УТВЕРЖДАЮ

Председатель Правления
Национального банка
Республики Беларусь

_____ П.В.Каллаур

«16» июня 2020 г.

**ТЕХНИЧЕСКИЕ ТРЕБОВАНИЯ И ПРАВИЛА
ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ**

Информационные технологии и безопасность
ОБЕСПЕЧЕНИЕ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ БАНКОВ РЕСПУБЛИКИ БЕЛАРУСЬ
Рекомендации по документационному обеспечению деятельности в области обеспечения информационной безопасности в соответствии с требованиями ТТП ИБ 1.1 – 2020

Інфармацыйныя тэхналогіі і бяспека
ЗАБЕСПЯЧЭННЕ ІНФАРМАЦЫЙНАЙ БЯСПЕКІ БАНКАЎ РЭСПУБЛІКІ БЕЛАРУСЬ
Рэкамендацыі па дакументацыйнаму забеспячэнню дзейнасці ў галінезабеспячэння інфармацыйнай бяспекі ў адпаведнасці з патрабаваннямі ТТП ИБ 1.1– 2020

Национальный банк Республики Беларусь

Ключевые слова: банковская система Республики Беларусь, информационная безопасность, документация, политика информационной безопасности, положение информационной безопасности, инструкция информационной безопасности, требования информационной безопасности

Содержание

Введение

Приемлемый потребностям банковской системы Республики Беларусь уровень информационной безопасности может быть обеспечен на основе комплексного подхода, предполагающего планомерное использование правовых, организационных, программно-технических и других мер обеспечения информационной безопасности на единой концептуальной и методической основе.

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

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

ТЕХНИЧЕСКИЕ ТРЕБОВАНИЯ И ПРАВИЛА ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ

Информационные технологии и безопасность
ОБЕСПЕЧЕНИЕ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ БАНКОВ РЕСПУБЛИКИ БЕЛАРУСЬ
Рекомендации по документационному обеспечению деятельности в области обеспечения информационной безопасности в соответствии с требованиями ТТП ИБ 1.1 – 2020

Інфармацыйныя тэхналогіі і бяспека
ЗАБЕСПЯЧЭННЕ ІНФАРМАЦЫЙНАЙ БЯСПЕКІ БАНКАЎ РЭСПУБЛІКІ БЕЛАРУСЬ
Рэкамендацыі па дакументацыйнаму забеспячэнню дзейнасці ў галіне забеспячэння інфармацыйнай бяспекі ў адпаведнасці з патрабаваннямі ТТП ИБ 1.1 – 2020

Information Technology and Security
ENSURING THE INFORMATION SECURITY OF BANKS OF THE REPUBLIC OF BELARUS
Recommendations for the documentation of information security activities in accordance with the requirements of the TRR IS 1.1 – 2020

Датавведения2020-_-__

1 Область применения

Настоящие Технические требования и правила распространяются на банки и небанковская кредитно-финансовые организации Республики Беларусь, открытое акционерное общество «Банк развития Республики Беларусь» (далее – банковская система, БС)и устанавливает рекомендации к структуре, составу, назначению и содержанию внутренних документов по обеспечению информационной безопасности (далее – ИБ) организаций БС в соответствии с требованиями Технических требований и правил Национального банка Республики Беларусь (далее – Национальный банк) ТТП ИБ 1.1-2020 «Информационные технологии и безопасность. Обеспечение информационной безопасности банков Республики Беларусь. Общие положения и терминология» (далее – ТТП ИБ 1.1).

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.

Рекомендации в области стандартизации применяются на добровольной основе, если только в отношении конкретных положений обязательность не установлена действующим законодательством Республики Беларусь, нормативным актом Национального банка или условиями договоров организации БС со сторонними организациями.

Настоящие Технические требования и правила разработаны с учетом рекомендаций 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».

2 Нормативные ссылки

Нормативные документы, упомянутые в настоящих Технических требованиях и правилах, обязательны для их применения. Для датированных документов используют только указанные издания. Для недатированных документов используют самые последние издания (с учетом всех изменений).

В настоящих Технических требованиях и правилах использованы ссылки на следующие документы:

СТБ 1.5-2017 Правила построения, изложения, оформления и содержания технических кодексов установившейся практики и государственных стандартов;

СТБ 6.38-2016 Унифицированные системы документации Республики Беларусь. Система организационно-распорядительной документации. Требования к оформлению документов;

ТТП ИБ 1.1-2020 Информационные технологии и безопасность. Обеспечение информационной безопасности банков Республики Беларусь. Общие положения и терминология;

СТБ ISO/IEC 27002-2012 Информационные технологии. Методы обеспечения безопасности. Кодекс практики для менеджмента информационной безопасности.

3 Структура документов по обеспечению информационной безопасности

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

- действующих нормативных правовых актов (далее – НПА), технических нормативных правовых актов (далее – ТНПА) Республики Беларусь по обеспечению ИБ;
- нормативных правовых актов Национального банка;
- локальных нормативных правовых актов (далее – ЛНПА) организации БС по обеспечению ИБ.

3.2 В состав внутренних документов организаций БС 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 (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;
- документы, содержащие требования 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, либо ограничения по выполнению отдельных действий, связанных с реализацией защитных мер, в используемых технологических процессах (технические задания, регламенты, порядки, положения, инструкции);
- документы, содержащие свидетельства выполненной деятельности по обеспечению ИБ (документы четвертого уровня), отражают достигнутые результаты (промежуточные и окончательные), относящиеся к обеспечению ИБ организации БС.

Рисунок 1. Структура внутренних документов организации БС по обеспечению ИБ

3.3 Рекомендуется, чтобы положения документов по обеспечению ИБ организации БС:

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

3.5 При наличии у организации БС сети филиалов (территориальных учреждений) в каждом из филиалов (территориальном учреждении) рекомендуется иметь единый для организации БС, утвержденный комплект ЛНПА по обеспечению ИБ. В случае возникновения необходимости учета специфики конкретных филиалов в них должны быть разработаны собственные ЛНПА, учитывающие эту специфику. Рекомендуется, чтобы документы по обеспечению ИБ филиала (территориального учреждения) организации БС базировались на положениях документов по обеспечению ИБ, принятых головной организацией (центральным аппаратом) организации БС, и не противоречили им.

3.6 Пример требований стандарта [3] 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, включая способы контроля реализации требований политики ИБ организации БС. Корпоративная политика ИБ организации БС определяет содержание, назначение и требования к деятельности по обеспечению ИБ организации БС без указания специфических деталей.

4.1.2 В корпоративной политике ИБ организации БС Республики Беларусь 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 может быть представлена как в виде комплекта документов, так и в виде единого обобщающего документа. В названии политики ИБ должно быть указано название организации, которой принадлежит политика.

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

- определение ИБ в терминах деятельности данной организации БС, области действия политики ИБ, а также целей, задач и принципов обеспечения ИБ организации БС;
- 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 6ТТП ИБ 1.1-2020, на противодействие которым ориентирована корпоративная политика ИБ;
- высокоуровневое изложение правил и требований в области ИБ, представляющих особую важность для организации БС, например:
- обеспечение соответствия требованиям законодательства Республики Беларусь и НПА Национального банка в области обеспечения ИБ;
- требования к управлению ИБ;
- требования по предотвращению и обнаружению компьютерных вирусов и другого вредоносного программного обеспечения;
- требования по управлению непрерывностью информационной безопасности;
- 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, ответственных за их соблюдение и/или реализацию;
- положения по контролю реализации корпоративной политики информационной безопасности организации БС;
- 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, связанных с ее информационной сферой:

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

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

Кроме того, в состав документов данного уровня рекомендуется включить планы работ по

обеспечению ИБ организации БС и ЛНПА по обеспечению ИБ организации БС.

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, 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 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, 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;

Примечание – К ссылочным документам относятся документы, ознакомление с которыми обязательно для адекватного понимания текста политики ИБ. Например, если в тексте политики говорится о требованиях к информации, распространение и (или) предоставление которой ограничено и(или) служебной информации ограниченного распространения [1], то в ссылочных документах должен быть указан документ, определяющий перечень сведений, которые относятся к данной информации.

- 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 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.

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, а также указывать руководителей, исполнителей и ответственность за выполнение этих мероприятий.

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 устанавливают требования и характеристики, предназначенные для всеобщего и многократного использования, касающиеся обеспечения ИБ организации БС. Стандарты технологий обеспечения ИБ организации БС могут разрабатываться как в отношении специализированных технологий обеспечения ИБ, так и в отношении технологий, реализуемых банковскими информационными системами. Стандарты технологий обеспечения ИБ могут быть разработаны в виде ЛНПА или стандарта организации[2].

4.2.9 Структуру и содержание документов, описывающих стандарты технологий по обеспечению ИБ организации БС рекомендуется разрабатывать на основе требований СТБ 6.38-2016,СТБ 1.5-2017.

4.2.10 К разработке и согласованию частных политик обеспечения ИБ рекомендуется привлекать представителей:

- руководства организации БС и профильных подразделений;

- служб информатизации и безопасности.

4.2.11 Документы второго уровня могут быть утверждены руководителем организации БС (профильного подразделения организации БС), 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 ТТП ИБ 1.1-2020и СТБ ISO/IEC 27002-2012, 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.

4.3.2 В документах, содержащих требования ИБ к процедурам, выполняемым как структурными подразделениями организации БС, 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.

4.4.2 К этой группе документов относятся, например:

- реестры и описи (например, опись информационных активов организации БС);
- 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, 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 законодательства Республики Беларусь, нормативными актами Национального банка, так и требованиями ЛНПА самой организации БС.

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.

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, а ее работники ознакомлены с требуемыми документами;
- обеспечить доступ к документам только тем работникам организации БС, 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 законодательства Республики Беларусь, нормативные документыНационального банка и ЛНПА организации БС.

Приложение А
(справочное)

Пример требований стандарта ГОСТ Р ИСО/МЭК 13335-1-2006 к структуре (иерархии) и содержанию внутренних документов ИБ организации

В данном приложении приведен пример требований стандарта ГОСТ Р ИСО/МЭК 13335-1к составу и содержанию внутренних документов ИБ организации, соответствующий подразделам 4.2 и 4.3 указанных стандартов.

4.2 Иерархия политик

Политика безопасности организации может состоять из принципов безопасности и директив для организации в целом. Политика безопасности организации должна отражать более широкий круг аспектов политики организации, включая аспекты, которые касаются прав личности, законодательных требований и стандартов.

Политика информационной безопасности может содержать принципы и директивы, специфичные для защиты чувствительной и ценной или иной важной для организации информации. Содержащиеся в ней принципы строятся на основе принципов политики безопасности и, таким образом, согласованы с ними.

Политика безопасности информационно-телекоммуникационных технологий (далее – ИТТ) организации должна отражать существенные принципы безопасности ИТТ и директивы, применимые к политике безопасности и политике информационной безопасности, и порядок использования ИТТ в организации.

Политика безопасности ИТТ должна отражать принципы безопасности и директивы, содержащиеся в политике безопасности ИТТ организации. Она должна также содержать детали особых требований безопасности и защитных мер, подлежащих реализации, и процедуры правильного использования защитных мер для обеспечения адекватной безопасности. Во всех случаях важно, чтобы принятый подход был эффективен в отношении потребностей бизнеса организации.

В некоторых случаях политика безопасности ИТТ может быть включена в состав технической и управленческой политики организации, которые вместе составляют основу политики ИТТ. Эта политика должна содержать несколько убедительных положений важности безопасности, если она необходима для соблюдения данной политики. Пример иерархических отношений, которые могут возникать между политиками, показан на рисунке 3. Вне зависимости от организационной структуры или документации, принятой в организации, важно, чтобы учитывались различные стороны политики и поддерживалась их согласованность.

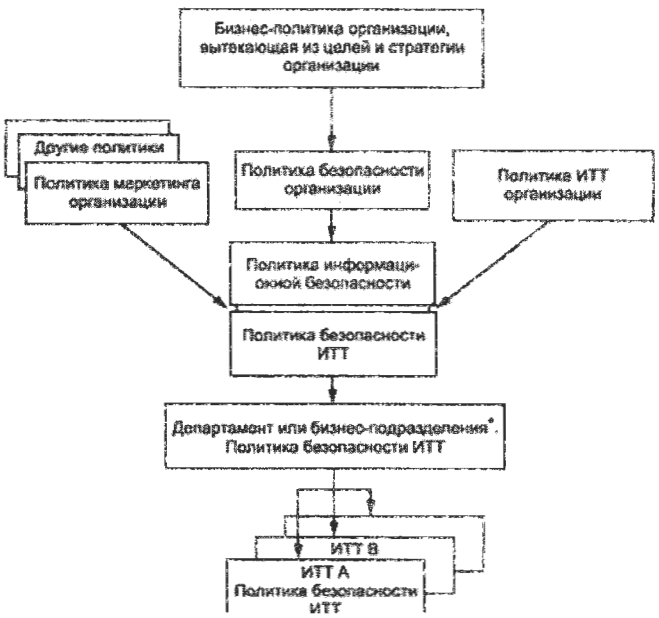

Рисунок 3 - Иерархия политик

* Глубина иерархии (число слов) зависит от нескольких факторов (например, размера организации).
Другие более детальные политики безопасности требуются для специфических систем и услуг или групп ИТТ и

услуг. Эти политики обычно известны как политики безопасности ИТТ. С позиций управления очень важно, чтобы их предмет и границы были ясны и базировались одновременно на бизнес-требованиях и технических требованиях.

4.3 Элементы политики безопасности информационно-телекоммуникационных технологий организации

Политика безопасности ИТТ должна формироваться, исходя из согласованных целей и стратегий безопасности ИТТ организации. Необходимо выработать и сохранять политику безопасности ИТТ, соответствующую законодательству, требованиям регулирующих органов, политике в области бизнеса, безопасности и политике ИТТ.

Чем более организация полагается на ИТТ, тем важнее ее безопасность, которая обеспечивает выполнение бизнес-задач. При формировании политики безопасности ИТТ следует помнить об особенностях культуры, окружающей среды организации, поскольку они влияют на подход к безопасности, например, на защитные меры, которые могут быть легко приняты в одной среде и быть абсолютно неприемлемы в другой. Деятельность в области безопасности, изложенная в политике безопасности ИТТ, может основываться на организационных целях и стратегиях, результатах предыдущих исследований по оценке и управлению риском, результатах мероприятий по сопровождению создаваемых защитных мер, мониторинге, аудите и анализе безопасности ИТТ в процессе текущей деятельности и отчетах об инцидентах безопасности. Любая серьезная угроза или уязвимость, замеченная в ходе данных мероприятий, должна быть соотнесена с политикой организации, описывающей общий подход к решению этих проблем безопасности. Детальные действия излагаются в различных политиках безопасности ИТТ или других вспомогательных документах, например, в организационных методах безопасности.

В разработке политики безопасности ИТТ организации должны принимать участие представители направлений, связанных с:

- аудитом;
- правом;
- финансами;
- информационными системами (специалисты и пользователи);
- коммунальными службами/инфраструктурой (лица, отвечающие за здания, размещение, электроснабжение и кондиционирование);
- персоналом;
- безопасностью;
- руководством.

В соответствии с целями безопасности и стратегией, принятой организацией для достижения этих целей, определяется надлежащий уровень детализации политики безопасности ИТТ организации. Политика безопасности ИТТ должна распространяться на:

- предмет и задачи безопасности;
- цели безопасности с учетом правовых и регулирующих обязательств, а также с учетом бизнес-целей;
- требования безопасности ИТТ к обеспечению конфиденциальности, целостности, доступности, безотказности, подотчетности и аутентичности информации и средств ее обработки;
- ссылки на стандарты, лежащие в основе данной политики;
- администрирование информационной безопасности, охватывающее организационные и индивидуальные ответственности и полномочия;
- подход к управлению риском, принятый в организации;
- метод определения приоритетов реализации защитных мер;
- уровень безопасности и остаточный риск, определяемый руководством организации;
- общие правила контроля доступа (логический контроль доступа, а также контроль физического доступа в здания, помещения, к системам и информации);
- подходы к осведомленности о безопасности и повышение квалификации в области безопасности в рамках организации;
- процедуры проверки и поддержания безопасности;
- общие вопросы защиты персонала;
- способы, которыми политика безопасности будет доведена до сведения всех заинтересованных лиц;
- условия анализа или аудита политики безопасности;
- метод контроля изменений в политике безопасности.

Организации должны оценить свои требования, окружающую среду и уровень развития и определить наиболее отвечающую им специфическую проблему безопасности. Эта проблема включает в себя:

- требования безопасности ИТТ, например, требования конфиденциальности, целостности,

доступности, неотказуемости, аутентичности и достоверности, особенно с учетом мнений владельцев активов;

- организационную инфраструктуру и распределение обязанностей;
- интеграцию безопасности при совершенствовании системы и закупках;
- определение методов и уровней классификации информации;
- стратегию управления рисками;
- планирование непрерывности Информационной безопасности;
- вопросы, связанные с персоналом (особое внимание должно быть уделено персоналу, занимающему ответственные должности, такому как технический персонал и системные администраторы);
- осведомленность и обучение персонала;
- правовые и регулирующие обязательства;
- менеджмент, осуществляемый независимым экспертом;
- управление инцидентами информационной безопасности.

Как отмечено выше, результаты исследований по оценке риска, проверок соответствия безопасности и инцидентов безопасности могут оказывать влияние на политику безопасности ИТТ организации. Это, в свою очередь, может потребовать пересмотра или совершенствования ранее определенной стратегии или политики безопасности.

Для обеспечения адекватной поддержки всех связанных с безопасностью мер политика безопасности ИТТ должна быть одобрена руководством организации.

На основе политики безопасности ИТТ должны быть подготовлены директивные указания, обязательные для всех руководителей и сотрудников организации. Это может потребовать подписания каждым сотрудником документа, подтверждающего его обязанности в рамках безопасности данной организации. Далее следует развивать и осуществлять программу осведомленности о безопасности, разъясняющую эти обязанности.

Должен быть назначен ответственный за политику безопасности ИТТ, который должен обеспечивать соответствие политики требованиям и актуальному статусу данной организации. Обычно им является сотрудник службы безопасности, который несет ответственность за следующие действия: проверку соответствия безопасности, ревизию, аудит, обработку инцидентов, выявление слабых мест в безопасности и внесение изменений в политику безопасности ИТТ организации, которые могут потребоваться по результатам подобных 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 ТТП ИБ 1.1-2020, стандарта СТБ ISO/IEC 27002-2012.

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 приведены в таблице Б.2.

Таблица Б.2 Пример состава планов ИБ

Планы ИБ
План аудита ИБ (внешнего и/или внутреннего)
План действий после аудита ИБ
План обучения в области обеспечения ИБ
План обеспечения непрерывности информационной безопасности и восстановления после прерываний

Библиография

[1] Закон Республики Беларусь от 10.11.2008 № 455-З «Об информации, информатизации и защите информации»
[2] Закон Республики Беларусь от 05.01.2004 № 262-З «О техническом нормировании и стандартизации»
[3] ГОСТ Р ИСО/МЭК 13335-1-2006 «Информационная технология. Методы и средства обеспечения безопасности. Часть 1. Концепция и модели менеджмента безопасности информационных и телекоммуникационных технологий»