УТВЕРЖДАЮ

Председатель Правления
Национального банка
Республики Беларусь

_____ П.В.Каллаур

«26» июня 2020 г.

**ТЕХНИЧЕСКИЕ ТРЕБОВАНИЯ И ПРАВИЛА
ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ**

Информационные технологии и безопасность
ОБЕСПЕЧЕНИЕ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ БАНКОВ РЕСПУБЛИКИ БЕЛАРУСЬ
Общие положения и терминология

Інфармацыйныя тэхналогіі і бяспека
ЗАБЕСПЯЧЭННЕ ІНФАРМАЦЫЙНАЙ БЯСПЕКІ БАНКАЎ РЭСПУБЛІКІ БЕЛАРУСЬ
Агульныя палажэнні і тэрміналогія

Национальный банк Республики Беларусь

Ключевые слова: банковская деятельность, банковский технологический процесс, банковские автоматизированные системы, информационная безопасность, защита информации, политика информационной безопасности

Содержание

Введение

Развитие и укрепление банковской системы Республики Беларусь, а также обеспечение эффективного и бесперебойного функционирования платежной системы Республики Беларусь являются целями деятельности Национального банка Республики Беларусь. Важнейшим условием реализации этих целей является обеспечение необходимого и достаточного уровня информационной безопасности банков, их активов (в том числе информационных), который во многом определяется уровнем информационной безопасности банковских технологических процессов (платежных, информационных и др.), автоматизированных банковских систем, эксплуатирующихся организациями банковской системы Республики Беларусь.

Особенности банковской системы таковы, что негативные последствия сбоев в работе отдельных банков могут привести к быстрому развитию системного кризиса платежной системы Республики Беларусь, нанести ущерб интересам собственников и клиентов. В случаях наступления инцидентов информационной безопасности значительно возрастают результирующий риск и возможность нанесения ущерба банкам. Поэтому для банков угрозы информационным активам, т. е. угрозы информационной безопасности представляют существенную опасность.

Для противостояния таким угрозам и обеспечения эффективности мероприятий по ликвидации неблагоприятных последствий инцидентов информационной безопасности (их влияния на операционные, кредитные и иные риски) в банках следует обеспечить достаточный уровень информационной безопасности. Необходимо также сохранять этот уровень в течение длительного времени. По этим причинам обеспечение информационной безопасности является для банков и небанковских кредитно-финансовых организаций Республики Беларусь важным элементом их деятельности.

Деятельность, относящаяся к обеспечению информационной безопасности, должна контролироваться. В связи с этим Национальный банк Республики Беларусь является сторонником регулярной оценки уровня информационной безопасности в банках и небанковских кредитно-финансовых организациях Республики Беларусь, оценки рисков и принятия мер, необходимых для управления этими рисками.

Исходя из этого, разработаны настоящиеТехнические требования и правила по обеспечению информационной безопасности, которые являются базовыми для развивающей и обеспечивающей его группы требований и правил, в целом составляющих комплекс Технических требований и правил по обеспечению информационной безопасности банков и небанковских кредитно-финансовых организаций Республики Беларусь.

Основные цели разработки Технических требований и правил по обеспечению информационной безопасности банков и небанковских кредитно-финансовых организаций Республики Беларусь:

– развитие и укрепление банковской системы Республики Беларусь;

– повышение доверия к банкам и банковской системе Республики Беларусь в целом;

– повышение стабильности функционирования банков и на этой основе - стабильности функционирования банковской системы Республики Беларусь в целом;

– достижение адекватности мер по защите от реальных угроз информационной безопасности;

– предотвращение и (или) снижение ущерба от инцидентов информационной безопасности.

Основные задачи разработки Технических требований и правилпо обеспечению информационной безопасности банков и небанковских кредитно-финансовых организаций Республики Беларусь:

– установление единых требований по обеспечению информационной безопасности банков и небанковских кредитно-финансовых организаций Республики Беларусь;

–повышение эффективности мероприятий по обеспечению и поддержанию информационной безопасности банков и небанковских кредитно-финансовых организаций Республики Беларусь.

Настоящие Технические требования и правила разработаны с учетом международных стандартов ISO/IEC 27000, а также отдельных положений стандарта Банка России СТО БР ИББС-1.0-2014 «Обеспечение информационной безопасности организаций банковской системы Российской Федерации. Общие положения».

ТЕХНИЧЕСКИЕ ТРЕБОВАНИЯ И ПРАВИЛА ПО ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ

Информационные технологии и безопасность
ОБЕСПЕЧЕНИЕ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ БАНКОВ РЕСПУБЛИКИ БЕЛАРУСЬ.
Общие положения и терминология

Інфармацыйныя тэхналогіі і бяспека
ЗАБЕСПЯЧЭННЕ ІНФАРМАЦЫЙНАЙ БЯСПЕКІ БАНКАЎ РЭСПУБЛІКІ БЕЛАРУСЬ.
Агульныя палажэнні і тэрміналогія

Information technology and security
ENSURING THE INFORMATION SECURITY OF BANKS OF THE REPUBLIC OF BELARUS
General provisions and terminology

1 Область применения

Настоящие Технические требования и правила распространяются на банки и небанковские кредитно-финансовые организации Республики Беларусь, открытое акционерное общество «Банк развития Республики Беларусь» (далее – организации БС) и устанавливает положения, концептуальную схему, модели угроз и нарушителей информационной безопасности.

Настоящие Технические требования и правила предназначены для применения при построении, проверке и оценке систем информационной безопасности и систем менеджмента информационной безопасности организаций БС.

2 Нормативные ссылки

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

СТБ ISO 9000-2006 Системы менеджмента качества. Основные положения и словарь.

ТТП ИБ 2.1-2020 Информационные технологии и безопасность. Обеспечение информационной безопасности банков Республики Беларусь. Требования к системам менеджмента информационной безопасности.

ТТП ИБ 5.1-2020 Информационные технологии и безопасность. Обеспечение информационной безопасности банков Республики Беларусь. Оценка соответствия информационной безопасности банков Республики Беларусь требованиям ТТП ИБ 1.1-2020 и ТТП ИБ 2.1-2020.

Примечание – При пользовании настоящимиТехническими требованиями и правилами целесообразно проверить действие технических нормативных правовых актов в области технического нормирования и стандартизации (далее – 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 настоящимиТехническими требованиями и правиламиследует 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 настоящих Технических требованиях и правилах применяют следующие термины с соответствующими определениями[1].

3.1**Система:** комплекс, состоящий из процессов, технических и программных средств, устройств и персонала, обладающий возможностью удовлетворять установленным потребностям или целям (СТБ ИСО/МЭК 12207);

3.2**Банковская система:** компонент финансовой системы Республики Беларусь, включающий в себя банки и небанковские кредитно-финансовые организации Республики Беларусь, открытое акционерное

1 Термины, установленные настоящими Техническими требованиями и правилами, применяются во всех видах документации и во всех видах деятельности по обеспечению информационной безопасности в банке.

общество «Банк развития Республики Беларусь».

3.3 **Менеджмент:** скоординированная деятельность по руководству и управлению организацией (СТБ ISO 9000).

3.4 **Информация:** сведения о лицах, предметах, фактах, событиях, явлениях и процессах независимо от формы их представления [2].

3.5 **Документированная информация (документ):** зафиксированная на материальном носителе информация с реквизитами, позволяющими ее идентифицировать [2].

Примечание – Под материальным носителем подразумевается материал с определенными физическими свойствами, который может быть использован для записи и хранения информации.

3.6 **Инфраструктура:** комплекс взаимосвязанных структур, составляющих основу для решения проблемы (задачи).

3.7 **Информационная инфраструктура:** совокупность технических средств, систем и технологий создания, преобразования, передачи, использования и хранения информации. Информационная инфраструктура включает информационные центры, банки данных и знаний, системы связи и обеспечивает доступ потребителей к информационным ресурсам.

3.8 **Технология**: совокупность взаимосвязанных методов, способов, приемов предметной деятельности.

3.9 **Процесс:** совокупность взаимосвязанных или взаимодействующих видов деятельности, преобразующих входы в выходы (СТБ ISO 9000).

3.10 **Информационная технология:** совокупность процессов, методов осуществления поиска, получения, передачи, сбора, обработки, накопления, хранения, распространения и (или) предоставления информации, а также пользования информацией и защиты информации [2].

3.11 **Технологический процесс:** процесс, реализующий некоторую технологию.

3.12 **Информационная система:** совокупность банков данных, информационных технологий и комплекса (комплексов) программно-технических средств [2].

3.13 **Банковский технологический процесс:** технологический процесс, содержащий операции по изменению и (или) определению состояния банковской информации, используемой при функционировании или необходимой для реализации банковских услуг.

Примечания:

1 Операции над банковской информацией могут выполняться вручную или быть автоматизированными, например, с помощью комплексов средств автоматизации автоматизированных банковских систем.

2 Операции над банковской информацией требуют указания ролей их участников (исполнителей и лиц, принимающих решения или имеющих полномочия по изменению технологических процессов, в том числе персонала автоматизированных банковских систем).

В зависимости от вида деятельности выделяют: банковский информационный технологический процесс, банковский платежный технологический процесс и др.

3.14 **Банковский информационный технологический процесс:** часть банковского технологического процесса, реализующая действия с информацией, необходимые для выполнения организацией БС своих функций, и не являющаяся банковским платежным технологическим процессом.

3.15 **Платежная информация:** информация, на основании которой совершаются операции, связанные с перемещением денежных средств с одного счета на другой.

3.16 **Неплатежная информация:** информация, необходимая для функционирования организации БС, не являющаяся платежной информацией, которая может включать в себя, например, данные статистической отчетности и внутрихозяйственной деятельности, аналитическую, финансовую и справочную информацию.

3.17 **Банковский платежный технологический процесс:** часть банковского технологического процесса, реализующая действия с информацией, связанные с осуществлением переводов денежных средств, платежного клиринга и расчета, и действия с архивами указанной информации.

3.18 **Автоматизированная банковская система:** автоматизированная система, реализующая банковский технологический процесс или его часть.

3.19 **Комплекс средств автоматизации автоматизированной банковской системы:** совокупность всех компонентов автоматизированной банковской системы, за исключением людей.

3.20 **Авторизация:** предоставление субъекту прав к объекту.

3.21 **Идентификация:** процесс присвоения идентификатора (уникального имени); сравнение предъявляемого идентификатора с перечнем присвоенных идентификаторов.

3.22 **Аутентификация:** установление подлинности субъекта на основании проверки соответствия предъявленных им идентификатора и ключа аутентификацииПроверка принадлежности субъекту доступа предъявленного им идентификатора (подтверждение подлинности).

3.23 **Регистрация:** фиксация данных о совершенных действиях (событиях).

3.24 **Роль:** заранее определенная совокупность правил, устанавливающих допустимое взаимодействие между субъектом и объектом.

Примечания:

1К субъектам относятся лица из числа руководителей организации БС, его персонала, клиентов или инициируемые от их имени процессы по выполнению действий над объектами.

2 Объектами могут быть: аппаратное средство, программное средство, программно-аппаратное средство, информационный ресурс, услуга, процесс, система, над которыми выполняются действия.

3.25 **Актив:** все, что имеет ценность для организации БС и находится в ее распоряжении.

Примечание –к активам организации БС могут относиться:

1) работники (персонал);

2) банковские ресурсы (финансовые, вычислительные (аппаратные и программные), телекоммуникационные, люди и их квалификация, навыки и опыт и др.);

3) 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;

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

5) банковские продукты и услуги, предоставляемые клиентам.

3.26 **Информационный актив:** информация, имеющая ценность для ее владельца.

3.27 **Классификация информационных активов:** разделение существующих информационных активов организации БС по типам, выполняемое в соответствии со степенью тяжести последствий от потери их значимых свойств информационной безопасности.

3.28 **Объект среды информационного актива:** материальный объект среды использования и (или) эксплуатации информационного актива (объект хранения, передачи, обработки, уничтожения и т. д.).

3.29 **Безопасность:** состояние защищенности интересов (целей) организации в условиях угроз.

3.30 **Информационная безопасность:** состояние защищенности сбалансированных интересов личности, общества и государства от внешних и внутренних угроз в информационной сфере.

Примечания:

1) Защищенность достигается обеспечением совокупности свойств информационной безопасности - доступности, целостности, конфиденциальности информационных активов. Приоритетность свойств информационной безопасности определяется ценностью указанных активов для интересов (целей) организации БС.

2) Информационная сфера представляет собой совокупность информации, информационной инфраструктуры, субъектов, осуществляющих сбор, формирование, распространение, хранение и использование информации, а также системы регулирования отношений, возникающих при этом.

3.31 **Безопасность информационных активов:** сохранение конфиденциальности, целостности и доступности информационных активов.

3.32 **Доступность информационных активов:** свойство информационной безопасности, состоящее в том, что информационные активы предоставляются авторизованному пользователю, причем в виде и месте, необходимом пользователю, и в то время, когда они ему необходимы.

3.33 **Конфиденциальность информационных активов:** свойство информационной безопасности, состоящее в том, что обработка, хранение и передача информационных активов осуществляется таким образом, что информационные активы доступны только авторизованным пользователям, объектам системы или процессам.

3.34 **Целостность информационных активов:** свойство информационной безопасности сохранять неизменность или обнаруживать факт изменения в своих информационных активах.

3.35 **Ресурс организации БС:** актив организации БС, который используется или потребляется в процессе выполнения некоторой деятельности.

3.36 **Система информационной безопасности:** совокупность защитных мер, защитных средств и процессов их эксплуатации, включая ресурсное и административное (организационное) обеспечение.

3.37 **Система менеджмента информационной безопасности:** часть менеджмента организации БС, предназначенная для создания, реализации, эксплуатации, мониторинга, анализа, поддержки и совершенствования системы обеспечения информационной безопасности.

3.38 **Система обеспечения информационной безопасности:** совокупность системы информационной безопасности и системы менеджмента информационной безопасности организации БС.

3.39 **Область действия системы обеспечения информационной безопасности (область действия СОИБ):** совокупность информационных активов и элементов информационной инфраструктуры организации БС.

3.40 **Осознание необходимости обеспечения информационной безопасности (осознание ИБ):**понимание руководством организации БСнеобходимости самостоятельно, на основе принятых в этойорганизации БСценностей и накопленных знаний формировать и учитывать в рамках основной деятельности организации БСпрогноз результатов деятельности по обеспечению информационной безопасности, а также поддерживать эту деятельность адекватно прогнозу.

Примечание – осознание информационной безопасности является внутренней побудительной причиной для руководства организации БС инициировать и поддерживать деятельность по обеспечению информационной безопасности в отличие от побуждения или принуждения, когда решение об инициировании и поддержке деятельности по обеспечению информационной безопасности определяется соответственно либо возникшими проблемами банка, либо внешними факторами, например, требованиями законов.

3.41 **Риск:** мера, учитывающая вероятность реализации угрозы и величину потерь (ущерба) от реализации этой угрозы.

Примечание –риск информационной безопасности часто выражается как сочетание последствий события

информационной безопасности и связанной вероятностью его возникновения.

3.42 **Риск нарушения информационной безопасности (риск нарушения ИБ):** риск, связанный с угрозой информационной безопасности, который включает в себя киберриск - как риск возникновения у банка потерь (убытков) и (или) дополнительных затрат, риск не получить запланированные доходы вследствие противоправных действий лиц (группы лиц) в отношении компьютерных и информационных систем или сетей, систем связи, информационных ресурсов и потоков банка, совершаемых посредством использования информационных и телекоммуникационных технологий,в целях несанкционированного доступа к указанным объектам информационной инфраструктуры банка и направленных на нарушение конфиденциальности, целостности, доступности, подлинности и сохранности защищаемой информации.

3.43 **Допустимый риск нарушения информационной безопасности:** риск нарушения информационной безопасности, предполагаемый ущерб от которого организация БС в данное время и в данной ситуации готова принять.

3.44 **Обработка риска нарушения информационной безопасности:** процесс выбора и осуществления защитных мер, снижающих риск нарушения информационной безопасности, или мер по переносу, принятию или уходу от риска.

3.45 **Остаточный риск нарушения информационной безопасности:** риск, остающийся после обработки риска нарушения информационной безопасности.

3.46 **Оценка риска нарушения информационной безопасности:** систематический и документированный процесс выявления, сбора, использования и анализа информации, позволяющий провести оценивание рисков нарушения информационной безопасности, связанных с использованием информационных активов организации БС на всех стадиях их жизненного цикла.

3.47 **Защитная мера:** сложившаяся практика, процедура или механизм, которые используются для уменьшения риска нарушения информационной безопасности организации БС.

3.48 **Угроза:** опасность, предполагающая возможность потерь (ущерба).

3.49 **Безопасность** организации БС**:** состояние защищенности интересов (целей) организации БС в условиях угроз.

3.50 **Угроза информационной безопасности (угроза ИБ):** угроза нарушения свойств информационной безопасности (доступности, целостности или конфиденциальности) информационных активов организации БС.

3.51 **Уязвимость информационной безопасности (уязвимость ИБ):** слабость в инфраструктуре организации БС, включая систему обеспечения информационной безопасности, которая может быть использована для реализации или способствовать реализации угрозы информационной безопасности.

3.52 **Ущерб:** утрата активов, повреждение (утрата свойств) активов и (или) инфраструктуры организации БС или другой вред активам и (или) инфраструктуре организации БС, наступивший в результате реализации угроз информационной безопасности через уязвимости информационной безопасности.

3.53 **Инцидент информационной безопасности в организации БС (инцидент ИБ):** событие или комбинация событий, указывающая на свершившуюся, предпринимаемую или вероятную реализацию угрозы информационной безопасности, результатом которой являются:

— нарушение или возможное нарушение работы средств защиты информации в составе системы обеспечения информационной безопасности организации БС;

— нарушение или возможное нарушение требований законодательства, нормативных актов и предписаний регулирующих и надзорных органов, внутренних документов организации БС в области обеспечения информационной безопасности, нарушение или возможное нарушение в выполнении процессов системы обеспечения информационной безопасности организации БС;

— нарушение или возможное нарушение в выполнении банковских технологических процессов организации БС;

— нанесение или возможное нанесение ущерба организации БС и (или) ее клиентам.

3.54 **Нарушитель информационной безопасности (нарушитель ИБ):** субъект, реализующий угрозы информационной безопасности, нарушая установленные правила доступа к активам организации БС или распоряжения ими.

3.55 **Модель нарушителя информационной безопасности (модель нарушителя ИБ):** описание и классификация нарушителей информационной безопасности, включая описание их опыта, знаний, доступных ресурсов, необходимых для реализации угрозы, возможной мотивации их действий, а также способы реализации угроз информационной безопасности со стороны указанных нарушителей.

3.56 **Модель угроз информационной безопасности (модель угроз ИБ):** описание источников угроз информационной безопасности; методов реализации угроз информационной безопасности; объектов, пригодных для реализации угроз информационной безопасности; уязвимостей, используемых источниками угроз информационной безопасности; типов возможных потерь (например, нарушение доступности, целостности или конфиденциальности информационных активов); масштабов потенциального ущерба.

3.57 **План работ по обеспечению информационной безопасности:** документ, устанавливающий перечень намеченных к выполнению работ или мероприятий по обеспечению информационной

безопасности организации БС, их последовательность, объем (в той или иной форме), сроки выполнения, ответственных лиц и конкретных исполнителей.

3.58 **Свидетельства выполнения деятельности по обеспечению информационной безопасности:** документ или элемент документа, содержащий достигнутые результаты (промежуточные или окончательные), относящиеся к обеспечению информационной безопасности организации БС.

3.59 **Политика информационной безопасности (политика ИБ):** документация, определяющая высокоуровневые цели, содержание и основные направления деятельности по обеспечению информационной безопасности, предназначенная для организации БС в целом.

3.60 **Частная политика информационной безопасности:** политика информационной безопасности применительно к одной или нескольким областям информационной безопасности, видам и технологиям деятельности организации БС.

3.61 **Мониторинг информационной безопасности (мониторинг):** постоянное наблюдение за объектами и субъектами, действиями и процессами, влияющими на информационную безопасность организации БС, а также регистрация, сбор, анализ и обобщение результатов наблюдений.

3.62 **Аудит информационной безопасности организации БС (аудит ИБ):** периодический, независимый и документированный процесс получения свидетельств аудита и объективной их оценки с целью установления степени выполнения в организации БС установленных требований по обеспечению информационной безопасности.

Примечания:

1 Внутренние аудиты, иногда называемые аудитами первой стороны, проводятся обычно самойорганизацией БС или от его имени для анализа со стороны руководства организации БС и других внутренних целей и могут служить основанием для декларирования организацией БС своего соответствия.

2 Внешние аудиты включают аудиты, обычно называемые аудитами второй стороны или аудитами третьей стороны. Аудиты второй стороны проводятся сторонами, заинтересованными в деятельности организации БС. Аудиты третьей стороны проводятся внешними независимыми организациями.

3 Независимость при аудите предполагает полную свободу аудитора (самостоятельность) в отборе и анализе свидетельства аудита (изложение фактов или другой информации, связанной с критериями аудита) в отношении объекта аудита.

3.63 **Оценка соответствия информационной безопасности; оценка соответствия ИБ**: систематический и документируемый процесс получения свидетельств деятельности организации БС по реализации требований информационной безопасности и установлению степени выполнения в организации БС критериев оценки (аудита) информационной безопасности.

3.64 **Самооценка информационной безопасности; самооценка ИБ**: оценка соответствия информационной безопасности, выполняемая работниками организации БС.

3.65 **Критерий оценки (аудита) информационной безопасности (критерий оценки (аудита) ИБ)**: правило принятия решенияо соответствии требованию в области информационной безопасности.

Примечания

1 В качестве критериев могут выступать некоторые требования в области информационной безопасности.

2 Совокупность критериев характеризует некоторый уровень информационной безопасности организации БС.

3 Критерии аудита информационной безопасности используются для сопоставления с ними свидетельств аудита информационной безопасности.

3.66 **Свидетельства оценки соответствия (аудита) информационной безопасности установленным критериям (свидетельства оценки соответствия (аудита) ИБ):** записи, изложение фактов или другая документированная информация, которые имеют отношение к критериям оценки соответствия (аудита) информационной безопасности и могут быть проверены.

Примечание - Свидетельства оценки соответствия (аудита) информационной безопасности могут быть качественными или количественными.

3.67 **Выводы аудита информационной безопасности (выводы аудита ИБ):** результат оценки собранных свидетельств аудита информационной безопасности.

3.68 **Заключение по результатам аудита информационной безопасности (аудиторское заключение, заключение по результатам аудита ИБ):** качественная или количественная оценка степени соответствия установленным критериям аудита информационной безопасности, представленная аудиторской группой после рассмотрения всех выводов аудита информационной безопасности в соответствии с целями аудита.

3.69 **Область аудита информационной безопасности (область аудита ИБ):** содержание и границы аудита информационной безопасности.

Примечание – Область аудита информационной безопасности обычно включает местонахождение, организационную структуру, виды деятельности проверяемойорганизации БС и процессы, которые подвергаются аудиту информационной безопасности, а также охватываемый период времени.

3.70 **Программа аудита информационной безопасности (программа аудита ИБ):** план деятельности по проведению одного или нескольких аудитов информационной безопасности (и других проверок информационной безопасности), запланированных на конкретный период времени и направленных на достижение конкретной цели.

Примечание – Программа аудита информационной безопасности включает всю деятельность, необходимую для планирования, проведения, контроля, анализа и совершенствования аудитов информационной безопасности (других

проверок информационной безопасности).

3.71 **Менеджмент:** скоординированная деятельность по руководству и управлению.

4 Сокращения

АБС – автоматизированная банковская система;
БС –банковская система Республики Беларусь;
ЖЦ – жизненный цикл;
ИБ – информационная безопасность;
НСД – несанкционированный доступ;
НРД – нерегламентированные действия в рамках предоставленных полномочий;
ОС – операционная система;
ПО – программное обеспечение;
СКЗИ – средства криптографической защиты информации;
СМИБ – система менеджмента информационной безопасности;
СИБ – система информационной безопасности;
СОИБ – система обеспечения информационной безопасности;
ТНПА –технический нормативный правовой акт.

5 Исходная концептуальная схема (парадигма) обеспечения информационной безопасности организаций БС

5.1 Сущность бизнеса заключается в вовлечении актива, принадлежащего собственнику (организации БС), в бизнес-процесс. Эта деятельность всегда подвержена рискам, так как и на сам актив, и на бизнес-процесс могут воздействовать различного рода угрозы.

Каждая угроза имеет свой источник и имеет соответствующую вероятность реализации.

Выделяют источники угроз природного, техногенного и антропогенного характера. Источники угроз антропогенного характера могут быть как злоумышленные, так и незлоумышленные.

5.2 В основе исходной концептуальной схемы ИБ организаций БС рассматривается противоборство собственника [2] и злоумышленника [3] с целью нарушения свойств конфиденциальности, целостности, доступности информационных активов. Однако другие незлоумышленные действия или источники угроз также рассматриваются в настоящих Технических требованиях и правилах.

Если злоумышленнику удается установить такой контроль, то, как самойорганизации БС, так и клиентам, которые доверили ей свои собственные активы, наносится ущерб.

5.3 Руководство организации БС должно знать, что следует защищать. Для этого необходимо определить и защитить все информационные активы (ресурсы), реализация угроз в отношении которых может нанести ущерб организации БС.

5.4 Наибольшими возможностями для нанесения ущерба организации БС обладает его собственный персонал. В этом случае содержанием деятельности злоумышленника является прямое нецелевое использование предоставленного ему в порядке выполнения служебных обязанностей контроля над активами либо нерегламентированная деятельность для получения контроля над активами, либо умышленная бездеятельность в части исполнения своих служебных (должностных) обязанностей. При этом злоумышленник будет стремиться к сокрытию следов своей деятельности.

Внешний злоумышленник, как правило, имеет сообщника (сообщников) внутри организации БС.

Незлоумышленные действия собственных работников создают либо уязвимости ИБ, либо инциденты, влияющие на свойства доступности, целостности и конфиденциальности актива или параметры системы, которая этот актив поддерживает.

5.5 Практически никогда не известно о готовящемся нападении, оно, как правило, бывает неожиданным. Нападения, как правило, носят локальный и конкретный характер по месту, цели и времени.

5.6 Злоумышленник изучает объект нападения, как правило, не только теоретически, никак не проявляя себя, но и практически, путем выявления уязвимостей АБС. Путем поиска или создания уязвимостей АБС он отрабатывает наиболее эффективный метод нападения (получения контроля над активом).

С целью снижения рисков нарушения ИБ АБС и управления ими собственник создает уполномоченный орган - свою службу ИБ (подразделение (лицо) в организации БС, ответственное за обеспечение

---

2 Под собственником здесь понимается субъект хозяйственной деятельности, имеющий права владения, распоряжения или пользования активами, который заинтересован или обязан (согласно требованиям законов или иных законодательных или технических нормативных правовых актов) обеспечивать защиту активов от угроз, которые могут снизить их ценность или нанести ущерб.

3 Под злоумышленником здесь понимается лицо, которое совершает или совершило заранее обдуманное действие или бездействие с осознанием его опасных последствий или не предвидело, но должно было и могло предвидеть возможность наступления таких последствий (адаптировано из [3], статья 22).

ИБ), организует создание и эксплуатацию СОИБ, а также организует эксплуатацию АБС в соответствии с правилами и требованиями, задаваемыми СОИБ. Одна из задач службы ИБ - выявление следов активности нарушителя.

5.7 Одним из главных инструментов собственника в обеспечении ИБ является прогноз, основанный на опыте (составление модели угроз и модели нарушителя[4]).

Чем обоснованнее и точнее сделан прогноз, тем потенциально ниже риски нарушения ИБ при минимальных ресурсных затратах. При этом следует учитывать, что со временем угрозы их источники и риски могут изменяться, поэтому модели следует периодически пересматривать.

5.8 Наиболее правильный и эффективный способ добиться минимизации рисков нарушения ИБ организации БС – разработать политику ИБ и в соответствии с ней реализовывать, эксплуатировать и совершенствовать СОИБ организации БС.

5.9 Политика ИБ разрабатывается на основе накопленного в организации БС опыта в области обеспечения ИБ, результатов идентификации активов, подлежащих защите, результатов оценки рисков с учетом особенностей бизнеса и технологий, требований законодательства Республики Беларусь, нормативных правовых актов Национального банка Республики Беларусь, а также интересов и бизнес-целей конкретнойорганизации БС.

5.10 Соблюдение политики ИБ в значительной степени является элементом корпоративной этики, поэтому на уровень ИБ организации БС серьезное влияние оказывают отношения как в коллективе, так и между коллективом и собственником или менеджментом организации БС, представляющим интересы собственника. Поэтому этими отношениями необходимо управлять. Понимая, что наиболее критичным элементом безопасности организации БС является его персонал, собственник должен всемерно поощрять заинтересованность и осведомленность персонала в решении проблем ИБ.

5.11 Не каждая организация БС располагает потенциалом для самостоятельного составления моделей угроз и нарушителя, а также политики ИБ. В этом случае эти модели должны составляться с привлечением сторонних компетентных организаций.

Модели угроз и нарушителя должны учитывать разработки авторитетных и компетентных специалистов в области ИБ и банковской деятельности, а также международный опыт в этой сфере. Модели должны быть документированы.

5.12 При разработке моделей угроз и моделей нарушителя необходимо учитывать, что из всех возможных объектов нападения с наибольшей вероятностью нарушитель выберет наиболее слабо контролируемый, где его деятельность будет оставаться необнаруженной максимально долго. Следовательно, все операции в банковских технологических процессах, где осуществляется взаимодействие персонала со средствами и системами автоматизации должны особенно тщательно контролироваться.

5.13 Стратегия обеспечения ИБ организации БС заключается как в эффективном использовании по имеющемуся плану заранее разработанных мер по обеспечению ИБ, противостоящих атакам злоумышленников, так и в регулярном пересмотре (актуализации) моделей и политик ИБ, а также корректировке СОИБ. В случае реализации угроз должен быть использован дополнительный (специально разработанный) план действий, позволяющий свести к минимуму возможные потери и восстановить эффективность СОИБ.

5.14 Любой целенаправленной деятельности (бизнесу) свойственны риски. Это - объективная реальность, и понизить эти риски можно лишь до определенного остаточного уровня. Оставшаяся часть риска (остаточный риск), определяемая в том числе факторами среды деятельности организации БС, должна быть признана приемлемой, принята либо отклонена. В этом случае от риска следует либо уклониться (изменить среду деятельности), либо перевести на кого-нибудь (например, застраховать). Таким образом, уровень защищенности интересов (целей) организации БС определяется величиной принятых ею остаточных рисков, а также эффективностью работ по поддержанию принятых рисков на допустимом, низком (остаточном) уровне.

5.15 Риски нарушения ИБ должны быть согласованы и иерархически связаны с рисками основной деятельности (бизнес-деятельности) организации БС через возможный ущерб.

Риски нарушения ИБ выражаются в возможности потери состояния защищенности интересов (целей) организации БС в информационной сфере и возникновения, вследствие этого, ущерба для бизнеса или убытков.

Потеря состояния защищенности интересов (целей) организации БС в информационной сфере заключается в утрате свойств доступности, целостности или конфиденциальности информационных активов, утрате заданных целями бизнеса параметров или доступности информационной инфраструктуры организации БС.

5.16 Уязвимость ИБ создает предпосылки к реализации угрозы через нее (инцидент ИБ). Реализация угрозы нарушения ИБ приводит к утрате защищенности интересов (целей) в информационной сфере, в

---

4 Модели ИБ (угроз и нарушителей) предназначены отражать будущее, вследствие чего они носят прогнозный характер. Модели ИБ разрабатываются на основе фактов прошлого и опыта, но ориентированы на будущее. При разработке моделей (прогнозе) используется имеющийся опыт и знания, поэтому чем выше знания, тем точнее прогноз.

результате чего организации БС наносится ущерб. Тяжесть ущерба совместно с вероятностью приводящего к нему инцидента ИБ определяют величину риска.

5.17 Постоянный анализ и изучение инфраструктуры организации БС с целью выявления и устранения уязвимостей ИБ - основа эффективной работы СОИБ.

5.18 Анализ и оценка рисков нарушения ИБ должна основываться на идентификации активов организации БС, на их ценности для целей и задач организации БС, на моделях угроз и нарушителей ИБ.

5.19 При принятии решений о внедрении защитных мер для противодействия идентифицированным угрозам (рискам) необходимо учитывать, что это увеличивает сложность СОИБ организации БС и, как правило, порождает новые риски. Поэтому при выборе решения о внедрении защитных мер для обработки существующих рисков учитывают вопросы использования защитных мер и их влияния на общую структуру рисков организации БС.

5.20 Организация БС осуществляет свою деятельность путем реализации совокупности процессов, среди которых возможно выделение следующих групп:

– основные процессы, обеспечивающие достижение целей и задач организации БС;

– вспомогательные процессы, обеспечивающие качество, в том числе обеспечение ИБ организации БС;

– процессы менеджмента (управления), обеспечивающие поддержку параметров основных и вспомогательных процессов в заданных пределах и их корректировку в случае изменения внешних или внутренних условий.

Такое разделение процессов является условным, так как основные и вспомогательные процессы нередко образуют единое целое, например, функционирование защитных мер составляет часть группы основных процессов. В то же время процессы менеджмента отделены от основных и вспомогательных процессов, которые являются объектами менеджмента.

5.21 Совокупность защитных мер, реализующих обеспечение ИБ организации БС, процессов их эксплуатации, включая ресурсное и административное (организационное) обеспечение, составляет СИБ организации БС.

Совокупность процессов менеджмента ИБ, включая ресурсное и административное (организационное) обеспечение этих процессов, составляет СМИБ организации БС.

Совокупность СИБ и СМИБ составляет СОИБ организации БС.

5.22 Процессы эксплуатации защитных мер функционируют в реальном времени. Совокупность защитных мер и процессов их использования должны обеспечивать текущий требуемый уровень ИБ в условиях штатного функционирования, а также в условиях реализации учтенных в моделях угроз организации БС, приводящих к возникновению:

– локальных инцидентов ИБ;

– широкомасштабных катастроф и аварий различной природы, последствия которых могут иметь отношения к ИБ организации БС.

5.23 СОИБ должна быть определена, спланирована и регламентирована. Однако даже правильно выстроенные процессы и используемые защитные меры в силу объективных причин со временем имеют тенденцию к ослаблению своей эффективности, что ведет к деградации системы защиты и возрастанию рисков нарушения ИБ.

Для поддержания системы защиты на должном уровне в качестве оперативной меры используется мониторинг событий и инцидентов в СИБ. Менеджмент событий и инцидентов безопасности, выявленных в процессе мониторинга, позволяет избежать деградации и обеспечить требуемый уровень безопасности активов.

Для оценки состояния ИБ защищаемого актива и выявления признаков деградации используемых защитных мер проводится оценка соответствия системы требованиям настоящим Техническим требованиям и правилам.

5.24 Для реализации и поддержания ИБ в организации БС необходима реализация четырех групп процессов:

– планирование СИБ организации БС (планирование);

– реализация СИБ организации БС (реализация);

– мониторинг и анализ СИБ организации БС (проверка);

– поддержка и улучшение СИБ организации БС (совершенствование).

Указанные группы процессов составляют СМИБ организации БС.

5.25 Менеджмент ИБ является частью общего корпоративного менеджмента организации БС, который ориентирован на содействие достижению целей деятельности организации через обеспечение защищенности ее информационной сферы.

Группы процессов СМИБ организации БС следует организовывать в виде циклической модели Деминга: «планирование - реализация - проверка - совершенствование», которая является основой модели менеджмента качества по СТБ ISO9001 и менеджмента ИБ по СТБ ISO/IEC27001. Организация и выполнение процессов СМИБ необходимы, в том числе для обеспечения уверенности в том, что хороший практический опыт организации БС документируется, становится обязательным к применению, а СОИБ

совершенствуется.

5.26 Основой для построения СОИБ организации БС являются требования законодательства, технических нормативных правовых актов Республики Беларусь, нормативных правовых актов Национального банка Республики Беларусь, контрактные обязательства организации БС, а также условия ведения бизнеса, выраженные в форме оценок рисков на основе идентификации активов и уязвимостей, построения моделей нарушителей и угроз.

5.27 На рисунке 1 приведена взаимосвязь СИБ, СМИБ и СОИБ организации БС.

Рисунок 1 - Система обеспечения информационной безопасности организации БС

5.28 Руководству организации БС необходимо инициировать, поддерживать и контролировать выполнение процессов СОИБ. Степень выполнения указанной деятельности со стороны руководства организации БС определяется осознанием необходимости обеспечения ИБ. Осознание необходимости обеспечения ИБ организации БС проявляется в использовании руководством бизнес-преимуществ обеспечения ИБ, способствующих формированию условий для дальнейшего развития бизнеса организации БС с допустимыми (приемлемыми) рисками.

5.29 Осознание необходимости обеспечения ИБ является внутренним побудительным мотивом руководства организации БС постоянно инициировать, поддерживать, анализировать и контролировать СОИБ в отличие от ситуации, когда решение о выполнении указанных видов деятельности принимается либо в результате возникших проблем, либо определяется внешними факторами.

5.30 Осознание необходимости обеспечения ИБ организации БС выражается посредством выполнения в рамках СМИБ деятельности со стороны руководства, направленной на инициирование, поддержание, анализ и контроль СОИБ организации БС.

6 Модели угроз и нарушителей информационной безопасности организации БС

6.1 Модели угроз и нарушителей должны быть основным инструментом при развертывании, поддержании и совершенствовании СОИБ организации БС.

6.2 Деятельность организации БС поддерживается информационной инфраструктурой, входящей в ее состав, которая обеспечивает реализацию банковских технологий и может быть представлена в виде иерархии следующих основных уровней:

– физического (линии связи, аппаратные средства и др.);
– сетевого оборудования (маршрутизаторы, коммутаторы, концентраторы и др.);
– сетевых приложений и сервисов;
– операционных систем (ОС);
– систем управления базами данных (СУБД);
– банковских технологических процессов и приложений;
– бизнес-процессов организации БС.

6.3 На каждом из уровней угрозы и их источники (в том числе злоумышленники), методы и средства защиты и подходы к оценке эффективности различны.

6.4 Главной целью злоумышленника является получение контроля над информационными активами на уровне бизнес-процессов. Прямое нападение на уровне бизнес-процессов, например путем раскрытия

конфиденциальной банковской аналитической информации, более эффективно для злоумышленника и опаснее для собственника, чем нападение, осуществляемое через нижние уровни, требующее специфических знаний, опыта и ресурсов (в том числе временных), и поэтому менее эффективно по соотношению «затраты/получаемый результат».

Другими целями злоумышленника могут являться нарушения функционирования бизнес-процессов организации БС путем нарушения доступности или целостности информационных активов, например, посредством распространения вредоносных программ или нарушения правил эксплуатации ЭВМ или их сетей.

6.5 Организация БС должна определить конкретные объекты среды информационных активов на каждом из уровней информационной инфраструктуры.

6.6 Основными источниками угроз ИБ являются:

– неблагоприятные события природного, техногенного и социального характера;

– террористы и криминальные элементы;

– зависимость от поставщиков/провайдеров/партнеров/клиентов;

– сбои, отказы, разрушения/повреждения программных и технических средств;

– работники организации БС, реализующие угрозы ИБ с использованием легально предоставленных им прав и полномочий (внутренние нарушители ИБ);

– работники организации БС, реализующие угрозы ИБ вне легально предоставленных им прав и полномочий, а также субъекты, не являющиеся работниками организации БС, но осуществляющие попытки НСД и НРД (внешние нарушители ИБ);

– несоответствие требованиям надзорных и регулирующих органов и/или действующему законодательству.

6.7 Наиболее актуальные источники угроз на физическом уровне, уровне сетевого оборудования и уровне сетевых приложений:

– внешние нарушители ИБ - лица, разрабатывающие/распространяющие вирусы и другие вредоносные программные коды; лица, организующие DoS, DDoSи иные виды атак; лица, осуществляющие попытки НСД и НРД;

– внутренние нарушители ИБ: персонал, имеющий право доступа к аппаратному оборудованию, в том числе сетевому, администраторы серверов, сетевых приложений и т. п.;

– комбинированные источники угроз: внешние и внутренние нарушители ИБ, действующие совместно и (или) согласованно;

– сбои, отказы, разрушения/повреждения программных и технических средств.

6.8 Наиболее актуальные источники угроз на уровнях операционных систем, систем управления базами данных, банковских технологических процессов:

– внутренние нарушители ИБ: администраторы ОС, администраторы СУБД, пользователи банковских приложений и технологий, администраторы ИБ и т. д.;

– комбинированные источники угроз: внешние и внутренние нарушители ИБ, действующие в сговоре[5].

6.9 Наиболее актуальные источники угроз на уровне бизнес-процессов:

– внутренние нарушители ИБ: авторизованные пользователи и операторы АБС, представители менеджмента организации БС и др.;

– комбинированные источники угроз: внешние нарушители ИБ (например, конкуренты) и внутренние, действующие в сговоре;

– несоответствие требованиям надзорных и регулирующих органов и/или действующему законодательству.

6.10 Источники угроз для реализации угрозы используют уязвимости ИБ.

6.11 Хорошей практикой в организациях БС является разработка моделей угроз и нарушителей ИБ для организации БС в целом, а также при необходимости для ее отдельных банковских процессов.

Степень детализации параметров моделей угроз и нарушителей ИБ может быть различна и определяется реальными потребностями каждойорганизации БС индивидуально.

7 Система информационной безопасности организаций БС

7.1 Общие положения

7.1.1 Выполнение требований к СИБ организации БС является основой для обеспечения должного уровня ИБ. Формирование требований к СИБ организации БС должно проводиться на основе:

– требований настоящих Технических требований и правил;

– выполнения деятельности в рамках СМИБ организации БС, определенной в разделе 8 (в частности, деятельности по разработке планов обработки рисков нарушения ИБ).

---

5 На данных уровнях и уровне бизнес-процессов реализация угроз внешними нарушителями ИБ, действующими самостоятельно без соучастия внутренних нарушителей, практически невозможна.

Требования к СИБ организации БС должны быть оформлены документально.

7.1.2 Требования подразделов 7.2 - 7.9 образуют базовый набор требований к СИБ, применимый к большинству организаций БС. В соответствии с особенностями конкретнойорганизации БС данный базовый набор требований может быть расширен путем выполнения деятельности в рамках процессов СМИБ, например, определения области действия СОИБ организации БС, анализа и оценки рисков нарушения ИБ.

7.1.3 Требования к СИБ должны быть сформированы, в том числе для следующих областей:

– назначения и распределения ролей и обеспечения доверия к персоналу;

– обеспечения ИБ на стадиях ЖЦ АБС;

– защиты от НСД и НРД, управления доступом и регистрацией всех действий в АБС, в телекоммуникационном оборудовании, автоматических телефонных станциях и т. д.;

– антивирусной защиты;

– использования ресурсов сети Интернет;

– использования СКЗИ;

– защиты банковских платежных и информационных технологических процессов.

В конкретнойорганизации БС требования к СИБ могут формироваться и для других областей и направлений деятельности.

7.1.4 При распределении прав доступа работников и клиентов к информационным активам организации БС следует руководствоваться принципами:

– «знать своего клиента»[6];

– «знать своего служащего»[7];

– «необходимо знать»[8],

– а также рекомендуется использовать принцип «двойное управление»[9].

7.1.5 Формирование ролей должно осуществляться на основании существующих бизнес-процессов организации БС и проводиться с целью исключения концентрации полномочий и снижения риска инцидентов ИБ, связанных с потерей информационными активами свойств доступности, целостности или конфиденциальности.

Формирование ролей не должно выполняться по принципу фиксации фактически сложившихся прав и полномочий персонала организации БС.

7.1.6 Для обеспечения ИБ и контроля за качеством обеспечения ИБ в организации БС должны быть определены роли, связанные с деятельностью по обеспечению ИБ. Руководство организации БС должно осуществлять координацию своевременности и качества выполнения ролей, связанных с обеспечением ИБ.

7.1.7 ИБ АБС должна обеспечиваться на всех стадиях ЖЦ АБС, автоматизирующих банковские технологические процессы, с учетом интересов всех сторон, вовлеченных в процессы ЖЦ (разработчиков, заказчиков, поставщиков продуктов и услуг, эксплуатирующих и надзорных подразделений организации БС).

7.1.8 При принятии руководством организации БС решений об использовании сети Интернет, при формировании документов, регламентирующих порядок использования сети Интернет, а также иных документов, связанных с обеспечением ИБ при использовании сети Интернет, необходимо учитывать следующие положения:

–сеть Интернет не имеет единого органа управления (за исключением службы управления пространством имен и адресов) и не является юридическим лицом, с которым можно было бы заключить договор (соглашение). Провайдеры (посредники) сети Интернет могут обеспечить только те услуги, которые реализуются непосредственно ими;

–существует вероятность несанкционированного доступа, потери и искажения информации, передаваемой посредством сети Интернет;

–существует вероятность атаки злоумышленников на оборудование, программное обеспечение и информационные ресурсы, подключенные/доступные из сети Интернет;

---

6 «Знать своего клиента» (KnowyourCustomer) - принцип, используемый регулирующими органами для выражения отношения к финансовым организациям с точки зрения знания деятельности их клиентов.

7 «Знать своего служащего» (KnowyourEmployee) - принцип, демонстрирующий озабоченность организации по поводу отношения служащих к своим обязанностям и возможных проблем, таких как злоупотребление имуществом, аферы или финансовые трудности, которые могут приводить к проблемам с безопасностью.

8 «Необходимо знать» (NeedtoKnow) - принцип, ограничивающий полномочия по доступу к информации и ресурсам по обработке информации на уровне минимально необходимых для выполнения определенных обязанностей.

9 «Двойное управление» (DualControl) - принцип сохранения целостности процесса и борьбы с искажением функций системы, требующий дублирования (алгоритмического, временного, ресурсного или иного) действий до завершения определенных транзакций.

–гарантии по обеспечению ИБ при использовании сети Интернет никаким органом/учреждением/ организацией не предоставляются.

7.1.9 В рамках банковских платежных технологических процессов в качестве активов, защищаемых в первую очередь, следует рассматривать:

– банковский платежный технологический процесс;

– платежную информацию;

– информацию, распространение и (или) предоставление которой ограничено, в том числе персональные данные, банковская тайна [1] [2] и данные держателей платежных карточек, как это определено международным стандартом PCI DSS.

7.1.10 Если в организации БС, в ее АБС обрабатываетсяинформация, распространение и (или) предоставление которой ограничено (не отнесенная к государственным секретам), то в целях организации мер по ее защите должна применяться система защиты информации, аттестованная в порядке, установленном Оперативно-аналитическим центром при Президенте Республики Беларусь [4].

Если в организации БС обрабатываются данные держателей платежных карточек, то в целях их защиты должны выполняться требования стандарта PCI DSS.

7.1.11 Для создания системы защиты информации должны использоваться средства технической и криптографической защиты информации, имеющие сертификат соответствия, выданный в Национальной системе подтверждения соответствия Республики Беларусь, или положительное экспертное заключение по результатам государственной экспертизы,порядок проведения которой определяется Оперативно-аналитическим центром при Президенте Республики Беларусь[4]. Протокол https в системах СДБО может применяться в случае, если выполнение криптографических преобразований вызываются функцией сертифицированного средства криптографической защиты информации.

7.1.12 Проектирование, создание и эксплуатация системы защиты информации организации БС должно осуществляться в порядке, установленном нормативными правовыми актами Республики Беларусь [4].

7.2 Общие требования по обеспечению информационной безопасности при назначении и распределении ролей и обеспечении доверия к персоналу

7.2.1 В организации БС должны быть выделены и документально определены роли его работников.

Формирование и назначение ролей работников организации БС следует осуществлять с учетом соблюдения принципа предоставления минимальных прав и полномочий, необходимых для выполнения служебных обязанностей.

7.2.2 Роли следует персонифицировать с установлением ответственности за их выполнение. Ответственность должна быть документально зафиксирована в должностных инструкциях или организационно-распорядительных документах организации БС.

7.2.3 С целью предупреждения возникновения и снижения рисков нарушения ИБне допускается совмещения в рамках одной роли следующих функций: разработки и сопровождения АБС/ПО, их разработки и эксплуатации, сопровождения и эксплуатации, администратора системы и администратора ИБ, выполнения операций в АБС и контроля их выполнения.

7.2.4 В организации БС должны быть документально определены, выполняться и регистрироваться процедуры контроля деятельности работников, обладающих совокупностью полномочий (ролями), позволяющими получить контроль над защищаемым информационным активом организации БС.

7.2.5 В организации БС должны быть документально определены процедуры приема на работу, влияющую на обеспечение ИБ, включающие:

–проверку подлинности предоставленных документов, заявляемой квалификации, точности и полноты биографических данных;

– проверку в части профессиональных навыков и оценку профессиональной пригодности.

Указанные процедуры должны предусматривать документальную фиксацию результатов проводимых проверок.

7.2.6 Рекомендуется документально определить процедуры регулярной проверки (с документальной фиксацией результатов) в части профессиональных навыков и оценки профессиональной пригодности работников, а также внеплановой проверки (с документальной фиксацией результатов) при

выявлении фактов их нештатного поведения, участия в инцидентах ИБ или подозрений в таком поведении или участии.

7.2.7 Все работники организации БС должны давать письменное обязательство о соблюдении конфиденциальности, приверженности правилам корпоративной этики, включая требования по недопущению конфликта интересов.

При взаимодействии с внешними организациями и клиентами требования по ИБ должны регламентироваться положениями, включаемыми в договоры (соглашения) с ними.

7.2.8 Обязанности персонала по выполнению требований ИБ должны включаться в трудовые контракты (соглашения, договоры) и (или) должностные инструкции.

Невыполнение работниками организации БС требований ИБ должно приравниваться к

невыполнению должностных обязанностей и приводить как минимум к дисциплинарной ответственности.

7.3 Общие требования по обеспечению информационной безопасности автоматизированных банковских систем на стадиях жизненного цикла

7.3.1 При формировании требований ИБ рекомендуется рассматривать следующие общие стадии модели ЖЦ АБС:

1) разработка технических заданий;
2) проектирование;
3) создание и тестирование;
4) приемка (включая оценку соответствия – испытания, аттестацию и т. п.) и ввод в действие;
5) эксплуатация;
6) сопровождение и модернизация;
7) снятие с эксплуатации.

В случае самостоятельной разработки АБС в организации БС следует рассматривать все стадии ЖЦ АБС, а в случае приобретения готовых АБС следует рассматривать стадии 4—7 ЖЦ АБС.

7.3.2 Выполнение работ на всех стадиях жизненного цикла АБС в части вопросов обеспечения ИБ должно осуществляться по согласованию и под контролем службы ИБ.

7.3.3 При привлечении к выполнению работ (оказанию услуг) в сфере защиты информации сторонних организаций должны соблюдаться требования нормативных правовых актов Республики Беларусь в области лицензирования деятельности по технической и (или) криптографической защите информации [5].

7.3.4 В технические задания на разработку или модернизацию АБС следует включать требования к обеспечению информационной безопасности, установленные и используемые для обеспечения ИБ в рамках технологических процессов организации БС, реализуемых создаваемой или модернизированной АБС.

7.3.5 При разработке технических заданий на системы дистанционного банковского обслуживания должно быть учтено, что защита данных должна обеспечиваться в условиях:

– попыток доступа к банковской информации анонимных, неавторизованных злоумышленников при использовании сетей общего пользования;

– возможности ошибок авторизованных пользователей систем;

– возможности ненамеренного или неадекватного использования конфиденциальных данных авторизованными пользователями.

7.3.6 На стадии создания и тестирования АБС и (или) их компонентов организация БС обеспечивает реализацию запрета использования защищаемой информации в качестве тестовых данных, анонимность данных и контроль адекватности предоставления и разграничения доступа.

7.3.7 Эксплуатируемые АБС и (или) их компоненты должны быть снабжены документацией, содержащей описание реализованных в АБС защитных мер, в том числе описание состава и требований к реализации организационных защитных мер, состава и требований к эксплуатации технических защитных мер.

Организации БС следует проводить анализ принятия разработчиком АБС защитных мер, направленных на обеспечение безопасности разработки АБС и безопасности ее поставки.

В договор (контракт) о разработке АБС или поставке готовых платформ АБС и их компонентов организацией БС должны включаться положения по сопровождению поставляемых изделий на весь срок их службы. В случае невозможности включения в договор (контракт) указанных положений должен быть приобретен полный комплект рабочей конструкторской и программной документации, обеспечивающий возможность сопровождения АБС и их компонентов без участия разработчика. Если оба указанных варианта неприемлемы, например, вследствие высокой стоимости или позиции фирмы-поставщика (разработчика), руководство организации БС должно оценить и документально оформить допустимость риска нарушения ИБ, возникающего по причине невозможности сопровождения АБС и их компонентов.

7.3.8 На стадии эксплуатации АБС должны быть определены, выполняться и регистрироваться процедуры:

– контроля работоспособности (функционирования, эффективности) реализованных в АБС защитных мер, в том числе контроль реализации организационных защитных мер, контроль состава и параметров настройки применяемых технических защитных мер;

– контроля отсутствия уязвимостей в оборудовании и программном обеспечении АБС;

– контроля внесения изменений в параметры настройки АБС и применяемых технических защитных мер;

– контроля необходимого обновления программного обеспечения АБС, включая программное обеспечение технических защитных мер.

7.3.9 На стадии эксплуатации АБС должны быть определены, выполняться, регистрироваться и контролироваться процедуры, необходимые для обеспечения восстановления всех реализованных функций по обеспечению ИБ.

7.3.10 На стадии эксплуатации АБС должны быть определены, выполняться и регистрироваться

процедуры контроля состава, устанавливаемого и (или) используемого ПО АБС.

7.3.11 На стадии эксплуатации АБС должны быть определены, выполняться и контролироваться процедуры, необходимые для обеспечения сохранности носителей защищаемой информации.

7.3.12 На стадии сопровождения (модернизации) должны быть документально определены и выполняться процедуры контроля, обеспечивающие защиту от:

– умышленного несанкционированного раскрытия, модификации или уничтожения информации;

– неумышленной модификации, раскрытия или уничтожения информации;

– отказа в обслуживании или ухудшения качества обслуживания.

Результаты выполнения контроля должны документироваться.

7.3.13 На стадии сопровождения (модернизации) АБС, в которых обрабатываетсяинформация, распространение и (или) предоставление которой ограничено (не отнесенная к государственным секретам), в том числе АБС, задействованных в реализации банковского платежного технологического процесса, должны быть определены, выполняться и регистрироваться процедуры:

– фиксации внесенных изменений;

– проверки функциональности АБС, в том числе применяемых мер защиты информации, после внесения изменений.

7.3.14 На стадии снятия с эксплуатации должны быть документально определены, выполняться и документироваться процедуры, обеспечивающие удаление информации, несанкционированное использование которой может нанести ущерб бизнес-деятельности организации БС, и информации, используемой средствами обеспечения ИБ, из постоянной памяти АБС и с внешних носителей, за исключением архивов электронных документов и протоколов электронного взаимодействия, ведение и сохранность которых в течение определенного срока предусмотрено соответствующими актами законодательства, ТНПА и (или) договорными документами.

7.3.15 Ворганизации БС должны быть выделены и назначены роли, связанные с эксплуатацией и контролем эксплуатации АБС и применяемых технических защитных мер, в том числе с внесением изменений в параметры их настройки.

Для всех АБС должны быть определены и выполняться процедуры контроля их эксплуатации (в части вопросов обеспечения ИБ) со стороны службы ИБ. Проведение мероприятий по контролю эксплуатации АБС и их результаты должны регистрироваться.

7.4 Общие требования по обеспечению информационной безопасности при управлении доступом и регистрации

7.4.1 Должны быть определены, выполняться, регистрироваться и контролироваться процедуры выявления, учета и классификации (отнесение к одному из типов) информационных активов организации БС. Права доступа работников и клиентов организации БС к информационным активам и (или) их типам должны быть учтены и зафиксированы.

7.4.2 В АБС должны быть реализованы меры по защите от НСД и НРД, в том числе с использованием соответствующих средств защиты информации

При реализации защиты от НСД должнобыть обеспечено сокрытие вводимых субъектами доступа аутентификационных данных на устройствах отображения информации. Размещение устройств отображения информации АБС должно препятствовать ее несанкционированному просмотру.

7.4.3 В организации БС должны быть определены, выполняться, регистрироваться и контролироваться следующие правила и процедуры:

– идентификации и аутентификации субъектов доступа, в том числе внешних субъектов доступа, которые не являются работниками организации БС, и программных процессов (сервисов);

– идентификации объектов доступа и закрепления за ними субъектов доступа, разграничения доступа к информационным активам на основе ролевого метода, с определением для каждой роли полномочий по доступу к информационным активам;

– определения прав и обязанностей субъектов АБС;

– управления идентификационными и аутентификационными данными;

– управления учетными записями субъектов доступа;

– управления средствами аутентификации, в том числе хранением, выдачей, инициализацией, блокированием средств аутентификации и принятием мер в случае утраты и (или) компрометации средств аутентификации;

– защиты обратной связи при вводе аутентификационной информации, путем исключения отображения для пользователя действительного значения аутентификационной информации и (или) количества вводимых пользователем символов аутентификационной информации;

– управления предоставлением/отзывом и блокированием доступа, в том числе доступа, осуществляемого через внешние информационно-телекоммуникационные сети;

– регистрации действий субъектов доступа с обеспечением возможности контроля целостности и защиты данных регистрации;

– контроля за соблюдением правил генерации и смены паролей субъектов;

– защиты от подбора реквизитов доступа, выявления и блокирования неуспешных попыток доступа;

– блокирования сеанса доступа после установленного времени бездействия или по запросу субъекта доступа, требующего выполнения процедур повторной аутентификации и авторизации для продолжения работы;

– ограничения действий пользователей по изменению настроек их автоматизированных мест (использование ограничений на изменение BIOS, UEFI);

– определение действий субъектов информационной системы, которые могут совершаться такими субъектами до их идентификации и аутентификации;

– ограничения действий пользователей по изменению параметров настроек АБС и реализации контроля действий эксплуатационного персонала по изменению параметров настроек АБС;

– выявления и блокирования несанкционированного перемещения (копирования) информации, в том числе баз данных, файловых ресурсов, виртуальных машин;

– использования технологий беспроводного доступа к информации, в случае их применения, и защиты внутренних беспроводных соединений;

– использования мобильных устройств для доступа к информации в случае их применения.

Процедуры управления доступом должны исключать возможность «самосанкционирования».

7.4.4 В организации БС необходимо документально определить процедуры мониторинга ИБ и анализа данных регистрации, действий и операций, позволяющие выявлять неправомерные или подозрительные операции и транзакции для чего, среди прочего, следует:

– определить состав и содержание информации о событиях безопасности, подлежащих регистрации (идентификация и аутентификация пользователей, нарушения прав доступа пользователей, выявленные нарушения информационной безопасности и др.)

– определить, сроки хранения информации о событиях безопасности, подлежащих регистрации;

– определить порядок сбора, записи и хранения информации о событиях безопасности в течение установленного срока хранения, но не менее шести месяцев;

– обеспечить резервирование необходимого объема памяти для записи данных;

– реализовать мониторинг (просмотр, анализ) информации о сбоях в механизмах сбора информации и о достижении предела объема (емкости) памяти устройств хранения уполномоченными субъектами АБС;

– обеспечить возможность мониторинга (просмотра, анализа) событий безопасности уполномоченными субъектами АБС;

– обеспечить реагирование на сбои при регистрации действий и операций, в том числе аппаратные и программные ошибки, сбои в технических средствах сбора данных;

– обеспечить генерацию временных меток для регистрируемых действий и операций и синхронизацию системного времени на технических средствах, используемых для целей мониторинга ИБ, анализа и хранения данных;

– применять системы сбора и обработки данных событий информационной безопасности.

В системах защиты информации АБС долженбыть реализован аудит безопасности в соответствии с требованиями ТНПА в сфере защиты информации.

Процедуры мониторинга и анализа должны использовать документально определенные критерии выявления неправомерных или подозрительных действий и операций. Указанные процедуры мониторинга и анализа рекомендуется применять на регулярной основе, например, ежедневно по выборке выполненных операций и транзакций определяемой организацией БС.

7.4.5 В организации БС необходимо определить и контролировать выполнение требований:

– к разделению сегментов вычислительных сетей, в том числе создаваемых с использованием технологии виртуализации;

– к межсетевому экранированию;

– к информационному взаимодействию между сегментами вычислительных сетей. Разделение сегментов вычислительных сетей следует осуществлять с целью обеспечения независимого выполнения банковских платежных технологических процессов организации БС, а также банковских информационных технологических процессов организации БС разной степени критичности, в том числе банковских информационных технологических процессов, в рамках которых осуществляется обработка информации, распространение и (или) предоставление которой ограничено, а также банковских информационных технологических процессов, обрабатывающих данные держателей платежных карточек.

7.4.6 В системах защиты информации АБС должны быть реализованы меры по обеспечению контроля за работоспособностью, параметрами настройки и правильностью функционирования средств вычислительной техники, сетевого оборудования, системного программного обеспечения и средств защиты информации.

7.4.7 Должен быть определен, выполняться, регистрироваться и контролироваться порядок доступа к объектам среды информационных активов, в том числе в помещения, в которых размещаются объекты среды информационных активов.

7.4.8 В организации БС должен быть определен, выполняться и контролироваться порядок

использования съемных носителей информации

7.4.9 Используемые в организации БС АБС, в том числе системы дистанционного банковского обслуживания, должны обеспечивать возможность регистрации:

– операций с данными о клиентских счетах, включая операции открытия, модификации и закрытия клиентских счетов;

– проводимых транзакций, имеющих финансовые последствия;

– операций, связанных с назначением и распределением прав пользователей.

7.4.10 Системы дистанционного банковского обслуживания должны реализовывать защитные меры, обеспечивающие невозможность отказа от авторства проводимых клиентами операций и транзакций.

Протоколам операций, выполняемых посредством систем дистанционного банковского обслуживания, рекомендуется придать свойство юридической значимости, например, путем внесения соответствующих положений в договоры на дистанционное банковское обслуживание.

7.4.11 При заключении договоров со сторонними организациями рекомендуется юридическое оформление договоренностей, предусматривающих необходимый уровень взаимодействия, в случае выхода инцидента ИБ за рамки отдельнойорганизации БС. Примером такого взаимодействия может служить приостановка выполнения распределенной между несколькими организациями БС транзакции в случае, если имеющиеся данные мониторинга и анализа протоколов операций позволяют предположить, что выполнение данной транзакции является частью замысла злоумышленников.

7.4.12 Должны быть документально оформлены и доведены до сведения работников и клиентов организации БС процедуры, определяющие действия в случае компрометации информации, необходимой для их идентификации, аутентификации и (или) авторизации, в том числе произошедшей по их вине, включая информацию о способах распознавания таких случаев.

Эти процедуры должны предусматривать документирование работниками и клиентами всех своих действий и их результатов.

7.4.13 В системах дистанционного банковского обслуживания должны быть реализованы механизмы информирования (регулярного, непрерывного или по требованию) клиентов обо всех операциях, совершаемых от их имени.

7.4.14 При осуществлении доступа на участке телекоммуникационных каналов и линий связи, в том числе беспроводных, не контролируемых организации БС, должны использоваться сетевые протоколы, обеспечивающие защиту сетевого соединения, контроль целостности сетевого взаимодействия и реализацию технологии двухсторонней аутентификации.

7.4.15 Передача защищаемых данных по каналам связи, имеющим выход за пределы контролируемой организации БС зоны, должна осуществляться только при условии обеспечения их защиты от НСД.

7.4.16 В организации БС должны применяться меры, направленные на обеспечение защиты от НСД, повреждения или нарушения целостности данных о действиях и операциях, а также меры по защите информации, необходимой для идентификации, аутентификации и (или) авторизации клиентов и работников организации БС. Все попытки НСД к такой информации должны регистрироваться. Доступ к данным о действиях и операциях предоставляется только с целью выполнения служебных обязанностей.

При увольнении или изменении должностных обязанностей работников организации БС, имевших доступ к указанным данным, необходимо выполнить регламентированные процедуры соответствующего пересмотра прав доступа.

7.4.17 Работа всех пользователей АБС должна осуществляться под уникальными и персонифицированными учетными записями.

7.5 Общие требования по обеспечению информационной безопасности средствами антивирусной защиты

7.5.1 На всех автоматизированных рабочих местах и серверах АБС, если иное не предусмотрено технологическим процессом, должны применяться средства антивирусной защиты.

В организации БС должны быть определены, выполняться, регистрироваться и контролироваться процедуры установки и регулярного обновления средств антивирусной защиты (версий и баз данных) на автоматизированных рабочих местах и серверах АБС.

Рекомендуется организовать функционирование постоянной антивирусной защиты в автоматическом режиме и автоматический режим установки обновлений антивирусного программного обеспечения и его баз данных.

Установка и обновление антивирусных средств в организации БС должны контролироваться представителями подразделения организации БС, ответственными за обеспечение ИБ.

7.5.2 Должны быть разработаны и введены в действие инструкции по антивирусной защите, учитывающие особенности банковских технологических процессов.

7.5.3 Перед подключением съемных носителей информации к средствам вычислительной техники, задействованным в рамках осуществления банковских технологических процессов, рекомендуется проводить их антивирусную проверку на специально выделенном автономном средстве вычислительной техники.

7.5.4 В организации БС должна быть организована антивирусная фильтрация всего трафика электронного почтового обмена.

7.5.5 Рекомендуется организовать построение эшелонированной централизованной системы антивирусной защиты, предусматривающей использование средств антивирусной защиты различных производителей и их раздельную установку на:

– рабочих станциях и серверах;

– серверном оборудовании сервисов электронной почты;

– технических средствах межсетевого экранирования.

7.5.6 Должны быть документально определены и выполняться процедуры предварительной проверки устанавливаемого или изменяемого программного обеспечения на отсутствие вирусов. После установки или изменения программного обеспечения должна быть выполнена антивирусная проверка. Результаты установки, изменения программного обеспечения и антивирусной проверки должны документироваться.

7.5.7 Должны быть документально определены процедуры, выполняемые в случае обнаружения компьютерных вирусов, в которых следует зафиксировать:

– необходимые меры по отражению и устранению последствий вирусной атаки;

– порядок официального информирования руководства;

– порядок приостановления при необходимости работы (на период устранения последствий вирусной атаки).

7.5.8 Должны быть документально определены и выполняться процедуры контроля отключения и обновления антивирусных средств на всех автоматизированных рабочих местах и серверах АБС. Результаты контроля должны документироваться.

7.5.9 Ответственность (руководителей, работников) за выполнение требований по антивирусной защите необходимо предусмотреть в локальных правовых актах по организации антивирусной защиты.

7.6 Общие требования по обеспечению информационной безопасности при использовании ресурсов сети Интернет

7.6.1 Решение об использовании сети Интернет для производственной деятельности должно документально приниматься руководством организации БС. При этом цели использования сети Интернет должны быть явно перечислены, например, сеть Интернет в организации БС может использоваться для:

– ведения дистанционного банковского обслуживания;

– получения и распространения информации, связанной с банковской деятельностью (например, путем создания информационных веб-сайтов организации БС);

– информационно-аналитической работы в интересах организации БС;

– обмена электронными сообщениями, например, почтовыми.

Использование сети Интернет в неустановленных целях должно быть явно запрещено.

С целью ограничения использования сети Интернет в неустановленных целях в организации БС рекомендуется провести выделение ограниченного числа пакетов, содержащих перечень сервисов и ресурсов сети Интернет, доступных для пользователей. Наделение работников организации БС правами пользователя конкретного пакета должно оформляться документально и выполняться в соответствии с его должностными обязанностями и назначенными ему ролями.

7.6.2 В организации БС должен быть документально определен порядок подключения и использования ресурсов сети Интернет, включающий положение о контроле со стороны подразделения (лица), ответственного за обеспечение ИБ в организации БС.

Должны быть разработаны и введены в действие инструкции и рекомендации по использованию сети Интернет, учитывающие особенности банковских технологических процессов.

Должны быть определены и выполняться процедуры протоколирования посещения ресурсов сети Интернет работниками организации БС. Данные о посещенных работниками организации БСресурсов сети Интернет должны быть доступны работникам службы ИБ.

7.6.3 В организации БС, осуществляющей дистанционное банковское обслуживание клиентов должны применяться средства защиты информации (межсетевые экраны, антивирусные средства, средства криптографической защиты информации и др.), обеспечивающие прием и передачу информации только в установленном формате и только для конкретной технологии.

7.6.4 Рекомендуется выполнить выделение и организовать физическую изоляцию от внутренних сетей тех компьютеров, с помощью которых осуществляется взаимодействие с сетью Интернет в режиме онлайн.

7.6.5 При осуществлении дистанционного банковского обслуживания должны применяться защитные меры, предотвращающие возможность подмены авторизованного клиента злоумышленником в рамках сеанса работы. Все попытки таких подмен должны регистрироваться установленным образом.

7.6.6 Передача защищаемых данных с использованием сети Интернет должна осуществляться только при условии обеспечения их защиты от НСД.

7.6.7 Все операции клиентов в течение всего сеанса работы с системами дистанционного бан-

ковского обслуживания должны выполняться только после выполнения процедур идентификации, аутентификации и авторизации. В случаях нарушения или разрыва соединения необходимо обеспечить повторное выполнение указанных процедур.

Для доступа пользователей к системам дистанционного банковского обслуживания рекомендуется использовать специализированное клиентское программное обеспечение со встроенными механизмами защиты.

7.6.8 Почтовый обмен через сеть Интернет должен осуществляться с использованием защитных мер. Перечень указанных защитных мер и порядок их использования должны быть определены документально.

Рекомендуется организовать почтовый обмен с сетью Интернет через ограниченное количество точек, состоящих из внешнего (подключенного к сети Интернет) и внутреннего (подключенного к внутренним сетям организации БС) почтовых серверов с безопасной системой репликации почтовых сообщений между ними (интернет-киоски).

7.6.9 Электронная почта должна архивироваться. Архив должен быть доступен подразделению (лицу), ответственному за обеспечение ИБ в организации БС. Изменения в архиве не допускаются. Порядок доступа к информации архива должен быть документально определен. Целями создания архивов электронной почты являются:

– контроль информационных потоков, в том числе с целью предотвращение утечек информации;

– использование архивов при проведении разбирательств по фактам утечек информации.

7.6.10 Рекомендуется не применять практику хранения и обработки банковской информации (в том числе открытой) на компьютерах, с помощью которых осуществляется взаимодействие с сетью Интернет в режиме онлайн. Наличие банковской информации на таких компьютерахдолжно определяться бизнес-целями организации БС и документально санкционироваться ее руководством.

7.6.11 При взаимодействии с сетью Интернет должны быть документально определены и использоваться защитные меры противодействия атакам злоумышленников и распространению спама[10].

7.7 Общие требования по порядку криптографической защиты информации

7.7.1 Криптографическая защита информации в организациях БС реализуется в порядке, установленном нормативными правовыми актами Оперативно-аналитического центра при Президенте Республики Беларусь, в случаях, если данные акты на них распространяются [4]. В иных случаях, организации БС используют криптографическую защиту информации самостоятельно в целях защиты от возможных атак, а также для соответствия требованиям, предъявляемым при взаимодействии с международными платежными системами.

Необходимость применения криптографической защиты информации определяется организацией БС самостоятельно, если иное не предусмотрено нормативными правовыми актами Республики Беларусь.

7.7.2 Применение СКЗИ в организации БС должно проводиться в соответствии с моделью угроз ИБ и моделью нарушителя ИБ, принятыми организацией БС, и описываться при проектировании системы защиты информации. Рекомендуется утвердить частную политику ИБ, касающуюся применения СКЗИ в организации БС.

7.7.3 Для обеспечения безопасности необходимо использовать СКЗИ, которые:

– допускают встраивание в технологические процессы обработки электронных сообщений, обеспечивают взаимодействие с прикладным программным обеспечением на уровне обработки запросов на криптографические преобразования и выдачи результатов;

– поставляются разработчиками с полным комплектом эксплуатационной документации, включая описание ключевой системы, правила работы с ней, а также обоснование необходимого организационно-штатного обеспечения.

7.7.4 Установка и ввод в эксплуатацию, а также эксплуатация СКЗИ должны осуществляться в соответствии с эксплуатационной и технической документацией к этим средствам.

7.7.5 При применении СКЗИ должны поддерживаться непрерывность процессов протоколирования работы СКЗИ и обеспечения целостности программного обеспечения для среды функционирования СКЗИ, представляющую собой совокупность технических и программных средств, совместно с которыми происходит штатное функционирование СКЗИ и которые способны повлиять на выполнение предъявляемых к СКЗИ требований.

7.7.6 ИБ процессов изготовления криптографических ключей СКЗИ должна обеспечиваться комплексом технологических, организационных, технических и программных мер и средств защиты, предусмотренных технической документацией на СКЗИ.

7.7.7 Для повышения уровня безопасности при эксплуатации СКЗИ и их ключевых систем рекомендуется реализовать процедуры мониторинга, регистрирующего все значимые события, состоявшиеся в процессе обмена криптографически защищенными данными, и все инциденты ИБ.

7.7.8 Порядок применения СКЗИ определяется руководством организации БС на основании

---

10 Спам - общее наименование не запрошенных пользователями электронных посланий и рекламных писем, рассылаемых в Интернете по ставшим известными рассылающей стороне адресам пользователей.

указанных выше в данном разделе документов и должен включать:

– порядок ввода в действие, включая процедуры встраивания СКЗИ в АБС;

– порядок эксплуатации;

– порядок восстановления работоспособности в аварийных случаях;

– порядок внесения изменений;

– порядок снятия с эксплуатации;

– порядок управления ключевой системой;

– порядок обращения с носителями ключевой информации, включая действия при смене и компрометации ключей.

7.7.9 Криптографические ключи могут изготавливаться организацией БС и (или) клиентом организации БС самостоятельно. Отношения, возникающие между организациями БС и их клиентами, регулируются заключаемыми договорами.

7.8 Общие требования по обеспечению информационной безопасности банковских платежных технологических процессов

7.8.1 Банковский платежный технологический процесс должен быть документирован.

7.8.2 Должны быть документально определены перечни программного обеспечения, устанавливаемого и (или) используемого в компьютерах и АБС и необходимого для выполнения конкретных банковских платежных технологических процессов. Состав программного обеспечения, установленного и используемого в компьютерах и АБС, должен соответствовать определенному в установленном порядке перечню. Выполнение данных требований должно контролироваться с документированием результатов.

7.8.3 Порядок обмена платежной информацией должен быть зафиксирован в договорах между участниками, осуществляющими обмен платежной информацией.

7.8.4 Работники организации БС, в том числе администраторы автоматизированных систем и средств защиты информации, не должны обладать полномочиями для бесконтрольного создания, авторизации, уничтожения и изменения платежной информации, а также проведения несанкционированных операций по изменению состояния банковских счетов.

7.8.5 Результаты технологических операций по обработке платежной информации должны контролироваться (проверяться) и удостоверяться уполномоченными на то лицами или автоматизированными процессами.

Рекомендуется, чтобы обработку платежной информации и контроль (проверку) результатов обработки осуществляли разные работники/автоматизированные процессы.

7.8.6 Обязанности по администрированию средств защиты платежной информации рекомендуется возлагать приказом или распоряжением по организации БС на администраторов ИБ с отражением этих обязанностей в их должностных инструкциях.

7.8.7 Комплекс мер по обеспечению ИБ банковского платежного технологического процесса должен предусматривать, в том числе:

– защиту платежной информации от искажения, фальсификации, переадресации, несанкционированного уничтожения, ложной авторизации электронных платежных сообщений;

– доступ работника организации БС только к тем ресурсам банковского платежного технологического процесса, которые необходимы ему для исполнения должностных обязанностей или реализации прав, предусмотренных технологией обработки платежной информации;

– контроль (мониторинг) исполнения установленной технологии подготовки, обработки, передачи и хранения платежной информации;

– аутентификацию входящих электронных платежных сообщений;

– двустороннюю аутентификацию автоматизированных рабочих мест (рабочих станций и серверов), участников обмена электронными платежными сообщениями;

– возможность ввода платежной информации в АБС только для авторизованных пользователей;

– контроль, направленный на исключение возможности совершения злоумышленных действий (двойной ввод, сверка, установление ограничений в зависимости от суммы совершаемых операций и т. д.);

– восстановление платежной информации в случае ее умышленного (случайного) разрушения (искажения) или выхода из строя средств вычислительной техники;

– сверку выходных электронных платежных сообщений с соответствующими входными и обработанными электронными платежными сообщениями при осуществлении межбанковских расчетов;

– возможность блокирования приема к исполнению распоряжений клиентов;

– доставку электронных платежных сообщений участникам обмена.

Кроме того, в организации БС рекомендуется организовать авторизованный ввод платежной информации в АБС двумя работниками с последующей программной сверкой результатов ввода на совпадение (принцип «двойного управления»).

7.8.8 При проектировании, разработке и эксплуатации систем дистанционного банковского обслуживания должны быть документально определены и выполняться процедуры, реализующие в том числе механизмы:

– снижения вероятности выполнения непреднамеренных или случайных операций или транзакций авторизованными клиентами;

– доведения информации о возможных рисках, связанных с выполнением операций или транзакций до клиентов.

Клиенты систем дистанционного банковского обслуживания должны быть обеспечены детальными инструкциями, описывающими процедуры выполнения операций или транзакций.

7.8.9 Должны быть документально определены процедуры обслуживания средств вычислительной техники, используемых в банковском платежном технологическом процессе, включая замену и модификацию их программных и (или) аппаратных частей.

7.8.10 Должна осуществляться и быть регламентирована процедура периодического контроля всех реализованных программно-техническими средствами функций (требований) по обеспечению ИБ платежной информации. Регламентирующие документы должны быть согласованы со службой либо лицом, отвечающим в организации БС за обеспечение ИБ.

7.8.11 Должны быть определены, выполняться и регистрироваться процедуры контроля отсутствия размещения на устройствах, задействованных в осуществлении банковского платежного технологического процесса, находящихся в общедоступных местах вне зоны постоянного контроля организации БС, в том числе банкоматов и платежных терминалов, специализированных средств, используемых для несанкционированного съема информации.

7.8.12 Должна осуществляться и быть регламентирована процедура восстановления всех реализованных программно-техническими средствами функций по обеспечению ИБ платежной информации. Регламентирующие документы должны быть согласованы со службой либо лицом, отвечающим в организации БС за обеспечение ИБ.

7.9 Общие требования по обеспечению информационной безопасности банковских информационных технологических процессов

7.9.1 В организации БС рекомендуется провести классификацию неплатежной информации.

Классификацию неплатежной информации следует проводить в соответствии со степенью тяжестипоследствий потери ее свойств ИБ, в частности свойств доступности, целостности и конфиденциальности.

7.9.2 Информационная безопасность банковских информационных технологических процессов должна обеспечиваться в соответствии с положениями настоящих Технических требований и правил.Для каждого из типов неплатежных информационных активов (типов неплатежной информации), полученных в результате классификации, должен быть документально определен набор требований по их защите.

7.9.3 Банковские информационные технологические процессы должны быть документированы в организации БС. Если технологический процесс реализован во вне АБС (не входит в состав АБС), то программно-технические средства его реализующие должны быть изолированы от АБС на сетевом уровне.

7.9.4 Должны быть документально определены перечни программного обеспечения, устанавливаемого и (или) используемого для выполнения банковских информационных технологических процессов.

7.9.5 Должна быть регламентирована и осуществляться процедура периодического контроля (с документированием результатов) всех реализованных мер по обеспечению защищенности неплатежной информации. Регламентирующие документы должны быть согласованы со службой ИБ.

7.9.6 Должны быть определены, выполняться и контролироваться требования по обеспечению ИБ в процессе взаимодействия АБС организации БС с информационными системами сторонних организаций (внешними информационными системами).

8 Проверка и оценка информационной безопасности организации БС

8.1 Проверка и оценка ИБ организации БС проводится путем выполнения следующих процессов:

– мониторинга ИБ и контроля защитных мер;

– самооценки ИБ;

– аудита ИБ;

– анализа функционирования СОИБ (в том числе со стороны руководства).

8.2 Основными целями мониторинга и контроля защитных мер в организации БС являются оперативное и постоянное наблюдение, сбор, анализ и обработка данных под заданные цели. Такими целями анализа могут быть:

– контроль реализации положений внутренних документов по обеспечению ИБ в организации БС;

– выявление нештатных, в том числе злоумышленных действий в АБС организации БС;

– выявление инцидентов ИБ.

Мониторинг и контроль защитных мер проводится персоналом организации БС, ответственным за ИБ.

8.3 При подготовке к внешнему аудиту ИБ рекомендуется проведение внутреннего аудита ИБ (самооценки). Внутренний аудит ИБ проводится собственными силами и по инициативе руководства организации БС.

Порядок проведения внутреннего аудита ИБ в организации БС определен требованиямиТТП ИБ 5.1.

В процессе внутреннего аудита ИБ проводятся оценка степени выполнения требований настоящих Технических требований и правил и на ее основе - вычисление итогового уровня ИБ организации БС. Порядок проведения указанной деятельности (оценка и вычисление) регламентируется ТТП ИБ 5.1.

8.4 Внешний аудит ИБ, проводимый внешними по отношению к организации БС независимыми проверяющими организациями, является одной из форм проверки и оценки (контроля) выполнения организацией БС требований настоящих Технических требований и правил.

Внешний аудит ИБ проводится как для собственных целей самой организации БС, так и с целью повышения доверия к ней со стороны других организаций.

Внешний аудит ИБ проводится в соответствии с требованиями ТТП ИБ 5.1.

В процессе внешнего аудита ИБ проводятся оценка степени выполнения требований настоящих Технических требований и правил и на ее основе - вычисление итогового уровня ИБ организации БС. Порядок проведения указанной деятельности (оценка и вычисление) регламентируется ТТП ИБ 5.1.

В качестве проверяющих организаций рекомендуется привлекать организации, имеющие квалификацию и опыт проведения оценки соответствия ИБ установленным требованиям.

8.5 Анализ функционирования СОИБ проводится персоналом организации БС, ответственным за обеспечение ИБ, а также руководством организации БС на основании подготовленных для руководства документов (данных).

Основными целями проведения анализа функционирования СОИБ является:

– оценка эффективности СОИБ;

– оценка соответствия СОИБ требованиям законодательства Республики Беларусь и ТНПА;

– оценка соответствия СОИБ существующим и возможным угрозам ИБ;

– оценка следования принципам ИБ и выполнения требований ИБ, закрепленных в политике ИБ организации БС, а также в иных внутренних документах организации БС.

Результаты, полученные в ходе анализа функционирования СОИБ, являются основой для совершенствования СОИБ.

Требования к проведению анализа функционирования СОИБ определены в ТТП ИБ 2.1.

8.6 Оценка соответствия ИБ в виде аудита ИБ или самооценки ИБ проводится организацией БС не реже одного раза в два года.

Библиография

[1] Банковский кодекс Республики Беларусь (в ред. Закона Республики Беларусь от 17.07.2018 № 133-З).

[2] Закон Республики Беларусь «Об информации, информатизации и защите информации» от 10 ноября 2008 г. № 455-З.

[3] Уголовный кодекс Республики Беларусь от 9 июля 1999 г. № 275-З.

[4] Положение о порядке технической и криптографической защиты информации в информационных системах, предназначенных для обработки информации, распространение и (или) предоставление которой ограничено (приказ Оперативно-аналитического центра при Президенте Республики Беларусь от 20.02.2020 № 66).

[5] Положение о лицензировании отдельных видов деятельности, утвержденное Указом Президента Республики Беларусь от 1 сентября 2010 г. № 450 «О лицензировании отдельных видов деятельности» (глава 21).