность документов перед их утверждением и изданием;
— периодически пересматривать и при необходимости обновлять документы, а также утверждать их повторно;
— гарантировать возможность выявления изменений, вносимых в документы, и возможность определения текущего статуса документов;
— обеспечить уверенность в том, что требуемые документы доступны работникам организации БС РФ, а ее работники ознакомлены с требуемыми документами;
— обеспечить доступ к документам только тем работникам организации БС РФ, которые имеют отношение к этим документам;
— обеспечить реализацию защиты документов от несанкционированного изменения;
— обеспечить уверенность в том, что документы удобочитаемы и идентифицируемы;
— обеспечить выявление документов, созданных вне организации;
— предотвратить использование устаревших документов;
— использовать соответствующую маркировку для устаревших документов при их сохранении с какой-либо целью.

5.3. Менеджмент документов по обеспечению ИБ должен учитывать существующие требования законодательных актов и нормативных документов Российской Федерации, нормативных актов Банка России и внутренних документов организации БС РФ.

Приложение А
(справочное)

Пример требований международного стандарта ISO/IEC 13335-1 к структуре (иерархии) и содержанию внутренних документов ИБ организации

В данном приложении приведен пример требований международного стандарта ISO/IEC 13335-1 к составу и содержанию внутренних документов ИБ организации, соответствующий подразделам 4.2 и 4.3 указанного международного стандарта.

4.2. Иерархия политик

Корпоративная политика безопасности может состоять из принципов безопасности и указаний для организации в целом. Корпоративные политики безопасности должны отражать более широкие политики, включая те, которые касаются прав личности, требований и стандартов закона.

Политика информационной безопасности может содержать принципы и указания, относящиеся к защите информации, которая является чувствительной или важной для организации. Принципы, содержащиеся в политике информационной безопасности, извлекаются из принципов корпоративной политики безопасности и, таким образом, согласованы с ними.

Корпоративная политика безопасности информационных и коммуникационных технологий должна отражать существенные принципы безопасности информационных и коммуникационных технологий и указания, применимые к корпоративной политике безопасности и политике информационной безопасности, а также общие положения использования систем информационных и коммуникационных технологий внутри организации.

Политика безопасности систем информационных и коммуникационных технологий должна отражать принципы безопасности и указания, содержащиеся в корпоративной политике безопасности информационных и коммуникационных технологий. Она должна также содержать детали конкретных требований безопасности и защитных мер, подлежащих реализации, и процедур для правильного использования защитных мер с целью обеспечения адекватной безопасности. Во всех случаях важно, чтобы выбранный подход был эффективным по отношению к потребностям бизнеса организации.

Там, где это целесообразно, корпоративная политика безопасности информационных и коммуникационных технологий может быть включена в спектр политик — технических политик и политик менеджмента, которые все вместе образуют базис для корпоративной политики информационных и коммуникационных технологий. Эта политика должна включать некоторые убедительные слова о важности безопасности, особенно если безопасность необходима для согласования с этой политикой. На рисунке 2 показан пример возможного иерархического отношения политик. Независимо от документации и организационной структуры важно, чтобы учитывались различные положения описанных политик и поддерживалась согласованность между ними.

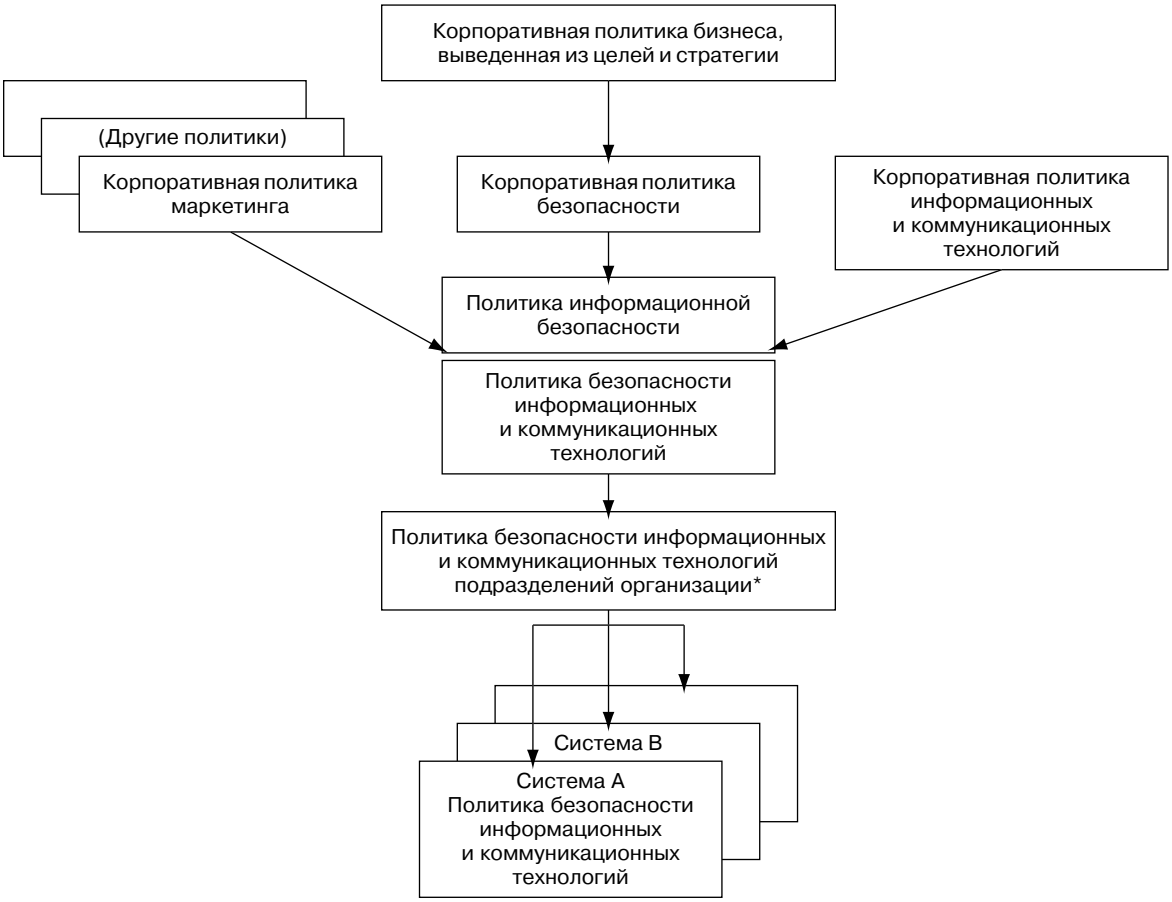
Другие, более детальные политики безопасности информационных и коммуникационных технологий требуются для специальных систем и услуг или группы систем и услуг информационных и коммуникационных технологий. Они обычно называются политиками безопасности систем информационных и коммуникационных технологий. Важным аспектом менеджмента является то, чтобы сфера и границы таких политик были четко определены, а сами политики были основаны на технических требованиях и требованиях бизнеса.

4.3. Элементы корпоративной политики безопасности информационных и коммуникационных технологий

Корпоративная политика безопасности информационных и коммуникационных технологий должна разрабатываться на основе принятых корпоративных целей и стратегии безопасности информационных и коммуникационных технологий. Необходимо установить и поддерживать корпоративную политику безопасности информационных и коммуникационных технологий, совместимую с политиками: законодательной, нормативной, корпоративного бизнеса, безопасности и информационных и коммуникационных технологий.

Чем больше организация полагается на информационные и коммуникационные технологии, тем более важной становится безопасность информационных и коммуникационных технологий, которая обеспечивает уверенность в том, что цели бизнеса будут достигнуты. При составлении корпоративной политики безопасности информационных и коммуникационных технологий должны учитываться характеристики культуры, среды и организации, поскольку они могут влиять на подход к безопасности.

Рисунок 2. Иерархия политик



* Глубина иерархии (число уровней) зависит от ряда факторов, например, размера организации.

Например, некоторые защитные меры, которые легко могут быть приняты в одной среде, могут стать полностью неприемлемыми в другой среде. Деятельности по безопасности, описанные в корпоративной политике безопасности информационных и коммуникационных технологий, могут быть основаны на целях и стратегии организации, на результатах предшествующего оценивания рисков безопасности и на анализах менеджмента, а также на результатах предпринятых действий, таких, как проверка соответствия безопасности реализованных защитных мер, мониторинга аудита, анализа безопасности информационных и коммуникационных технологий при повседневном использовании и отчетов по инцидентам безопасности. Любая серьезная угроза или уязвимость, обнаруженная в процессе этих деятельностей, должна быть рассмотрена с помощью корпоративной политики безопасности информационных и коммуникационных технологий, описывающей общий подход организации к решению таких проблем безопасности. Подробные действия описываются в различных политиках безопасности систем информационных и коммуникационных технологий или в других поддерживающих документах, например, в операционных процедурах безопасности.

При разработке корпоративной политики безопасности информационных и коммуникационных технологий должны участвовать представители следующих служб организации:

- аудит;
- законодательство;
- финансы;
- информационные системы (техники и пользователи);
- коммунальные услуги/инфраструктура (т.е., лица, ответственные за структуру зданий и мебель, электроснабжение и кондиционирование);
- персонал;
- безопасность;
- менеджмент бизнеса.

В соответствии с целями безопасности и стратегией, принятыми организацией для достижения своих целей, определен соответствующий уровень деталей для корпоративной политики безопасности информационных и коммуникационных технологий. Корпоративная полити-

ка безопасности информационных и коммуникационных технологий должна рассмотреть следующие общие области:

— сферу действия и назначение;
— цели безопасности относительно правовых и нормативных обязательств, а также цели бизнеса;
— требования безопасности информационных и коммуникационных технологий в терминах конфиденциальности, целостности, доступности, неотказуемости, учетности и аутентичности информации;
— ссылки к стандартам, на которых основывается политика;
— администрирование информационной безопасности, включая ответственности и полномочия, индивидуальные и организационные;
— подход менеджмента рисков, принятый организацией;
— способ определения приоритетов при реализации защитных мер;
— общий уровень безопасности и остаточного риска, найденный менеджментом;
— любые общие правила управления доступом (логический или физический доступ к зданиям, комнатам, системе и информации);
— подход к обучению и компетентности в вопросах безопасности в организации;
— общие процедуры, проверки и поддержки безопасности;
— общие вопросы безопасности персонала;
— способ ознакомления всех соответствующих лиц с политикой;
— обстоятельства, при которых политика должна пересматриваться или проходить аудит;
— метод контроля изменений в политике.

Организации должны оценивать свои требования, среду и культуру, чтобы определить специальные вопросы, которые наилучшим образом подходят для их обстоятельств. Такие вопросы могут включать:

— требования безопасности информационных и коммуникационных технологий, например, в терминах конфиденциальности, целостности, доступности, неотказуемости, учетности, аутентичности и надежности, особенно с точки зрения собственных активов;
— инфраструктуру организации и распределение ответственностей;
— интеграцию безопасности в разработку и снабжение системы;
— определение методов классификации информации и классов;
— стратегии менеджмента рисков;
— планирование непрерывности бизнеса;
— вопросы персонала (особое внимание должно уделяться персоналу, требующему доверия, например, обслуживающему персоналу и системным администраторам);
— компетентность и обучение;
— правовые и нормативные обязательства;
— менеджмент аутсорсинга;
— менеджмент инцидентов информационной безопасности.

Как обсуждалось ранее в этом подразделе, результаты предыдущего анализа оценивания рисков, проверка соответствия безопасности и инциденты информационной безопасности могут влиять на корпоративную политику безопасности информационных и коммуникационных технологий. Это, в свою очередь, может потребовать, чтобы ранее определенные стратегия или политика были пересмотрены или уточнены. Чтобы обеспечить адекватную поддержку всех мер, относящихся к безопасности, корпоративная политика безопасности информационных и коммуникационных технологий должна быть одобрена руководством.

На основе корпоративной политики безопасности информационных и коммуникационных технологий должны быть разработаны указания, обязательные для выполнения всеми менеджерами и служащими. Это может потребовать подписи на документе от каждого служащего, который признает за собой ответственность за безопасность внутри организации. Далее должна быть разработана и реализована Программа компетентности и обучения безопасности, в которой указываются все эти ответственности.

Должен быть назначен ответственный за корпоративную политику безопасности информационных и коммуникационных технологий и за обеспечение того, что эта политика отражает требования и действующий статус организации. Этот ответственный обычно является официальным лицом корпоративной безопасности информационных и коммуникационных технологий, который, кроме прочего, должен отвечать и за последующую деятельность, которая включает проверку соответствия безопасности, повторные анализы и аудиты, обработку инцидентов и слабостей безопасности и любые изменения в корпоративной политике безопасности информационных и коммуникационных технологий, которые могут оказаться необходимыми в результате проведения этих действий.

Приложение Б
(справочное)

Пример состава документов по обеспечению информационной безопасности

Б.1. В данном приложении приведен пример состава документационного обеспечения ИБ, основанный на положениях СТО БР ИББС-1.0, международного стандарта [2].

Б.2. Пример состава частных политик ИБ приведен в таблице Б.1.

Таблица Б.1. Пример состава частных политик ИБ

Частные политики ИБ
Политика использования электронной почты и ресурсов сети Интернет
Политика по обеспечению ИБ средствами антивирусной защиты
Политики мониторинга и менеджмента инцидентов информационной безопасности
Политика по обеспечению ИБ при управлении доступом и регистрации
Политика по обеспечению ИБ при назначении и распределении ролей и обеспечении доверия к персоналу
Политика по обеспечению ИБ банковских платежных технологических процессов
Политика по обеспечению ИБ банковских информационных технологических процессов

Б.3. Пример состава планов информационной безопасности и обоснования наличия таких планов приведены в таблице Б.2.

Таблица Б.2. Пример состава планов ИБ

Планы ИБ	Пункты стандартов
План аудита ИБ (внешнего и/или внутреннего)	СТО БР ИББС-1.0: 10
План действий после аудита ИБ	СТО БР ИББС-1.0: 5
План обучения в области обеспечения ИБ	СТО БР ИББС-1.0: 8.2.2
План обеспечения непрерывности бизнеса и восстановления после прерываний	СТО БР ИББС-1.0: 9.6

Библиография

[1] ISO/IEC 13335-1:2004 Information technology — Security techniques — Management of information and communications technology security — Part 1: Concepts and models for information and communications technology security management

[2] ISO/IEC 17799:2005 Information Technology — Code of practice for information security management

Ключевые слова: банковская система Российской Федерации, информационная безопасность, документация, политика информационной безопасности, положение информационной безопасности, инструкция информационной безопасности, требования информационной безопасности.