ТЕХНИЧЕСКИЙ КОДЕКС УСТАНОВИВШЕЙСЯ ПРАКТИКИ

ТКП 288-2010 (07040)

Банковские технологии
Управление рисками в сфере информационных технологий

Банкаўскія тэхналогіі
Упраўленне рызыкамі у сферы інфармацыйных тэхналогій

Издание официальное

Национальный банк Республики Беларусь
Минск

УДК МКС 35.240.40 КП 05

Ключевые слова: банковские технологии, информационные технологии, управление рисками, внутренний контроль, информационные системы, программные средства,

Предисловие

1 РАЗРАБОТАН Открытым акционерным обществом «Центр банковских технологий»
ВНЕСЕН Национальным банком Республики Беларусь

2 УТВЕРЖДЕН И ВВЕДЕН В ДЕЙСТВИЕ постановлением Правления Национального банка Республики Беларусь от 10.12.2010 № 540

3 ВВЕДЕН ВПЕРВЫЕ

Издан на русском языке

Содержание

Введение

1. Общие положения

Технический кодекс направлен на применение процессного подхода для создания, реализации, контроля, анализа, поддержания и совершенствования системы управления рисками в сфере банковских информационных технологий (далее – СУРИТ) являющейся частью общей системы управления операционными рисками банка.

Целью СУРИТ в банке являются:

– эффективность и результативность финансовой и хозяйственной деятельности банка при совершении банковских операций и других сделок, эффективность управления банковскими рисками, активами и пассивами, включая обеспечение сохранности активов банка;

– достоверность, полнота, объективность и своевременность составления и представления финансовой, бухгалтерской, статистической и иной отчетности (для внешних и внутренних пользователей), а также информационная безопасность;

– соблюдение банком и его работниками требований законодательства Республики Беларусь, локальных нормативных правовых актов банка;

– исключение вовлечения банка в финансовые операции, имеющие незаконный характер, в том числе предупреждение и пресечение деяний, связанных с легализацией доходов, полученных преступным путем, и финансированием террористической деятельности, а также своевременное представление в соответствии с законодательством Республики Беларусь сведений в государственные органы.

Применение в банке системы процессов наряду с их идентификацией и взаимодействием, а также управление процессами, направленное на получение желаемого результата, может называться «процессный подход».

Преимущество процессного подхода состоит в непрерывности управления, которое он обеспечивает на стыке отдельных процессов в рамках системы процессов, а также при их комбинации и взаимодействии.

СУРИТ включает следующие процессы:

– планирование (создание СУРИТ) – установление политики, целей, процессов и процедур, относящихся к управлению ИТ-рисками для достижения результатов в соответствии с общей политикой и целями банка;

– осуществление (реализация СУРИТ) – реализация и эксплуатация политики, средств управления, процессов и процедур в области СУРИТ;

– проверка (контроль и анализ СУРИТ) – оценка и, где применимо, измерение показателей процессов по отношению к политике, целям и практическому опыту в области СУРИТ;

– действие (поддержка и совершенствование СУРИТ) – осуществление действий по исправлению и предупреждению недостатков СУРИТ, основанных на результатах внутреннего аудита СУРИТ или другой соответствующей информации, для достижения непрерывного совершенствования СУРИТ.

2. Совместимость с другими системами управления

Технический кодекс может применяться наряду с СТБ П ISO/IEC 27001-2008, СТБ П 34.101.41-2009, СТБ П 34.101.42-2009, ISO/IEC 13335-1:2004 и ISO/IEC TR 13335-3:2007 с целью обеспечения постоянной комплексной реализации и эксплуатации сопутствующих стандартов по управлению инфраструктурой информационных технологий. Одна система управления, разработанная соответствующим образом, может таким образом удовлетворить требованиям всех данных стандартов.

ТЕХНИЧЕСКИЙ КОДЕКС УСТАНОВИВШЕЙСЯ ПРАКТИКИ

Банковские технологии
Управление рисками в сфере информационных технологий

Банкаўскія тэхналогіі
Упраўленне рызыкамі у сферы інфармацыйных тэхналогій

Banking technologies
Risk management in the sphere of IT

Дата введения 2011-03-01

1 Область применения

Технический кодекс устанавливает требования к процессам управления рисками в сфере информационных технологий банков, относящихся к категории операционного риска.

Использование банками технического кодекса при управлении рисками носит добровольный характер, если только в отношении отдельных положений обязательность их применения не установлена законодательством Республики Беларусь, в том числе нормативными правовыми актами Национального банка Республики Беларусь.

При применении технического кодекса банками обязательна ссылка на него и (или) прямого использования устанавливаемых в нем положений в локальных нормативных правовых актах банка, а также в договорах. При этом требования технического кодекса, содержащие положения долженствования, применяются на обязательной основе, а рекомендации применяются по решению банка.

Издание официальное

2 Нормативные ссылки

В техническом кодексе использованы ссылки на следующие технические нормативные правовые акты в области технического нормирования и стандартизации (далее – ТНПА):

СТБ П ISO/IEC 27001-2008 Информационные технологии. Технологии безопасности. Системы управления защитой информации. Требования

СТБ П 34.101.41-2009 Информационные технологии и безопасность. Обеспечение информационной безопасности банков Республики Беларусь. Общие положения

СТБ П 34.101.42-2009 Информационные технологии и безопасность. Обеспечение информационной безопасности банков Республики Беларусь. Аудит информационной безопасности

ISO/IEC 13335-1:2006 Information technology - Guidelines for the management of IT Security - Part 4: Selection of safeguards (Информационные технологии. Руководство по управлению безопасностью информационных технологий IT. Часть 4. Выбор защитных мер)

ISO/IEC TR 13335-3:2007 Information technology - Guidelines for the management of IT Security - Part 3: Techniques for the management of IT security (Информационные технологии. Руководящие указания по контролю безопасности информационных технологий. Часть 3. Методы контроля IT)

ISO/IEC TR 13335-4:2000 Information technology - Security techniques - Management of information and communications technology security - Part 1: Concepts and models for information and communications technology security management (Информационные технологии. Методы защиты. Управление безопасностью информационно-коммуникационных технологий. Часть 1. Концепция и модели управления безопасностью информационно-коммуникационных технологий)

ИСО/МЭК Руководство 73-2005 Менеджмент риска. Термины и определения.

Примечание – При пользовании настоящим техническим кодексом целесообразно проверить действие ТНПА по каталогу, составленному по состоянию на 1 января текущего года, и по соответствующим информационным указателям, опубликованным в текущем году.

Если ссылочные ТНПА заменены (изменены), то при пользовании настоящим техническим кодексом, следует руководствоваться замененными (измененными) ТНПА. Если ссылочные ТНПА отменены без замены, то положение, в котором дана ссылка на них, применяется в части, не затрагивающей эту ссылку.

3 Термины и определения

В техническом кодексе применяют следующие термины с соответствующими определениями:

3.1 актив банка: Все, что имеет ценность для банка и находится в его распоряжении.

Примечание – К активам банка могут относиться:

– банковские ресурсы (финансовые, людские, вычислительные, телекоммуникационные и др.);

– информационные активы, в том числе различные виды банковской информации (платежной, финансово-аналитической, служебной, управляющей и др.) на следующих фазах их жизненного цикла: генерация (создание), обработка, хранение, передача, уничтожение;

– банковские процессы (банковские платежные технологические процессы, банковские информационные технологические процессы, процессы жизненного цикла автоматизированных банковских систем и др.);

– банковские продукты и услуги, предоставляемые клиентам.

3.2 анализ риска: Систематическое использование информации для идентификации источников и оценки риска (ИСО/МЭК Руководство 73-2005).

Примечания

1 Анализ риска обеспечивает базу для оценивания риска, мероприятий по снижению риска и принятия риска.

2 Информация может включать в себя исторические данные, результаты теоретического анализа, мотивированное суждение и касаться причастных сторон

3 Процесс идентификации рисков применительно к безопасности информационной системы, определения вероятности их осуществления и потенциального воздействия, а также дополнительных контрмер, ослабляющих (уменьшающих) это воздействие

3.3 идентификация риска: Процесс нахождения, составления перечня и описания элементов риска (ИСО/МЭК Руководство 73-2005).

Примечания

1 Элементы риска могут включать в себя источники или опасности, события, последствия и вероятность.

2 Идентификация риска может также отражать интересы причастных сторон

3.4 идентификация источников риска: Процесс нахождения, составления перечня и описания источников риска (ИСО/МЭК Руководство 73-2005).

3.5 ключевой индикатор риска: Показатель, теоретически или эмпирически связанный с уровнем риска, принимаемым банком, при этом в общем случае не являясь его оценкой.

Примечание – В качестве ключевых индикаторов риска могут использоваться:

– количество допущенных ошибок при проведении операций, выявленных банком/внешними органами контроля;

– количество аварий, сбоев информационных систем;

– время (продолжительность) простоя информационных систем.

3.6 количественная оценка риска: Процесс присвоения значений вероятности и последствий риска (ИСО/МЭК Руководство 73-2005).

Примечание – Количественная оценка риска может учитывать стоимость, выгоды, интересы причастных сторон и другие переменные, рассматриваемые при оценивании риска.

3.7 критерии риска: Правила, по которым оценивают значимость риска (ИСО/МЭК Руководство 73-2005).

Примечание – Критерии риска могут включать в себя сопутствующие стоимость и выгоды, законодательные и обязательные требования, социально-экономические и экологические аспекты, озабоченность причастных сторон, приоритеты и другие затраты на оценку.

3.8 обработка риска: Процесс выбора и осуществления мер по изменению риска.

Примечания

1 Термин «обработка риска» иногда используют для обозначения самих мер.

2 Меры по обработке риска могут включать в себя предотвращение, уменьшение (снижение), перенос, принятие, или отказ от риска.

3.9 остаточный риск: Риск, сохраняющийся после обработки риска (ИСО/МЭК Руководство 73-2005).

3.10 перенос риска: Разделение с другой стороной бремени потерь или выгод от риска.

Примечания

1 Законодательные или обязательные требования могут ограничивать, запрещать или поручать перенос определенного риска.

2 Перенос риска может быть осуществлен страхованием или другими соглашениями.

3 Перенос риска может создавать новый риск или модифицировать существующий риск.

4 Перенос риска осуществляется с учетом стоимости и законодательных требований.

3.11 политика управления рисками в сфере информационных технологий банка; политика: Совокупность правил, определяющих и ограничивающих деятельность участников системы управления рисками в сфере информационных технологий банка.

3.12 предотвращение риска: Решение не быть вовлеченным в рискованную ситуацию или действие, предупреждающее вовлечение в нее (ИСО/МЭК Руководство 73-2005).

3.13 принятие риска: Решение принять риск (ИСО/МЭК Руководство 73-2005).

Примечание – Принятие риска зависит от критериев риска

3.14 риск в сфере банковских информационных технологий; ИТ-риск: Комбинация вероятности наступления события и уровня его негативного воздействия на прибыль банка вследствие использования в банке соответствующих информационных технологий.

3.15 снижение риска: Действия, предпринятые для уменьшения вероятности, негативных последствий или того и другого вместе, связанных с риском (ИСО/МЭК Руководство 73-2005).

4 Общие требования к системе управления рисками в сфере информационных технологий

4.1 Общие требования

4.1.1 СУРИТ представляет собой совокупность организационной структуры, стратегии, методик и процедур, являющихся средствами управления ИТ-рисками.

4.1.2 СУРИТ должна отвечать следующим требованиям:

– определять общие принципы для деятельности банка в отношении СУРИТ;

– учитывать требования нормативных правовых актов, внутренних норм и правил банка по обеспечению СУРИТ;

– отвечать требованиям стратегического управления рисками банка;

– устанавливать критерии, по которым оцениваются ИТ-риски;

– согласовываться и утверждаться органами управления банка.

4.1.3 СУРИТ учреждается, реализуется, управляется, контролируется, пересматривается, поддерживается и совершенствуется в контексте деятельности банка и рисков, с которыми он сталкивается.

Для постоянного улучшения результативности и эффективности СУРИТ необходимо:

– определить процессы, необходимые для СУРИТ;

– определить последовательность и взаимодействие процессов СУРИТ;

– определить критерии и методы, необходимые для обеспечения результативности, как при осуществлении, так и при управлении процессами СУРИТ;

– обеспечить наличие ресурсов и информации, необходимых для поддержки процессов СУРИТ и их мониторинга;

– осуществлять мониторинг и анализ процессов СУРИТ;

– принимать меры, необходимые для достижения запланированных результатов и постоянного улучшения процессов СУРИТ.

4.2 Процесс создания системы управления рисками в сфере информационных технологий

4.2.1 В рамках процесса создания СУРИТ определяется:

4.2.1.1 Область действия в рамках деятельности банка, организационной структуры банка и активов банка.

4.2.1.2 Порядок применения СУРИТ в рамках деятельности банка, организационной структуры банка и активов банка.

4.2.1.3 Порядок определения области рассмотрения, идентификации и оценки активов банка, включающий разработку процедур:

– идентификации активов банка и владельцев данных активов;

– идентификации ИТ-рисков для активов банка;

– идентификации источников ИТ-рисков;

– идентификации негативных воздействий на активы банка.

4.2.1.4 Подход к анализу ИТ-рисков, включающий:

– определение методики оценки ИТ-рисков;

– разработку критериев для принятия ИТ-рисков и установления приемлемых уровней ИТ-рисков.

4.2.1.5 Порядок анализа и оценки ИТ-рисков, включающий разработку процедур:

– оценки негативных воздействий на банк, которые могут быть результатом реализации ИТ-рисков;

– оценки вероятности реализации ИТ-рисков;

– определения уровней ИТ-рисков;

– определения необходимости обработки ИТ-рисков с использованием критериев принятия ИТ-рисков.

4.2.1.6 Порядок обработки ИТ-рисков, включающий процедуры:

– применения соответствующих средств управления;

– принятия ИТ-рисков при условии, что они четко соответствуют стратегии деятельности банка и критериям принятия ИТ-рисков, установленным банком;

– отказа от ИТ-рисков;

– передачи ИТ-рисков иным сторонам;

– выбора целей и средств контроля для обработки ИТ-рисков.

При данном выборе принимают во внимание критерии необходимости обработки ИТ-риска, а также требования нормативных правовых актов, организационной структуры банка, договорных отношений со сторонними организациями, целей и бизнес-процессов банка, влияющих на возникновение, повышение уровня или реализацию ИТ-рисков.

Примечание – Выбор целей и средств контроля для обработки ИТ-рисков должен осуществляться с использованием СТБ П ISO/IEC 27001-2008 Информационные технологии. Технологии безопасности. Системы управления защитой информации. Требования. Цели и средства контроля, перечисленные в СТБ П ISO/IEC 27001-2008 ,выбираются как часть данного процесса в качестве подходящих для удовлетворения установленных требований. Цели и средства контроля, перечисленные в СТБ П ISO/IEC 27001-2008, не являются исчерпывающими. Могут выбираться дополнительные цели и средства контроля.

4.2.1.7 Порядок мониторинга ИТ-рисков, включающий процедуры:

– мониторинга и пересмотра средств контроля;

– регулярного пересмотра эффективности СУРИТ;

– анализа пересмотра оценки ИТ-рисков в запланированные интервалы времени, а также остаточные ИТ-риски и установленные приемлемые уровни ИТ-риска;

– проверки СУРИТ.

4.3 Процесс реализации системы управления рисками в сфере информационных технологий

4.3.1 В рамках процесса реализации СУРИТ осуществляется:

– выполнение процесса управления ИТ-рисками;

– выполнение запланированных процедур обработки ИТ-рисков с целью достижения установленных целей контроля ИТ-рисков, включающих анализ стоимости контрмер направленных на уменьшение уровней ИТ-рисков, распределение ролей и ответственности в процессах управления ИТ-рисками;

– использование средств контроля.

4.4 Процесс контроля и анализа управления рисками в сфере информационных технологий

4.4.1 В процессе контроля и анализа в рамках СУРИТ выполняются следующие процедуры:

– регистрации всех действий и событий, оказывающих негативное влияние на работу СУРИТ;

– анализа средств контроля ИТ-рисков, процедур и результатов обработки ИТ-рисков в целях обнаружения ошибок;

– оценки мер и действий, предпринимаемых для недопущения реализации ИТ-рисков и снижения их уровней;

– анализа изменений в нормативных правовых актах, организационной структуре банка, договорных отношениях со сторонними организациями, целях и бизнес-процессах банка влияющих на возникновение, повышение уровня или реализацию ИТ-рисков;

– анализа результатов функционирования СУРИТ на соответствие целям СУРИТ;

– оценки необходимости внесения изменений в СУРИТ.

4.4.2 Процедуры процесса контроля и анализа должны выполняться регулярно через запланированные банком интервалы времени и при необходимости внепланово.

4.4.3 Внеплановое выполнение процедур процесса контроля и анализа рекомендуется выполнять в следующих случаях:

– реализации ИТ-рисков;

– изменений в СУРИТ;

– изменений в нормативных правовых актах, организационной структуре банка, договорных отношениях со сторонними организациями, целях и бизнес-процессах банка влияющих на возникновение, повышение уровня или реализацию ИТ-рисков.

4.4.4 Полученные данные в результате выполнения процедур контроля и анализа сохраняются и используются для оценки СУРИТ.

4.4.5 Процедуры процесса контроля и анализа и планы их выполнения должны документироваться и регулярно пересматриваться в целях улучшения.

4.4.6 В целях определения соответствия СУРИТ требованиям относящихся к ней нормативных правовых актов, внутренних норм и правил банка, а также оценки реализации процесса контроля и анализа необходимо проводить внутренний аудит СУРИТ. Внутренние аудиты СУРИТ проводят через запланированные интервалы с составлением отчета по результатам аудита. Процесс проведения внутреннего аудита СУРИТ должен документироваться.

4.5 Процесс поддержки эффективности и совершенствования системы управления рисками в сфере информационных технологий

4.5.1 В рамках процесса поддержки эффективности и совершенствования СУРИТ осуществляется:

4.5.1.1 Внесение изменений в СУРИТ для устранения несоответствия СУРИТ нормативным правовым актам, организационной структуре банка, целям и бизнес-процессам банка, влияющим на возникновение, повышение уровня или реализацию ИТ-рисков.

Действия по внесению изменений в СУРИТ:

– выявление несоответствий;

– определение причин несоответствий;

– реализация необходимых корректирующих мер;

– проверка принятых корректирующих мер.

4.5.1.2 Регулярное определение предупредительных мер для устранения причин возможных несоответствий СУРИТ требованиям нормативных правовых актов, организационной структуры банка, договорных отношений со сторонними организациями, целей и бизнес-процессов банка, влияющих на возникновение, повышение уровня или реализацию ИТ-рисков. Принятые предупредительные меры должны соответствовать степени значимости возможных ИТ-рисков.

Действия по совершенствованию СУРИТ:

– выявление недостатков в СУРИТ и возможных несоответствий;

– определение необходимых улучшений в СУРИТ;

– реализация улучшений в СУРИТ;

– оценка результатов совершенствования СУРИТ.

4.5.1.3 Информирование всех заинтересованных сторон об изменениях в СУРИТ.

4.5.2 Процедуры поддержки в рабочем состоянии и совершенствования СУРИТ и результаты их выполнения документируются и регулярно пересматриваются в целях улучшения.

5 Осуществление процесса управления рисками в сфере информационных технологий

5.1 Общие требования

Процесс управления ИТ-рисками должен включать следующие процедуры:

– определение области рассмотрения, идентификация и оценка активов банка;

– анализ ИТ-рисков;

– обработка ИТ-рисков;

– мониторинг ИТ-рисков.

ИТ-риски необходимо контролировать постоянно, периодически проводя их переоценку. Качественно выполненная и тщательно документированная первая оценка ИТ-рисков банка может существенно упростить последующую деятельность по управлению ИТ-рисками банка.

5.2 Общие требования к процедуре определения области рассмотрения, идентификации и оценки активов банка

5.2.1 Определение области рассмотрения и идентификация активов банка

5.2.1.1 Для определения области рассмотрения активов банка осуществляется выбор анализируемых объектов и уровня детализации, на котором они будут рассматриваться с учетом требуемых для анализа затрат времени и человеческих ресурсов. В целях сокращения затрат может рассматриваться совокупность только наиболее важных активов банка, с учетом, что оценка будет ограниченной. При этом рекомендуется создать модель (описание) информационной инфраструктуры банка, позволяющую определить, какие объекты информационной инфраструктуры банка выбраны для анализа ИТ-рисков, а какие остались за его рамками. Модель информационной инфраструктуры банка следует поддерживать в актуальном состоянии, чтобы при изменении информационной инфраструктуры банка или более глубоком анализе ИТ-рисков можно было оценить, какие объекты нуждаются в рассмотрении.

5.2.1.2 Анализ информационной инфраструктуры банка предназначен для формирования и документирования активов банка, подверженных ИТ-риску (приложение А). При составлении перечня активов банка рекомендуется анализировать следующие уровни информационной инфраструктуры банка:

– аппаратные средства, включающие оборудование (собственное и предоставленное поставщиками услуг), локальную вычислительную сеть (проводные и беспроводные участки), носители электронной информации;

– программное обеспечение (приобретенное, используемое по лицензии и разработанное банком);

– данные и информацию в электронной форме.

5.2.1.3 При проведении анализа информационной инфраструктуры банка рекомендуется выделять программные интерфейсы (приложения), которые обеспечивают взаимодействие внешних пользователей и персонала с информационной системой банка, в отдельную группу объектов информационной инфраструктуры банка в связи с их высокой значимостью и подверженностью угрозам.

5.2.1.4 Активы банка, включенные в определенную область рассмотрения, должны быть выявлены, и наоборот, любые активы банка, выведенные за область рассмотрения (независимо от причин), должны быть рассмотрены еще раз с тем, чтобы убедиться, что они не были пропущены.

5.2.2 Оценка активов банка

5.2.2.1 Ценность активов банка определяется исходя из их важности для достижения целей банка и осуществления его деятельности, а также их стоимости.

Оценка активов банка проводится по определенной в банке шкале и методике оценки активов банка.

Пример – Примером шкалы оценок может быть определение уровня ценности как "низкий", "средний" или "высокий" или, с большей степенью детализации, "пренебрежимо малый", "низкий", "средний", "высокий", "очень высокий".

5.2.2.2 Методика оценки активов банка должна обеспечивать получение количественных и качественных оценок, там, где получение количественных оценок невозможно. Используемая шкала оценок активов банка должна быть снабжена соответствующими пояснениями.

5.2.2.3 В ходе оценки активов банка рекомендуется выявлять зависимости одних активов банка от других, оказывающие влияние на оценку активов банка.

Данные о зависимостях, существующих между отдельными активами банка, должны способствовать идентификации некоторых видов ИТ-рисков

5.3 Общие требования к процедуре анализа рисков в сфере банковских информационных технологий

5.3.1 Общие требования к анализу источников рисков в сфере банковских информационных технологий, идентификации и оценке эффективности существующих мер по снижению рисков в сфере банковских информационных технологий

В ходе выполнения настоящей процедуры должны быть решены следующие задачи:

– выявлены и описаны все значимые угрозы активам банка и их источники – факторы ИТ-рисков, включая инциденты, приводящие к реализации ИТ-рисков (Приложение В – Таблица 1);

– определены уязвимости информационной инфраструктуры банка, увеличивающие вероятность реализации ИТ-рисков;

– определены существующие меры по снижению ИТ-рисков и проведена оценка их эффективности;

– составлен классификатор ИТ-рисков. Классификация ИТ-рисков должна быть единой, полной и непротиворечивой.

5.3.2 Общие требования к процедуре оценки рисков в сфере банковских информационных технологий

5.3.2.1 Оценка ИТ-рисков проводиться с учетом направленности деятельности банка, его организационной структуры и информационной инфраструктуры.

Примечание – Учитывая, что ИТ-риски банка являются категорией операционных рисков, рекомендуется рассматривать ИТ-риски с привязкой к бизнес-процессам банка, чтобы иметь возможность получения консолидированной оценки операционного риска каждого бизнес-процесса.

5.3.2.2 Величина ИТ-риска определяется ценностью подвергающихся риску активов банка, вероятностью реализации угроз, способных оказать негативное воздействие на деятельность банка, а также наличием действующих или планируемых мер, использование которых могло бы снизить уровень ИТ-риска.

5.3.2.3 Процедура оценки ИТ-рисков должна быть документирована и поддерживаться в актуальном состоянии.

5.3.2.4 Результатом оценки ИТ-рисков должно быть количественное и/или качественное измерение величины ИТ-рисков.

5.3.2.5 Для оценки ИТ-рисков рекомендуется использовать данные о частоте и последствиях инцидентов, приводящих к реализации ИТ-рисков.

5.3.2.6 Для оценки частоты инцидентов применяются следующие подходы:

– использование имеющихся статистических данных;

– получение частот происходящих инцидентов, приводящих к реализации ИТ-рисков, на основе аналитических или имитационных методов;

– использование мнений экспертов.

5.3.2.7 Данные, используемые для оценки частоты инцидентов, должны соответствовать типу системы, оборудования или деятельности подлежащих рассмотрению.

5.3.2.8 Анализ последствий используется для оценки вероятного воздействия на активы банка, которое вызывается инцидентом.

5.3.2.9 Анализ последствий должен:

– основываться на выбранных инцидентах;

– описывать любые последствия, являющиеся результатом инцидентов;

– учитывать существующие меры, направленные на смягчение последствий, наряду со всеми соответствующими условиями, оказывающими влияние на последствия;

– устанавливать критерии, используемые для полной идентификации последствий;

– рассматривать и учитывать как немедленные последствия, так и те, которые могут проявиться по прошествии определенного периода времени, если это не противоречит области рассмотрения активов банка;

– рассматривать и учитывать вторичные последствия, распространяющиеся на смежное оборудование и системы.

5.3.2.10 По результатам оценки ИТ-рисков в банке должен быть составлен перечень оцененных ИТ-рисков.

5.3.2.11 Используемый банком метод оценки ИТ-рисков должен быть повторяемым и прослеживаемым.

5.4 Общие требования к процедуре обработки рисков в сфере банковских информационных технологий

5.4.1 После оценки ИТ-рисков, должно быть принято решение относительно их обработки, выбора и реализации мер и средств по минимизации ИТ-риска:

– уменьшение ИТ-риска. ИТ-риск считается неприемлемым, и для его уменьшения выбираются и реализуются соответствующие меры и средства уменьшения ИТ-риска;

– передача ИТ-риска. ИТ-риск считается неприемлемым и на определённых условиях передается сторонней организации;

– принятие ИТ-риска. ИТ-риск считается осознанно допустимым, банк принимает возможные последствия в связи с тем, что стоимость контрмер значительно превосходит финансовые потери в случае реализации ИТ-риска либо банк не может найти подходящие меры и средства уменьшения ИТ-риска;

– приемлемость ИТ-риска. После выбора мер по снижению уровня ИТ-риска в результате применения контрмер всегда будут иметь место остаточные ИТ-риски. Данные остаточные риски должны оцениваться банком как приемлемые или неприемлемые. Такая оценка должна быть осуществлена путем рассмотрения потенциальных неблагоприятных воздействий на деятельность банка, которые могут быть вызваны остаточными ИТ-рисками. Должно быть принято решение о допустимости ИТ-рисков в связи с имеющимися ограничениями, либо необходимо предусмотреть дополнительные меры для снижения уровня неприемлемых ИТ-рисков;

– отказ от ИТ-риска. Отказ от процессов, являющихся источниками ИТ-риска.

5.4.2 Должен быть составлен план управления ИТ-рисками включающий в себя экономически оправданные механизмы управления и контрмеры, направленные на уменьшение ИТ-рисков.

5.4.3 ИТ-риски должны быть ранжированы и для каждого ИТ-риска должна быть определена соответствующая контрмера.

5.5 Мониторинг

5.5.1 В процессе мониторинга осуществляется непрерывный мониторинг ИТ-рисков, с целью быстрого выявления и исправления недостатков в процессах и процедурах по управлению ИТ-рисками.

5.5.2 Осуществляется накопление и анализ данных об ИТ-рисках в рамках общей системы управления операционными рисками банка, включая:

– сбор информации о технических и технологических сбоях, инцидентах в информационной системе банка;

– идентификацию ключевых индикаторов ИТ-риска;

– систематизацию и анализ накопленных данных.

5.5.3 В процессе мониторинга отслеживаются ключевые индикаторы ИТ-риска и пороговые значения установленных критериев, позволяющие предсказать возможные потери от реализовавшихся ИТ-рисков. Ключевые индикаторы ИТ-риска должны быть ориентированы на выявление потенциальных источников ИТ-рисков.

5.5.4 Процедуры мониторинга ИТ-рисков должны принимать во внимание:

– виды и сущность нарушений функционирования информационной системы;

– вид, степень сложности осуществляемых и планируемых банком банковских операций;

– состояние телекоммуникационных систем и информационных технологий в банке;

– уровень квалификации работников банка, а также кадровые и организационные изменения в его структуре.

5.5.5 Результаты мониторинга ИТ-рисков должны регулярно предоставляться заинтересованным лицам банка.

6 Требования к документации системы управления рисками в сфере информационных технологий

6.1 Документация СУРИТ должна включать:

– политику применения и цели СУРИТ;

– описание области действия СУРИТ;

– описание процессов, процедур и средств контроля СУРИТ;

– план обработки ИТ-рисков.

6.2 Должен осуществляться контроль документации СУРИТ включающий:

– согласование и утверждение документов СУРИТ;

– поддержание в актуальном состоянии документации СУРИТ (регулярный пересмотр и обновление документов СУРИТ);

– доведение документации СУРИТ до всех заинтересованных сторон банка;

– определение порядка хранения, использования и уничтожения документации СУРИТ.

6.3 Заинтересованные лица банка должны регулярно получать отчеты как от подразделений, осуществляющих операции, так и от подразделения, осуществляющего функции внутреннего контроля за эффективностью СУРИТ.

6.4 Отчеты СУРИТ должны содержать:

– оценку соответствия деятельности банка нормативным правовым актам и политике банка в области ИТ-рисков;

– информацию о внешних и внутренних факторах и условиях, которые могут оказывать влияние на ИТ-риски банка и принятие решений в сфере управления ими;

– данные о выявленных проблемных сферах и сферах потенциального возникновения проблем в управлении ИТ-рисками и предложения по их предотвращению (устранению).

Приложение А

(рекомендуемое)
Типовой перечень активов банка

a) Несетевые серверы:
   1) несетевые серверы общего назначения;
   2) прочие несетевые серверы.
b) Сетевые серверы:
   1) сетевые файл-серверы;
   2) сетевые серверы БД;
   3) сетевые серверы общего назначения;
   4) прочие сетевые серверы.
c) Несетевые рабочие станции:
   1) портативные, не имеющие постоянного расположения;
   2) стационарные рабочие станции с большим диапазоном возможностей (класса ПК);
   3) стационарные рабочие станции с ограниченными возможностями (класса X-терминала);
   4) прочие стационарные рабочие станции.
d) Сетевые рабочие станции:
   1) портативные, не имеющие постоянного расположения;
   2) стационарные рабочие станции с большим диапазоном возможностей (класса ПК);
   3) стационарные рабочие станции с ограниченными возможностями (класса X-терминала);
   4) прочие стационарные рабочие станции.
e) Локальные запоминающие устройства:
   1) накопители на жестких дисках;
   2) накопители на магнитной ленте;
   3) накопители на оптических дисках;
   4) прочие запоминающие устройства.
f) Сетевые запоминающие устройства:
   1) накопители на жестких дисках;
   2) накопители на магнитной ленте;
   3) накопители на оптических дисках:
   4) прочие сетевые запоминающие устройства.
g) Локальные печатающие устройства:
   1) принтер.
h) Сетевые печатающие устройства печати:
   1) сервер печати;
   2) сетевой принтер;
   3) принтер;
   4) другие сетевые устройства печати.
i) Сетевые распределительные компоненты:
   1) мост;
   2) коммутатор;
   3) маршрутизатор;
   4) повторитель;
   5) модем;
   6) мультиплексор;
   7) узел коммутации ATM;
   8) узел коммутации X.25;
   9) оконечный сетевой элемент;
   10) спутниковая станция связи;
   11) станция радиосвязи;
   12) прочие сетевые распределительные компоненты.
j) Сетевые шлюзы:
   1) шлюз трансляции сообщений;
   2) шлюз трансляции адресов;
   3) шлюз безопасности;
   4) управляющий шлюз;
   5) шлюз преобразования протоколов;

6) прочие шлюзы.

k) Управление сетью и управляющие серверы:
   1) системы, обеспечивающие протоколирование сообщений и управление сообщениями;
   2) сетевые серверы аутентификации;
   3) сетевой центр управления;
   4) другие средства сетевого управления и управляющие серверы.

l) Сетевые интерфейсы:
   1) постоянное соединение:
   2) синхронное;
   3) асинхронное.
   4) коммутируемое соединение:
   5) PSTN;
   6) ISDN;
   7) радиосоединение;
   8) прочие типы соединений.

m) Сетевые сервисы:
   1) объединение локальных сетей;
   2) канал с невысокой пропускной способностью;
   3) канал с пропускной способностью, соответствующий предъявляемым требованиям;
   4) маршрутизация сообщений;
   5) сетевое хранилище;

n) Сервисы общего назначения:
   1) Internet;
   2) другие сети общего назначения;
   3) телефония;
   4) прочие сетевые сервисы.

o) Сервисы конечного пользователя:
   1) электронная почта;
   2) прикладной обмен сообщениями;
   3) обмен электронными документами;
   4) передача файлов;
   5) сеансовая обработка;
   6) пакетная обработка;
   7) голос;
   8) видео;
   9) прочие сервисы конечного пользователя.

p) Коммуникационные протоколы:
   1) X.25;
   2) SDLS/HDLS;
   3) IP;
   4) CLNP (Connectionless Network Protocol);
   5) ATM;
   6) Frame Relay;
   7) TDM;
   8) протоколы спутникового обмена информацией;
   9) Ethernet;
   10) Token Ring;
   11) прочие протоколы.

q) Носители данных (Media):
   1) неэлектронные носители:
   2) устройства ввода;
   3) устройства вывода;
   4) важные записи;
   5) прочие виды носителей;
   6) электронные носители:
   7) магнитные ленты;
   8) диски;
   9) прочие виды носителей.

r) Прикладные и общесистемные программные средства.

s) Программно-технические компоненты автоматизированных систем.

t) Помещения, здания, сооружения ИТ.

u) Информационные активы, в том числе различные виды банковской информации (платежной, финансово-аналитической, служебной, управляющей и др.) на следующих фазах их жизненного цикла: генерация (создание), обработка, хранение, передача, уничтожение.

v) Банковские процессы (банковские платежные технологические процессы, банковские информационные технологические процессы, процессы жизненного цикла автоматизированных банковских систем и др.);

w) Банковские продукты и услуги, предоставляемые клиентам.

Приложение В
(рекомендуемое)

Рекомендуемый перечень и описание типовых источников (причин) рисков в сфере информационных технологий

Таблица 1

Источник (причины) ИТ-риска	Описание
Пожар	Неконтролируемый процесс горения, сопровождающийся уничтожением материальных ценностей и создающий опасность для жизни людей. Возможные причины: поджог, самовозгорание, природное явление.
Природные катастрофы, чрезвычайные ситуации и стихийные бедствия	Природные явления разрушительного характера (наводнения, землетрясения, извержения вулканов, ураганы, смерчи, тайфуны, цунами, и т.д.)
Техногенные катастрофы	Разрушительный процесс, развивающийся в результате нарушения нормального взаимодействия технологических объектов с компонентами окружающей природной среды, приводящий к гибели людей, разрушению и повреждению объектов экономики и компонентов окружающей природной среды.
Нарушение внутриклиматических условий	Негативное изменение климатических условий в помещениях, где расположены технические средства и/или находится персонал: значительные изменения температуры и влажности, повышение содержания углекислого газа, пыли и т. п. Возможные последствия: сбои, отказы и аварии технических средств, снижение работоспособности и нанесение ущерба здоровью персонала, нарушение непрерывности выполнения процессов, снижение качества информационных услуг (сервисов).
Нарушение электропитания	Нарушение или снижение качества электропитания. Возможные причины: техногенная катастрофа, стихийное бедствие, природное явление, террористический акт, пожар и т.п. Возможные последствия: сбои и отказы технических средств.
Нарушение функционирования систем жизнеобеспечения	Сбои и аварии в системах водоснабжения, канализации, отопления
Нарушения общественного порядка, общественная нестабильность	Нарушения общественного порядка (например, во время уличных фестивалей, концертов, спортивных мероприятий, производственных собраний, демонстраций и т. д.), гражданские беспорядки, социальные волнения, политическая нестабильность
Террористические действия	Злоумышленные действия в отношении активов банка, классифицируемые согласно законодательству Республики Беларусь как террористические акты, в том числе, захват или попытка захвата заложников на территории банка, обнаружение взрывных устройств, получение сообщения об угрозе взрыва объектов банка.
Шпионаж	Выведывание, собирание или похищение сведений, составляющей государственную или банковскую тайну
Саботаж	Сознательное неисполнение работниками определенных обязанностей или небрежное их исполнение
Халатность	Невыполнение или ненадлежащее выполнение персоналом своих обязанностей без злого умысла
Вредительство	Злоумышленное нанесение персоналом вреда активам банка. В первую очередь вредительство может быть направлено на технические и программные средства, а также на информационные активы. Возможные последствия: ущерб, вызванный нарушением свойств активов банка, включая их разрушение и уничтожение.

Источник (причины) ИТ-риска	Описание
Ошибка персонала	Любые несоответствующие установленному регламенту или сложившимся практикам действия персонала, совершаемые без злого умысла. Возможные причины: недостаточно чётко определенные обязанности, халатность, недостаточное обучение или квалификация персонала. Возникновению ошибок способствуют отсутствие дисциплинарного процесса и документирования процессов, предоставление избыточных полномочий, использование злоумышленником методов социального инжиниринга к персоналу. Возможные последствия: нарушение конфиденциальности целостности, утрата активов банка, нарушение непрерывности выполнения процессов, снижение качества информационных услуг (сервисов), сбои и отказы технических и программных средств.
Хищение	Совершенное с корыстной целью противоправное безвозмездное изъятие и/или обращение имущества банка в пользу злоумышленника или других лиц, причинившие ущерб собственнику или иному владельцу этого имущества. Возможные последствия: нарушение свойств активов банка, их утрата, нарушение непрерывности выполнения процессов, снижение качества информационных услуг (сервисов), прямой (непосредственный) ущерб деятельности банка.
Выполнение вредоносных программ	Внедрение в систему и выполнение вредоносных программ: программных закладок, «троянских коней», программных «вирусов» и «червей». Возможные причины: беспечность, халатность, низкая квалификация персонала (пользователей), наличие уязвимостей используемых программных средств. Возможные последствия: несанкционированный доступ к активам банка, нарушение их свойств, сбои, отказы и аварии программных средств, нарушение непрерывности выполнения процессов, снижение качества информационных услуг (сервисов).
Действия злонамеренного неавторизованного субъекта	Злоумышленные действия со стороны субъекта из внешней по отношению к области обеспечения среды информационной безопасности. Возможные последствия: разрушение и уничтожение технических и программных средств, внедрение и выполнение вредоносных программ, нарушение свойств, утрата активов банка.
Использование активов банка не по назначению	Умышленное использование активов банка в целях, отличных от целей банка. Возможные причины: отсутствие контроля персонала. Возможные последствия: нехватка вычислительных, сетевых или людских ресурсов, прямой ущерб банку.
Ложное сообщение об угрозе	Ложное сообщение об угрозе, такой как: пожар, террористический акт, техногенная катастрофа, гражданские беспорядки и т.д. Возможные последствия: нарушение свойств активов банка, их утрата, нарушение непрерывности выполнения процессов, снижение качества информационных услуг (сервисов).
Неконтролируемое уничтожение актива банка	Неумышленное уничтожение активов банка. Возможные причины: сбои оборудования, природные факторы и техногенные катастрофы. Возможные последствия: прямой ущерб банку.
Неконтролируемая модификация актива банка	Неумышленное изменение активов банка. Возможные причины: сбои оборудования, природные факторы и техногенные катастрофы. Возможные последствия: нарушение непрерывности выполнения процессов, прямой ущерб банку.

Источник (причины) ИТ-риска	Описание
Несанкционированный логический доступ	Несанкционированный логический доступ неавторизованных субъектов к активам банка. Возможные причины: компрометация пароля, предоставление пользователям/администраторам избыточных прав доступа, недостатки (отсутствие) механизмов аутентификации пользователей и администраторов, ошибки администрирования, оставление без присмотра программно-технических средств. Одним из путей получения несанкционированного доступа к системе является внедрение злоумышленником вредоносных программ с целью хищения пароля для входа систему или получения прав доступа. Возможные последствия: нарушение свойств активов банка, сбои, отказы и аварии программных и технических средств, нарушение непрерывности процессов и/или снижение качества информационных услуг (сервисов).
Несанкционированный физический доступ	Физический несанкционированный доступ неавторизованных лиц в контролируемую зону расположения технических средств и/или активов банка. Возможные причины: может осуществляться путем обхода средств контроля физического доступа или использования утраченных/похищенных средств обеспечения доступа. Возможные последствия: разрушение и уничтожение технических и программных средств, нарушение конфиденциальности, целостности, доступности активов банка, нарушение непрерывности процессов и/или снижение качества информационных услуг (сервисов).
Превышение допустимой нагрузки	Неумышленное превышение допустимой нагрузки на вычислительные, сетевые ресурсы системы. Выполнение работниками объема операций большего, чем это допускается психофизиологическими нормами. Возможные причины: малая вычислительная и/или пропускная мощность, неправильная организация бизнес-процессов. Возможные последствия: сбои и отказы технических средств, нарушение доступности технических средств, ошибки персонала, нанесение вреда здоровью.
Разрушение/повреждение, аварии технических средств и каналов связи	Физическое разрушение/повреждение технических средства (канала связи) или определенное сочетание отказов его элементов, приводящее к нарушениям функционирования, сопряженным с особо значительными техническими потерями, делающие невозможным функционирование технического средства (канала связи) в целом в течение значительного периода времени. Возможные причины: действие внешних (физический несанкционированный доступ, вредительство, террористический акт, техногенная катастрофа, стихийное бедствие, природное явление, гражданские беспорядки)и/или внутренних (значительные отказы элементов технических средств) факторов. Возможные последствия: нарушение свойств активов банка, их утрата, нарушение непрерывности выполнения процессов, снижение качества информационных услуг (сервисов).
Сбои и отказы программных средств	Нарушение работоспособности программных средств. Возможные причины: недопустимое изменение параметров или свойств программных средств под влиянием внутренних процессов (ошибок) и/или внешних воздействий со стороны вредоносных программ, оператора и технических средств. Возможные последствия: нарушение свойств активов банка, нарушение непрерывности выполнения процессов, снижение качества информационных услуг (сервисов).

Источник (причины) ИТ-риска	Описание
Сбои и отказы технических средств и каналов связи	Прерывание работоспособности технических средств или невозможность выполнения ими своих функций в заранее установленных границах. Возможные причины: недопустимое изменение характеристик технических средств под влиянием внутренних процессов, сложность технических средств, нехватка персонала, недостаточное техническое обслуживание. Возможные последствия: сбои, отказы программных средств, аварии систем, нарушение доступности активов банка, нарушение непрерывности выполнения процессов, снижение качества информационных услуг (сервисов).
Запугивание и шантаж	Умышленное психологическое воздействие на персонал, заключающееся в угрозе разоблачения, физической расправы или расправы с близкими. Возможные последствия: несанкционированные злоумышленные действия персонала.
Социальный инжиниринг	Умышленные действия сторонних лиц, преследующие мошеннические цели, реализуемые посредством обмана, введения в заблуждение работников банка. Возможные последствия: ошибки работников, нарушение свойств, утрата активов банка, нарушение непрерывности процессов, снижение качества информационных услуг (сервисов).
Несоответствие внутренних документов действующему законодательству	Несоответствие деятельности может привести к административным и уголовным санкциям со стороны судебных, надзорных и регулирующих органов в отношении должностных лиц банка, вызвать остановку отдельных видов деятельности банка.
Изменчивость и несогласованность требований надзорных и регулирующих органов, вышестоящих инстанций	Непостоянство, различия и коллизии в содержании требований и/или порядке их выполнения способны дезорганизовать деятельность подразделения или его отдельных служб, снизить ее эффективность и качество, а при определенных обстоятельствах, затруднить ее осуществление. Способствует «размыванию» или пересечению зон ответственности исполнителей и служб, манипуляции со стороны ответственных лиц и служб своими правами и обязанностями в ущерб общей деятельности. Приводит к перераспределению ресурсов в пользу той деятельности (зачастую не основной), за несоблюдение требований к которой наказание наиболее ощутимое для банка.
Угроза здоровью персонала	Угроза здоровью персонала в результате радиационных, биологических, механических, термических, химических и иных воздействий со стороны окружающей среды, объектов инженерной инфраструктуры, технических средств, пищевые отравления, производственный травматизм. Возможные причины: техногенные или природные катастрофы, аварии объектов инженерной инфраструктуры неисправность оборудования, несоблюдение правил техники безопасности и охраны труда, санитарных правил и т.д. Возможные последствия: нехватка персонала, денежные выплаты, судебные разбирательства.
Зависимость от партнеров/клиентов	Зависимость от партнёров заставляет банк полагаться на их информационную безопасность, банк должен быть уверена, что партнёр сможет обеспечить должный уровень безопасности.
Ошибки, допущенные при заключении контрактов с провайдерами внешних услуг	Неточности и неопределённости в договоре с провайдером внешних услуг, которые могут создавать проблемы в работе заказчика.
Нарушения договорных обязательств сторонними (третьими) лицами	Невыполнение со стороны третьих лиц взятых на себя обязательств перед подразделением по качеству, составу, содержанию и/или порядку оказания услуг, поставки продукции и т.д. Например, невыполнение требований банка разработчиками или поставщиками программно-технических средств и услуг, или внешними пользователями.

Источник (причины) ИТ-риска	Описание
Нарушения персоналом организационных мер по обеспечению информационной безопасности	Несоблюдение персоналом положений политик и регламентов по информационной безопасности.
Ошибки кадровой работы	Ошибки кадровой работы заключаются в приёме на работу неблагонадёжных и/или неквалифицированных сотрудников, увольнении сотрудников без проведения сопутствующих процедур по обеспечению информационной безопасности, непроведении или нерегулярном проведении обучения и проверок персонала
Ошибки в обеспечении безопасности информационных систем на стадиях жизненного цикла	Ошибки в обеспечении безопасности при разработке, эксплуатации, сопровождении и выводе из эксплуатации информационных систем
Разработка и использование некачественной документации	Некачественное выполнение документированного описания технологических процессов обработки, хранения, передачи данных, руководств для персонала, участвующего в этих технологических процессах, а также описания средств обеспечения информационной безопасности и руководств по их использованию
Использование программных средств и информации без гарантии источника	Использование в информационной системе банка непроверенных данных или нелицензионного программного обеспечения, которые поступили из внешних источников
Нарушения функциональности криптографической системы	Случайное или намеренное неправильное управление криптографическими ключами, криптографическими протоколами и алгоритмами, программно-аппаратными средствами систем криптографической защиты информации, приводящее к потере конфиденциальности, целостности и информации, нарушению неотказуемости приема - передачи информации, блокировке функционирования платежных и информационных систем банка
Нарушения функциональности архивной системы	Нарушение конфиденциальности и целостности архивных данных и/или непредоставление услуг архивной системой вследствие случайных ошибок пользователей или неправильного управления архивной системой, а также вследствие физических воздействий на компоненты архивной системы