**СТАНДАРТ БАНКА АБХАЗИИ СТО БА ИББС-1.0-2009**

**ОБЕСПЕЧЕНИЕ**

**ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ**

**ОРГАНИЗАЦИЙ БАНКОВСКОЙ СИСТЕМЫ**

**РЕСПУБЛИКИ АБХАЗИЯ**

**ЛИСТ САМООЦЕНКИ**

Январь 2019

|  |  |  |  |
| --- | --- | --- | --- |
| **Информация об организации** | | | |
| Наименование организации: |  | | |
| ФИО контактного лица: |  | Должность: |  |
| Телефон: |  | e-mail: |  |
| Адрес: |  | | |

|  |  |  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| **Групповой показатель M1 «Обеспечение информационной безопасности при назначении и распределении ролей и обеспечении доверия к персоналу»** | | | | | | | | | | | | |
| Обозначение частного показателя ИБ | Частный показатель ИБ | | Обязательность выполнения | Оценка частного показателя ИБ | | | | | | | | Описание выполненной оценки |
|  |  | |  | документированность | | выполнение | | | | | |  |
|  |  | |  | да | нет | 0 | 0,25 | 0,5 | 0,75 | 1 | н/о |  |
| М1.1 | Определены ли в документах организации роли ее работников? | | обязательный |  |  |  |  |  |  |  |  |  |
| М1.2 | Формируются ли роли, связанные с выполнением деятельности по обеспечению ИБ, на основании требований разделов 7 и 8 стандарта СТО БА ИББС-1.0? | | обязательный |  |  |  |  |  |  |  |  |  |
| М1.3 | Персонифицированы ли роли в организации с установлением ответственности за их выполнение? | | обязательный |  |  |  |  |  |  |  |  |  |
| М1.4 | Зафиксирована ли документально в должностных инструкциях ответственность за выполнение ролей? | | обязательный |  |  |  |  |  |  |  |  |  |
| М1.5 | Отсутствуют ли в организации роли, совмещающие функции разработки и сопровождения системы/ПО? | | рекомендуемый |  |  |  |  |  |  |  |  |  |
| М1.6 | Отсутствуют ли в организации роли, совмещающие функции разработки и эксплуатации системы/ПО? | | рекомендуемый |  |  |  |  |  |  |  |  |  |
| М1.7 | Отсутствуют ли в организации роли, совмещающие функции сопровождения и эксплуатации? | | рекомендуемы |  |  |  |  |  |  |  |  |  |
| М1.8 | Отсутствуют ли в организации роли, совмещающие функции администратора системы и администратора информационной безопасности? | | рекомендуемый |  |  |  |  |  |  |  |  |  |
| М1.9 | Отсутствуют ли в организации роли, совмещающие функции по выполнению операций в системе и контроля их выполнения? | | рекомендуемый |  |  |  |  |  |  |  |  |  |
| М1.10 | Определены ли документально в организации и выполняются ли процедуры контроля деятельности работников, обладающих совокупностью полномочий (ролями), позволяющих получить контроль над защищаемым информационным активом организации? | | обязательный |  |  |  |  |  |  |  |  |  |
| М1.11 | Определены ли в документах организации процедуры приема на работу, влияющую на обеспечение ИБ, включающие:  - проверку подлинности предоставленных документов, заявляемой квалификации, точности и полноты биографических навыков;  - проверку в части профессиональных навыков и оценку профессиональной пригодности? | | обязательный |  |  |  |  |  |  |  |  |  |
| М1.12 | Предусматривают ли указанные в частном показателе М1.11 процедуры документальную фиксацию результатов проводимых проверок? | | обязательный |  |  |  |  |  |  |  |  |  |
| М1.13 | Определены ли в документах организации процедуры регулярной проверки в части профессиональных навыков и оценки профессиональной пригодности работников? | | рекомендуемый |  |  |  |  |  |  |  |  |  |
| М1.14 | Предусматривают ли указанные в частном показателе М1.13 процедуры документальную фиксацию результатов проводимых проверок? | | рекомендуемый |  |  |  |  |  |  |  |  |  |
| М1.15 | Определены ли в документах организации процедуры внеплановой проверки работников при выявлении фактов их нештатного поведения, участия в инцидентах ИБ или подозрений в таком поведении или участии? | | рекомендуемый |  |  |  |  |  |  |  |  |  |
| М1.16 | Предусматривают ли указанные в частном показателе М1.15 процедуры документальную фиксацию результатов проводимых проверок? | | рекомендуемый |  |  |  |  |  |  |  |  |  |
| М1.17 | Обязаны ли все работники организации давать письменные обязательства о соблюдении конфиденциальности, приверженности правилам корпоративной этики, включая требования по недопущению конфликта интересов? | | обязательный |  |  |  |  |  |  |  |  |  |
| М1.18 | Регламентируются ли положениями, включенными в договоры (соглашения с внешними организациями и клиентами, требования по ИБ? | | обязательный |  |  |  |  |  |  |  |  |  |
| М1.19 | Определены ли в трудовых контрактах (соглашениях, договорах) и (или) должностных инструкциях обязанности персонала по выполнению требований ИБ? | | обязательный |  |  |  |  |  |  |  |  |  |
| М1.20 | Приравнивается ли невыполнение работниками организации требований ИБ к невыполнению должностных обязанностей и приводит ли как минимум к дисциплинарной ответственности? | | обязательный |  |  |  |  |  |  |  |  |  |
| **Групповой показатель M2 «Обеспечение информационной безопасности автоматизированных банковских систем на стадиях жизненного цикла»** | | | | | | | | | | | | |
| Обозначение частного показателя ИБ | | Частный показатель ИБ | Обязательность выполнения | Оценка частного показателя ИБ | | | | | | | | Описание выполненной оценки |
|  | |  |  | документированность | | выполнение | | | | | |  |
|  | |  |  | да | нет | 0 | 0,25 | 0,5 | 0,75 | 1 | н/о |  |
| М2.1 | | Рассматриваются ли при формировании требований ИБ следующие стадии модели ЖЦ АБС:  — разработка технических заданий;  — проектирование;  — создание и тестирование;  — приемка и ввод в действие;  — эксплуатация;  — сопровождение и модернизации;  — снятие с эксплуатации? | рекомендуемый |  |  |  |  |  |  |  |  |  |
| М2.2 | | Осуществляются ли разработка технических заданий и приемка АБС по согласованию и при участии подразделения (лиц) в организации, ответственных за обеспечение ИБ? | обязательный |  |  |  |  |  |  |  |  |  |
| М2.3 | | Осуществляются ли ввод в действие, эксплуатация и сопровождение (модернизация), снятие с эксплуатации АБС под контролем подразделений (лиц) в организации, ответственных за обеспечение ИБ? | обязательный |  |  |  |  |  |  |  |  |  |
| М2.4 | | Имеют ли соответствующие лицензии организации, которые привлекаются на договорной основе для разработки и(или) производства средств и систем защиты АБС? | обязательный |  |  |  |  |  |  |  |  |  |
| М2.5 | | Снабжены ли разрабатываемые АБС и (или) их компоненты документацией содержащей описание реализованных защитных мер, в том числе в отношении угроз ИБ (источников угроз), описанных в модели угроз организации? | обязательный |  |  |  |  |  |  |  |  |  |
| М2.6 | | Снабжены ли приобретаемые организацией АБС и (или) их компоненты документацией, содержащей описание реализованных защитных мер, в том числе в отношении угроз ИБ (источников угроз), описанных в модели угроз организации? | рекомендуемый |  |  |  |  |  |  |  |  |  |
| М2.7 | | Содержит ли документация на разрабатываемые АБС или приобретаемые готовые АБС и их компоненты описание реализованных защитных мер, предпринятых разработчиком относительно безопасности разработки и безопасности поставки? | обязательный |  |  |  |  |  |  |  |  |  |
| М2.8 | | Реализуется ли при взаимодействии организации с разработчиком АБС и их компонентов одна из трех альтернатив:  1) в договор (контракт) о разработке АБС или поставке готовых АБС и их компонентов включаются положения по сопровождению поставляемых изделий на весь срок их службы;  2) организация приобретает полный комплект рабочей конструкторской документации, обеспечивающий возможность сопровождения АБС и их компонентов без участия разработчика;  3) руководство организации оценивает и документально оформляет допустимость риска нарушения ИБ, возникающего при невозможности сопровождения АБС и их компонентов? | обязательный |  |  |  |  |  |  |  |  |  |
| М2.9 | | Учитывается ли при разработке технических заданий на системы дистанционного банковского обслуживания, 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? | обязательный |  |  |  |  |  |  |  |  |  |
| М2.10 | | Обеспечиваются ли на стадии тестирования анонимность данных и проверка адекватности разграничения доступа? | обязательный |  |  |  |  |  |  |  |  |  |
| М2.11 | | Определены ли в документах организации и выполняются ли на стадии эксплуатации АБС процедуры контроля работоспособности (функционирования, эффективности) реализованных в АБС защитных мер? | обязательный |  |  |  |  |  |  |  |  |  |
| М2.12 | | Предусматривают ли указанные в частном показателе М2.11 процедуры документальную фиксацию результатов контроля? | обязательный |  |  |  |  |  |  |  |  |  |
| М2.13 | | Определены ли в документах организации и выполняются ли на стадии сопровождения (модернизации) АБС процедуры контроля, обеспечивающие защиту от:  — умышленного несанкционированного раскрытия, модификации или уничтожения информации;  — неумышленной модификации, раскрытия или уничтожения информации;  — отказа в обслуживании или ухудшения обслуживания? | обязательный |  |  |  |  |  |  |  |  |  |
| М2.14 | | Предусматривают ли указанные в частном показателе М2.13 процедуры документальную фиксацию результатов контроля? | обязательный |  |  |  |  |  |  |  |  |  |
| М2.15 | | Проводятся ли на стадии сопровождения (модернизации) при любом внесении изменений в АБС процедуры проверки функциональности, результаты которых документируются? | обязательный |  |  |  |  |  |  |  |  |  |
| М2.16 | | Определены ли документально и выполняются ли на стадии снятия с эксплуатации процедуры, обеспечивающие удаление информации, несанкционированное использование которой может нанести ущерб бизнес-деятельности организации, 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 предусмотрены соответствующими нормативными и(или) договорными документами)? | обязательный |  |  |  |  |  |  |  |  |  |
| М2.17 | | Предусматривают ли указанные в частном показателе М2.16 процедуры документальную фиксацию результатов их выполнения? | обязательный |  |  |  |  |  |  |  |  |  |
| **Групповой показатель M3 "Обеспечение информационной безопасности при управлении доступом и регистрации"** | | | | | | | | | | | | |
| Обозначение частного показателя ИБ | | Частный показатель ИБ | Обязательность выполнения | Оценка частного показателя ИБ | | | | | | | | Описание выполненной оценки |
|  | |  |  | документированность | | выполнение | | | | | |  |
|  | |  |  | Да | Нет | 0 | 0,25 | 0,5 | 0,75 | 1 | н/о |  |
| М3.1 | | Определен ли в документах организации перечень информационных активов (их типов)? | обязательный |  |  |  |  |  |  |  |  |  |
| М3.2 | | Зафиксированы ли документально права доступа работников и клиентов к информационным активам организации? | обязательный |  |  |  |  |  |  |  |  |  |
| М3.3 | | Применяются ли в составе АБС встроенные защитные меры? | обязательный |  |  |  |  |  |  |  |  |  |
| М3.4 | | Применяются ли в составе АБС сертифицированные или разрешенные к применению руководством организации средства защиты информации от НСД и НРД и средства криптографической защиты информации? | рекомендуемый |  |  |  |  |  |  |  |  |  |
| М3.5 | | Определены ли в документах организации, утверждены ли руководством организации, выполняются ли и контролируются ли процедуры идентификации, аутентификации и авторизации? | обязательный |  |  |  |  |  |  |  |  |  |
| М3.6 | | Документируются ли результаты контроля процедур, указанных в частном показателе М3.5? | обязательный |  |  |  |  |  |  |  |  |  |
| М3.7 | | Определены ли в документах организации, выполняются ли и контролируются ли процедуры управления доступом? | обязательный |  |  |  |  |  |  |  |  |  |
| М3.8 | | Документируются ли результаты контроля процедур, указанных в частном показателе М3.7? | обязательный |  |  |  |  |  |  |  |  |  |
| М3.9 | | Определены ли в документах организации, выполняются ли и контролируются ли процедуры контроля целостности? | обязательный |  |  |  |  |  |  |  |  |  |
| М3.10 | | Документируются ли результаты контроля процедур, указанных в частном показателе М3.9? | обязательный |  |  |  |  |  |  |  |  |  |
| М3.11 | | Определены ли в документах организации, выполняются ли и контролируются ли процедуры регистрации событий и действий? | обязательный |  |  |  |  |  |  |  |  |  |
| М3.12 | | Документируются ли результаты контроля процедур, указанных в частном показателе М3.11? | обязательный |  |  |  |  |  |  |  |  |  |
| М3.13 | | Исключают ли процедуры управления доступом возможность "самосанкционирования"? | обязательный |  |  |  |  |  |  |  |  |  |
| М3.14 | | Определены ли в документах организации процедуры мониторинга и анализа данных регистрации, действий и операций, позволяющие выявить неправомерные или подозрительные операции и транзакции? | обязательный |  |  |  |  |  |  |  |  |  |
| М3.15 | | Используются ли специализированные программные и(или) технические средства для проведения процедур мониторинга и анализа данных регистрации, действий и операций? | рекомендуемый |  |  |  |  |  |  |  |  |  |
| М3.16 | | Используют ли процедуры мониторинга и анализа документально определенные критерии выявления неправомерных или подозрительных действий и операций? | обязательный |  |  |  |  |  |  |  |  |  |
| М3.17 | | Применяются ли процедуры мониторинга и анализа на регулярной основ (например, ежедневно) ко всем выполненным операциям и транзакциям | обязательный |  |  |  |  |  |  |  |  |  |
| М3.18 | | Регламентирован ли во внутренних документах организации порядок доступа работников организации в помещения, в которых размещаются объекты среды информационных активов? | обязательный |  |  |  |  |  |  |  |  |  |
| М3.19 | | Контролируется ли выполнение порядка доступа работников организации в помещения, в которых размещаются объекты среды информационных активов? | обязательный |  |  |  |  |  |  |  |  |  |
| М3.20 | | Оформляются ли документально результаты выполнения контроля порядка доступа работников организации в помещения, в которых размещаются объекты среды информационных активов? | обязательный |  |  |  |  |  |  |  |  |  |
| М3.21 | | Обеспечивают ли используемые в организации АБС, в том числе системы дистанционного банковского обслуживания, 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? | обязательный |  |  |  |  |  |  |  |  |  |
| М3.22 | | Реализованы ли в системах дистанционного банковского обслуживания, используемых в организации, защитные меры, обеспечивающие невозможность отказа от авторства проводимых клиентами операций и транзакций (например, ЭЦП)? | обязательный |  |  |  |  |  |  |  |  |  |
| М3.23 | | Придано ли протоколам операций, выполняемых посредством дистанционного банковского обслуживания, свойство юридической значимости, например, путем внесения соответствующих положений в договоры на дистанционное банковское обслуживание? | рекомендуемый |  |  |  |  |  |  |  |  |  |
| М3.24 | | Производится ли при заключении договоров со сторонними организациями юридическое оформление договоренностей, определяющих необходимый уровень взаимодействия в случае выхода инцидента ИБ за рамки отдельной организации? | рекомендуемый |  |  |  |  |  |  |  |  |  |
| М3.25 | | Определены ли в документах организации процедуры, определяющие действия работников и клиентов организации 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? | обязательный |  |  |  |  |  |  |  |  |  |
| М3.26 | | Доведены ли до сведения работников и клиентов организации процедуры, указанные в частном показателе М3.25? | обязательный |  |  |  |  |  |  |  |  |  |
| М3.27 | | Предусматривают ли указанные в частном показателе М3.26 процедуры документирование работниками и клиентами своих действий и их результатов? | обязательный |  |  |  |  |  |  |  |  |  |
| М3.28 | | Реализованы ли в системах дистанционного банковского обслуживания механизмы информирования (регулярного, непрерывного или по требованию) клиентов обо всех операциях, совершаемых от их имени? | обязательный |  |  |  |  |  |  |  |  |  |
| М3.29 | | Применяются ли в организации защитные меры, направленные на обеспечение защиты от НСД и НРД, повреждения или нарушения целостности информации, необходимой для регистрации, идентификации, аутентификации и(или) авторизации клиентов и работников организации? | обязательный |  |  |  |  |  |  |  |  |  |
| М3.30 | | Регистрируются ли все попытки НСД и НРД к информации, необходимой для идентификации, аутентификации и(или) авторизации клиентов и сотрудников организации? | обязательный |  |  |  |  |  |  |  |  |  |
| М3.31 | | Определена ли в документах организации и выполняется ли процедура пересмотра прав доступа при увольнении или изменении должностных обязанностей работников организации, имевших доступ к информации, необходимой для идентификации, аутентификации и(или) авторизации клиентов и сотрудников организации? | обязательный |  |  |  |  |  |  |  |  |  |
| М3.32 | | Осуществляется ли работа всех пользователей АБС под уникальными учетными записями? | обязательный |  |  |  |  |  |  |  |  |  |
| **Групповой показатель M4 "Обеспечение информационной безопасности средствами антивирусной защиты"** | | | | | | | | | | | | |
| Обозначение частного показателя ИБ | | Частный показатель ИБ | Обязательность выполнения | Оценка частного показателя ИБ | | | | | | | | Описание выполненной оценки |
|  | |  |  | документированность | | выполнение | | | | | |  |
|  | |  |  | Да | Нет | 0 | 0,25 | 0,5 | 0,75 | 1 | н/о |  |
| М4.1 | | Применяются ли на всех автоматизированных рабочих местах и серверах АБС организации, если иное не предусмотрено технологическим процессом, средства антивирусной защиты? | обязательный |  |  |  |  |  |  |  |  |  |
| М4.2 | | Определены ли в документах организации процедуры установки и регулярного обновления средств антивирусной защиты (версий и баз данных) на автоматизированных рабочих местах и серверах АБС? | обязательный |  |  |  |  |  |  |  |  |  |
| М4.3 | | Осуществляются ли установка и регулярное обновление средств антивирусной защиты (версий и баз данных) на автоматизированных рабочих местах и серверах АБС администраторами АБС или иными официально уполномоченными лицами? | обязательный |  |  |  |  |  |  |  |  |  |
| М4.4 | | Организован ли автоматический режим установки обновлений антивирусного программного обеспечения и его баз данных? | рекомендуемый |  |  |  |  |  |  |  |  |  |
| М4.5 | | Контролируются ли установка и обновление антивирусных средств представителями подразделения (лицами) в организации, ответственными за обеспечение ИБ? | обязательный |  |  |  |  |  |  |  |  |  |
| М4.6 | | Организовано ли функционирование постоянной антивирусной защиты в автоматическом режиме? | рекомендуемый |  |  |  |  |  |  |  |  |  |
| М4.7 | | Разработаны и введены ли в действие инструкции по антивирусной защите, учитывающие особенности банковских технологических процессов? | обязательный |  |  |  |  |  |  |  |  |  |
| М4.8 | | Проводится ли антивирусная фильтрация всего трафика электронного почтового обмена? | обязательный |  |  |  |  |  |  |  |  |  |
| М4.9 | | Построена ли в организации эшелонированная централизованная система антивирусной защиты, предусматривающая использование средств антивирусной защиты различных производителей и их раздельную установку на рабочих станциях, почтовых серверах и межсетевых экранах? | рекомендуемый |  |  |  |  |  |  |  |  |  |
| М4.10 | | Определены ли в документах организации и выполняются ли процедуры предварительной проверки устанавливаемого или изменяемого программного обеспечения на отсутствие вирусов? | обязательный |  |  |  |  |  |  |  |  |  |
| М4.11 | | Проводится ли антивирусная проверка после установки и изменения программного обеспечения? | обязательный |  |  |  |  |  |  |  |  |  |
| М4.12 | | Документируются ли результаты установки, изменения программного обеспечения и антивирусной проверки? | обязательный |  |  |  |  |  |  |  |  |  |
| М4.13 | | Определены ли в документах организации процедуры, выполняемые в случае обнаружения компьютерных вирусов, в которых зафиксированы:  - необходимые меры по отражению и устранению последствий вирусной атаки;  - порядок официального информирования руководства;  - порядок приостановления при необходимости работы (на период устранения последствий вирусной атаки)? | обязательный |  |  |  |  |  |  |  |  |  |
| М4.14 | | Определены ли в документах организации и выполняются ли процедуры контроля за отключением и обновлением антивирусных средств на всех автоматизированных рабочих местах и серверах АБС? | обязательный |  |  |  |  |  |  |  |  |  |
| М4.15 | | Предусматривают ли указанные в частном показателе М4.14 процедуры документальную фиксацию результатов контроля? | обязательный |  |  |  |  |  |  |  |  |  |
| М4.16 | | Возложена ли обязанность по выполнению предписанных мер антивирусной защиты на каждого работника организации, имеющего доступ к ЭВМ и(или) АБС, а ответственность за выполнение требований инструкции по антивирусной защите - на руководителей функциональных подразделений организации? | обязательный |  |  |  |  |  |  |  |  |  |
| **Групповой показатель M5 "Обеспечение информационной безопасности при использовании ресурсов сети Интернет"** | | | | | | | | | | | | |
| Обозначение частного показателя ИБ | | Частный показатель ИБ | Обязательность выполнения | Оценка частного показателя ИБ | | | | | | | | Описание выполненной оценки |
|  | |  |  | документированность | | выполнение | | | | | |  |
|  | |  |  | Да | Нет | 0 | 0,25 | 0,5 | 0,75 | 1 | н/о |  |
| М5.1 | | Принято ли документально руководством организации решение об использовании сети Интернет для производственной и(или) собственной хозяйственной деятельности, в котором явно перечислены цели использования сети Интернет? | обязательный |  |  |  |  |  |  |  |  |  |
| М5.2 | | Запрещается ли использование ресурсов сети Интернет в неустановленных целях? | обязательный |  |  |  |  |  |  |  |  |  |
| М5.3 | | Проведено ли в организации выделение ограниченного числа пакетов, содержащих перечень сервисов и ресурсов сети Интернет, доступных для пользователей? | рекомендуемый |  |  |  |  |  |  |  |  |  |
| М5.4 | | Проводится ли наделение работников организации правами пользователя конкретного пакета в соответствии с его должностными обязанностями, в частности, в соответствии с назначенными ему ролями? | рекомендуемый |  |  |  |  |  |  |  |  |  |
| М5.5 | | Оформляется ли документально наделение работников организации правами пользователя конкретного пакета? | рекомендуемый |  |  |  |  |  |  |  |  |  |
| М5.6 | | Определен ли документально в организации порядок подключения и использования ресурсов сети Интернет, включающий, в том числе положение о контроле со стороны подразделения (лиц) в организации, ответственных за обеспечение ИБ? | обязательный |  |  |  |  |  |  |  |  |  |
| М5.7 | | Применяются ли при осуществлении дистанционного банковского обслуживания с использованием сети Интернет средства защиты информации (межсетевые экраны, антивирусные средства, средства криптографической защиты информации), которые обеспечивают прием и передачу информации только в установленном формате и только по конкретной технологии? | обязательный |  |  |  |  |  |  |  |  |  |
| М5.8 | | Выполнено ли выделение и организована ли физическая изоляция от внутренних сетей тех ЭВМ, с помощью которых осуществляется взаимодействие с сетью Интернет в режиме on-line? | рекомендуемый |  |  |  |  |  |  |  |  |  |
| М5.9 | | Применяются ли при осуществлении дистанционного банковского обслуживания защитные меры, предотвращающие возможность подмены авторизованного клиента злоумышленником в рамках сеанса работы? | обязательный |  |  |  |  |  |  |  |  |  |
| М5.10 | | Регистрируются ли регламентированным образом попытки подмены авторизованного клиента злоумышленником в рамках сеанса работы? | обязательный |  |  |  |  |  |  |  |  |  |
| М5.11 | | Все ли операции клиентов в течение сеанса работы с системами дистанционного банковского обслуживания выполняются только после проведения процедур идентификации, аутентификации и авторизации? | обязательный |  |  |  |  |  |  |  |  |  |
| М5.12 | | Обеспечивается ли повторное выполнение процедур идентификации, аутентификации и авторизации в случаях нарушения или разрыва соединения при работе с системами дистанционного банковского обслуживания? | обязательный |  |  |  |  |  |  |  |  |  |
| М5.13 | | Используется ли специализированное клиентское программное обеспечение для доступа пользователей к системам дистанционного банковского обслуживания? | рекомендуемый |  |  |  |  |  |  |  |  |  |
| М5.14 | | Применяются ли защитные меры для осуществления почтового обмена через сеть Интернет? | обязательный |  |  |  |  |  |  |  |  |  |
| М5.15 | | Определены ли в документах организации перечень защитных мер и порядок их использования для осуществления почтового обмена через сеть Интернет? | обязательный |  |  |  |  |  |  |  |  |  |
| М5.16 | | Организован ли почтовый обмен с сетью Интернет через ограниченное количество точек, состоящих из внешнего (подключенного к сети Интернет) и внутреннего (подключенного к внутренним сетям организации) почтовых серверов с безопасной системой репликации почтовых сообщений между ними (интернет-киоски)? | рекомендуемый |  |  |  |  |  |  |  |  |  |
| М5.17 | | Осуществляется ли архивирование электронной почты? | обязательный |  |  |  |  |  |  |  |  |  |
| М5.18 | | Доступен ли архив электронной почты подразделению (лицу), ответственном за обеспечение ИБ? | обязательный |  |  |  |  |  |  |  |  |  |
| М5.19 | | Не допускаются ли изменения в архиве электронной почты? | обязательный |  |  |  |  |  |  |  |  |  |
| М5.20 | | Определен ли документально порядок доступа к информации архива электронной почты? | обязательный |  |  |  |  |  |  |  |  |  |
| М5.21 | | Не применяется ли в организации практика хранения и обработки банковской информации (в т.ч. открытой) на ЭВМ, с помощью которой осуществляется взаимодействие с сетью Интернет в режиме on-line? | рекомендуемый |  |  |  |  |  |  |  |  |  |
| М5.22 | | Всегда ли наличие банковской информации на ЭВМ, с помощью которых осуществляется взаимодействие с сетью Интернет в режиме on-line, определяется бизнес-целями организации и документально санкционируется ее руководством? | обязательный |  |  |  |  |  |  |  |  |  |
| М5.23 | | Определены ли документально и используются ли защитные меры, позволяющие обеспечить противодействие атакам хакеров и распространению спама? | обязательный |  |  |  |  |  |  |  |  |  |
| **Групповой показатель M6 «Обеспечение информационной безопасности при использовании средств криптографической защиты информации»** | | | | | | | | | | | | |
| Обозначение частного показателя ИБ | | Частный показатель ИБ | Обязательность выполнения | Оценка частного показателя ИБ | | | | | | | | Описание выполненной оценки |
|  | |  |  | документированность | | выполнение | | | | | |  |
|  | |  |  | Да | Нет | 0 | 0,25 | 0,5 | 0,75 | 1 | н/о |  |
| М6.1 | | Проводится ли применение СKЗИ в АБС в соответствии с моделью нарушителя, принятой в организации, с целью защиты информации при ее обработке хранении и передаче по каналам связи? | обязательный |  |  |  |  |  |  |  |  |  |
| М6.2 | | Утверждена ли политика (концепция) применения СKЗИ в организации? | рекомендуемый |  |  |  |  |  |  |  |  |  |
| М6.3 | | Допускают ли СKЗИ возможность встраивания в технологическую схему обработки электронных сообщений? | обязательный |  |  |  |  |  |  |  |  |  |
| М6.4 | | Обеспечивают ли СKЗИ взаимодействие с прикладным программным обеспечением на уровне обработки запросов на криптографические преобразования и выдачи результатов? | обязательный |  |  |  |  |  |  |  |  |  |
| М6.5 | | Поставляются ли СKЗИ разработчиками с полным комплектом эксплуатационной документации, включающей описание ключевой системы, правила работы с ней и обоснование необходимого организационно-штатного обеспечения? | обязательный |  |  |  |  |  |  |  |  |  |
| М6.6 | | Выполняется ли как минимум одна из трех альтернатив  - сертифицированы ли СKЗИ уполномоченным государственным органом; - реализованы ли СKЗИ на основе рекомендованных уполномоченным государственным органом алгоритмов либо алгоритмов, определенных условиями договора с контрагентом (клиентом) организации;  - соответствуют ли СKЗИ стандартам организации, взаимодействующей с проверяемой организацией? | обязательный |  |  |  |  |  |  |  |  |  |
| М6.7 | | Поддерживается ли непрерывность процессов протоколирования работы СKЗИ при применении СKЗИ в АБС? | обязательный |  |  |  |  |  |  |  |  |  |
| М6.8 | | Поддерживается ли непрерывность процессов обеспечения целостности программного обеспечения для всех звеньев АБС, взаимодействующих со СKЗИ? | обязательный |  |  |  |  |  |  |  |  |  |
| М6.9 | | Обеспечивается ли ИБ процессов изготовления ключевых документов СKЗИ комплексом технологических, организационных, технических и программных мер и средств защиты? | обязательный |  |  |  |  |  |  |  |  |  |
| М6. 10 | | Реализованы ли процедуры мониторинга, предусматривающие регистрацию всех значимых событий, состоявшихся в процессе обмена электронными сообщениями, и всех инцидентов ИБ? | рекомендуемый |  |  |  |  |  |  |  |  |  |
| М6. 11 | | Определен ли руководством порядок применения СKЗИ в АБС, включающий  - порядок ввода в действие, включая процедуры встраивания СKЗИ 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? | обязательный |  |  |  |  |  |  |  |  |  |
| М6. 12 | | Самостоятельно ли изготавливаются в организации и(или) физическим лицом ключи ЭЦП и(или) иных СKЗИ? | обязательный |  |  |  |  |  |  |  |  |  |
| М6. 13 | | Отражены ли в соответствующих договорах правовые и организационные последствия изготовления ключей СKЗИ для одной организации в другой организации? | обязательный |  |  |  |  |  |  |  |  |  |
| **Групповой показатель M7 «Обеспечение информационной безопасности банковских платежных технологических процессов»** | | | | | | | | | | | | |
| Обозначение частного показателя ИБ | | Частный показатель ИБ | Обязательность выполнения | Оценка частного показателя ИБ | | | | | | | | Описание выполненной оценки |
|  | |  |  | документированность | | выполнение | | | | | |  |
|  | |  |  | Да | Нет | 0 | 0,25 | 0,5 | 0,75 | 1 | н/о |  |
| М7.1 | | Определен ли в документах организации банковский платежный технологический процесс? | обязательный |  |  |  |  |  |  |  |  |  |
| М7.2 | | Определены ли документально перечни программного обеспечения, устанавливаемого и(или) используемого в ЭВМ и АБС и необходимого для выполнения конкретных банковских платежных технологических процессов? | обязательный |  |  |  |  |  |  |  |  |  |
| М7.3 | | Соответствует ли состав установленного и используемого в ЭВМ и АБС программного обеспечения определенному перечню? | обязательный |  |  |  |  |  |  |  |  |  |
| М7.4 | | Контролируется ли выполнение требований, оцениваемых в частных показателях М7.2, М7.3 с документированием результатов контроля? | обязательный |  |  |  |  |  |  |  |  |  |
| М7.5 | | Зафиксирован ли порядок обмена платежной информацией в договорах между участниками данного обмена? | обязательный |  |  |  |  |  |  |  |  |  |
| М7.6 | | Отсутствуют ли в организации работники, обладающие полномочиями для бесконтрольного создания, авторизации, уничтожения и изменения платежной информации, а также проведения несанкционированных операций по изменению состояния банковских счетов? | обязательный |  |  |  |  |  |  |  |  |  |
| М7.7 | | Контролируются (проверяются) ли и удостоверяются ли результаты технологических операций по обработке платежной информации лицами/автоматизированными процессами? | обязательный |  |  |  |  |  |  |  |  |  |
| М7.8 | | Осуществляются ли обработка платежной информации и контроль (проверка) результатов обработки разными работниками / автоматизированными процессами? | рекомендуемый |  |  |  |  |  |  |  |  |  |
| М7.9 | | Возложены ли обязанности по администрированию средств защиты платежной информации приказами или распоряжениями по организации на администраторов ИБ с отражением этих обязанностей в должностных инструкциях? | рекомендуемый |  |  |  |  |  |  |  |  |  |
| М7.10 | | Предусматривает ли комплекс мер по обеспечению ИБ банковского платежного технологического процесса защиту платежной информации от искажения, фальсификации, переадресации, несанкционированного уничтожения, ложной авторизации электронных платежных сообщений? | обязательный |  |  |  |  |  |  |  |  |  |
| М7.11 | | Предусматривает ли комплекс мер по обеспечению ИБ банковского платежного технологического процесса доступ работника организации только к тем ресурсам банковского платежного технологического процесса, которые необходимы ему для исполнения должностных обязанностей или реализации прав, предусмотренных технологией обработки платежной информации? | обязательный |  |  |  |  |  |  |  |  |  |
| М7.12 | | Предусматривает ли комплекс мер по обеспечению ИБ банковского платежного технологического процесса контроль (мониторинг) исполнения установленной технологии подготовки, обработки, передачи и хранения платежной информации? | обязательный |  |  |  |  |  |  |  |  |  |
| М7.13 | | Предусматривает ли комплекс мер по обеспечению ИБ банковского платежного технологического процесса аутентификацию входящих электронных платежных сообщений? | обязательный |  |  |  |  |  |  |  |  |  |
| М7.14 | | Предусматривает ли комплекс мер по обеспечению ИБ банковского платежного технологического процесса двустороннюю аутентификацию автоматизированных рабочих мест (рабочих станций и серверов), участников обмена электронными платежными сообщениями? | обязательный |  |  |  |  |  |  |  |  |  |
| М7.15 | | Предусматривает ли комплекс мер по обеспечению ИБ банковского платежного технологического процесса возможность ввода платежной информации в АБС только для авторизованных пользователей? | обязательный |  |  |  |  |  |  |  |  |  |
| М7.16 | | Предусматривает ли комплекс мер по обеспечению ИБ банковского платежного технологического процесса контроль, направленный на исключение возможности совершения злоумышленных действий (двойной ввод, сверка, установление ограничений в зависимости от суммы совершения операций и т.д.)? | обязательный |  |  |  |  |  |  |  |  |  |
| М7.17 | | Предусматривает ли комплекс мер по обеспечению ИБ банковского платежного технологического процесса восстановление платежной информации в случае ее умышленного (случайного) разрушения (искажения) или выхода из строя средств вычислительной техники? | обязательный |  |  |  |  |  |  |  |  |  |
| М7.18 | | Предусматривает ли комплекс мер по обеспечению ИБ банковского платежного технологического процесса при осуществлении межбанковских расчетов сверку выходных электронных платежных сообщений с соответствующими входными и обработанными электронными платежными сообщениями? | обязательный |  |  |  |  |  |  |  |  |  |
| М7.19 | | Предусматривает ли комплекс мер по обеспечению ИБ банковского платежного технологического процесса доставку электронных платежных сообщений участникам обмена? | обязательный |  |  |  |  |  |  |  |  |  |
| М7.20 | | Организован ли в организации авторизованный ввод платежной информации в АБС двумя работниками с последующей программной сверкой результатов ввода на совпадение (принцип "двойного управления")? | рекомендуемый |  |  |  |  |  |  |  |  |  |
| М7.21 | | Определены ли в документах организации и выполняются ли при проектировании, разработке, эксплуатации систем дистанционного банковского обслуживания процедуры, реализующие 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? | обязательный |  |  |  |  |  |  |  |  |  |
| М7.22 | | Обеспечены ли клиенты систем дистанционного банковского обслуживания детальными инструкциями, описывающими процедуры выполнения операций или транзакций? | обязательный |  |  |  |  |  |  |  |  |  |
| М7.23 | | Определены ли в документах организации и выполняются ли процедуры обслуживания средств вычислительной техники, используемых в банковском платежном технологическом процессе, включая замену их программных и(или) аппаратных частей? | обязательный |  |  |  |  |  |  |  |  |  |
| М7.24 | | Определена ли в документах организации, согласована ли со службой либо лицом, отвечающим в организации за обеспечение ИБ, и выполняется ли процедура периодического контроля всех реализованных программно-техническими средствами функций (требований) по обеспечению ИБ платежной информации? | обязательный |  |  |  |  |  |  |  |  |  |
| М7.25 | | Определена ли в документах организации, согласована ли со службой либо лицом, отвечающим в организации за обеспечение ИБ, и выполняется ли процедура восстановления всех реализованных программно-техническими средствами функций по обеспечению ИБ платежной информации? | обязательный |  |  |  |  |  |  |  |  |  |
| **Групповой показатель M8 "Обеспечение информационной безопасности банковских информационных технологических процессов"** | | | | | | | | | | | | |
| Обозначение частного показателя ИБ | | Частный показатель ИБ | Обязательность выполнения | Оценка частного показателя ИБ | | | | | | | | Описание выполненной оценки |
|  | |  |  | документированность | | выполнение | | | | | |  |
|  | |  |  | Да | Нет | 0 | 0,25 | 0,5 | 0,75 | 1 | н/о |  |
| М8.1 | | Проведена ли в организации классификация неплатежной информации? | рекомендуемы |  |  |  |  |  |  |  |  |  |
| М8.2 | | Проводится ли классификация неплатежной информации в соответствии со степенью тяжести последствий потери ее свойств ИБ, в частности свойств доступности, целостности и конфиденциальности? | рекомендуемый |  |  |  |  |  |  |  |  |  |
| М8.3 | | Определен ли документально набор требований по защите каждого из типов неплатежных информационных активов (типов неплатежной информации), полученных в результате классификации? | обязательный |  |  |  |  |  |  |  |  |  |
| М8.4 | | Возложены ли обязанности по администрированию средств защиты неплатежной информации приказами или распоряжениями по организации на администраторов ИБ с отражением этих обязанностей в должностных инструкциях? | рекомендуемый |  |  |  |  |  |  |  |  |  |
| М8.5 | | Определен ли документально порядок контроля функционирования со стороны лиц, отвечающих за ИБ, для каждой АБС организации? | обязательный |  |  |  |  |  |  |  |  |  |
| М8.6 | | Определены ли в документах организации банковские информационные технологические процессы, согласованы ли эти документы со службой ИБ организации? | обязательный |  |  |  |  |  |  |  |  |  |
| М8.7 | | Реализованы ли банковские информационные технологические процессы в рамках созданных для этих целей АБС? | обязательный |  |  |  |  |  |  |  |  |  |
| М8.8 | | Изолированы ли серверы, офисные ЭВМ и другое оборудование, не входящее в состав АБС, реализующих банковские информационные технологические процессы, от указанных АБС на уровне локальных вычислительных сетей способом, согласованным со службой либо лицом, отвечающим в организации за ИБ? | рекомендуемый |  |  |  |  |  |  |  |  |  |
| М8.9 | | Определены ли документально перечни программного обеспечения, устанавливаемого и(или) используемого в ЭВМ и АБС и необходимого для выполнения конкретных банковских информационных технологических процессов? | обязательный |  |  |  |  |  |  |  |  |  |
| М8.10 | | Соответствует ли состав установленного и используемого в ЭВМ и АБС программного обеспечения определенному перечню? | обязательный |  |  |  |  |  |  |  |  |  |
| М8.11 | | Контролируется ли выполнение требований частных показателей М8.9, М8.1 с документированием результатов контроля? | обязательный |  |  |  |  |  |  |  |  |  |
| М8.12 | | Регламентирована ли в документах организации, согласована ли со службой ИБ либо лицом, отвечающим за обеспечение ИБ, и выполняется ли процедура периодического контроля всех реализованных программно-техническими средствами и организационными мерами функций (требований) по обеспечению ИБ неплатежной информации? | обязательный |  |  |  |  |  |  |  |  |  |
| М8.13 | | Регламентирована ли в документах организации, согласована ли со службой ИБ либо лицом, отвечающим за обеспечение ИБ, и выполняется ли процедура восстановления всех реализованных программно-техническими средствами и организационными мерами функций по обеспечению ИБ неплатежной информации? | обязательный |  |  |  |  |  |  |  |  |  |
| **Групповой показатель M9 "Организация и функционирование службы ИБ организации БС РА"** | | | | | | | | | | | | |
| Обозначение частного показателя ИБ | | Частный показатель ИБ | Обязательность выполнения | Оценка частного показателя ИБ | | | | | | | | Описание выполненной оценки |
|  | |  |  | документированность | | выполнение | | | | | |  |
|  | |  |  | Да | Нет | 0 | 0,25 | 0,5 | 0,75 | 1 | н/о |  |
| М9.1 | | Сформирована ли руководством служба ИБ (назначено ли уполномоченное лицо) для реализации, эксплуатации, контроля и поддержания на должном уровне СОИБ, утверждены ли цели и задачи ее деятельности? | обязательный |  |  |  |  |  |  |  |  |  |
| М9.2 | | Имеет ли служба ИБ утвержденные руководством полномочия и ресурсы, необходимые для выполнения установленных целей и задач? | обязательный |  |  |  |  |  |  |  |  |  |
| М9.3 | | Имеет ли служба ИБ назначенного из числа руководства куратора, который при этом не является куратором службы информатизации (автоматизации)? | обязательный |  |  |  |  |  |  |  |  |  |
| М?9.4 | | Наделена ли служба ИБ собственным бюджетом? | рекомендуемый |  |  |  |  |  |  |  |  |  |
| М9.5 | | Сформированы ли для организаций, имеющих сеть филиалов или региональных представительств, подразделения ИБ (уполномоченные лица) на местах и обеспечены ли эти подразделения необходимыми ресурсами и нормативной базой? | рекомендуемый |  |  |  |  |  |  |  |  |  |
| М9.6 | | Наделена ли служба ИБ (уполномоченное лицо) полномочиями организовывать составление и контролировать выполнение всех планов по обеспечению ИБ организации? | обязательный |  |  |  |  |  |  |  |  |  |
| М9.7 | | Наделена ли служба ИБ (уполномоченное лицо) полномочиями разрабатывать и вносить предложения по изменению политик ИБ организации? | обязательный |  |  |  |  |  |  |  |  |  |
| М9.8 | | Наделена ли служба ИБ (уполномоченное лицо) полномочиями организовывать изменения существующих и принятие руководством новых внутренних документов, регламентирующих деятельность по обеспечению ИБ организации? | обязательный |  |  |  |  |  |  |  |  |  |
| М9.9 | | Наделена ли служба ИБ (уполномоченное лицо) полномочиями определять требования к мерам обеспечения ИБ организации? | обязательный |  |  |  |  |  |  |  |  |  |
| М9.10 | | Наделена ли служба ИБ (уполномоченное лицо) полномочиями контролировать работников организации в части выполнения ими требований внутренних документов, регламентирующих деятельность в области обеспечения ИБ, в первую очередь работников, имеющих максимальные полномочия по доступу к защищаемым информационным активам? | обязательный |  |  |  |  |  |  |  |  |  |
| М9.11 | | Наделена ли служба ИБ (уполномоченное лицо) полномочиями осуществлять мониторинг событий, связанных с обеспечением ИБ? | обязательный |  |  |  |  |  |  |  |  |  |
| М9.12 | | Наделена ли служба ИБ (уполномоченное лицо) полномочиями участвовать в расследовании событий, связанных с инцидентами ИБ, и выходить в случае необходимости с предложениями по применению санкций в отношении лиц, осуществивших НСД и НРД (например, нарушивших требования инструкций, руководств по обеспечению ИБ организации)? | обязательный |  |  |  |  |  |  |  |  |  |
| М9.13 | | Наделена ли служба ИБ (уполномоченное лицо) полномочиями участвовать в действиях по восстановлению работоспособности АБС после сбоев и аварий? | обязательный |  |  |  |  |  |  |  |  |  |
| М9.14 | | Наделена ли служба ИБ (уполномоченное лицо) полномочиями участвовать в создании, поддержании, эксплуатации и совершенствовании СОИБ организации? | обязательный |  |  |  |  |  |  |  |  |  |
| **Групповой показатель M10 «Определение/коррекция области действия СОИБ»** | | | | | | | | | | | | |
| Обозначение частного показателя ИБ | | Частный показатель ИБ | Обязательность выполнения | Оценка частного показателя ИБ | | | | | | | | Описание выполненной оценки |
|  | |  |  | документированность | | выполнение | | | | | |  |
|  | |  |  | Да | Нет | 0 | 0,25 | 0,5 | 0,75 | 1 | н/о |  |
| М10.1 | | Определена ли в документах организации и корректируется ли опись структурированных по классам защищаемых информационных активов (типов информационных активов — типов информации)? | обязательный |  |  |  |  |  |  |  |  |  |
| М10.2 | | Проводится ли классификация информационных активов по типам на основании оценок ценности информационных активов для интересов (целей) организации, например, в соответствии с тяжестью последствий потери свойств ИБ информационных активов? | рекомендуемый |  |  |  |  |  |  |  |  |  |
| М10.3 | | Содержит ли опись информационных активов информацию о принадлежности конкретного информационного актива к выделенным типам информационных активов (в случае наличия в организации классификации информационных активов)? | обязательный |  |  |  |  |  |  |  |  |  |
| М10.4 | | Содержит ли опись информационных активов (типов информационных активов) перечень их объектов среды, покрывающий все уровни информационной инфраструктуры организации, определенной в разделе 6 стандарта СТО БА ИББС-1.0? | обязательный |  |  |  |  |  |  |  |  |  |
| М10.5 | | Определены ли в документах организации процедуры анализа и пересмотра области действия СОИБ (в частности, процедуры пересмотра при изменении перечня информационных активов организации или типов информационных активов)? | обязательный |  |  |  |  |  |  |  |  |  |
| М10.6 | | Определены ли в документах организации роли по определению/коррекции области действия СОИБ и по составлению и пересмотру описи информационных активов (типов информационных активов), находящихся в области действия СОИБ? | обязательный |  |  |  |  |  |  |  |  |  |
| М10.7 | | Назначены ли в организации ответственные за выполнение ролей по определению/коррекции области действия СОИБ и по составлению и пересмотру описи информационных активов (типов информационных активов), находящихся в области действия СОИБ? | обязательный |  |  |  |  |  |  |  |  |  |
| **Групповой показатель M11 "Выбор/коррекция подхода к оценке рисков нарушения ИБ и проведению оценки рисков нарушения ИБ"** | | | | | | | | | | | | |
| Обозначение частного показателя ИБ | | Частный показатель ИБ | Обязательность выполнения | Оценка частного показателя ИБ | | | | | | | | Описание выполненной оценки |
|  | |  |  | документированность | | выполнение | | | | | |  |
|  | |  |  | Да | Нет | 0 | 0,25 | 0,5 | 0,75 | 1 | н/о |  |
| М11.1 | | Принята ли в организации и корректируется ли методика оценки рисков нарушения ИБ / подход к оценке рисков нарушения ИБ? | обязательный |  |  |  |  |  |  |  |  |  |
| М11.2 | | Определены ли в организации критерии принятия рисков нарушения ИБ и уровень допустимого риска нарушения ИБ? | обязательный |  |  |  |  |  |  |  |  |  |
| М11.3 | | Определяет ли методика оценки рисков нарушения ИБ / подход к оценке рисков нарушения ИБ организации способ и порядок качественного или количественного оценивания риска нарушения ИБ на основании оценивания:  — степени возможности реализации угроз ИБ выявленными и(или) предполагаемыми источниками угроз ИБ, зафиксированных в моделях угроз и нарушителей, в результате их воздействия на объекты среды информационных активов организации (типов информационных активов);  — степени тяжести последствий от потери свойств ИБ, в частности свойств доступности, целостности и конфиденциальности для рассматриваемых информационных активов (типов информационных активов)? | обязательный |  |  |  |  |  |  |  |  |  |
| М11.4 | | Определяет ли порядок оценки рисков нарушения ИБ необходимые процедуры оценки рисков нарушения ИБ, а также последовательность их выполнения? | обязательный |  |  |  |  |  |  |  |  |  |
| М11.5 | | Проводится ли оценка рисков нарушения ИБ для свойств ИБ всех информационных активов (типов информационных активов) области действия СОИБ? | обязательный |  |  |  |  |  |  |  |  |  |
| М11.6 | | Создан ли и поддерживается ли в актуальном состоянии единый информационный ресурс (база данных), содержащий информацию об инцидентах ИБ? | рекомендуемый |  |  |  |  |  |  |  |  |  |
| М11.7 | | Соотносятся ли величины рисков, полученные в результате оценивания рисков нарушения ИБ, с уровнем допустимого риска, принятого в организации? | обязательный |  |  |  |  |  |  |  |  |  |
| М11.8 | | Определен ли в документах организации перечень недопустимых рисков нарушения ИБ, сформированный на основе сравнения полученных в результате оценивания рисков нарушения ИБ величин рисков с уровнем допустимого риска, принятого в организации? | обязательный |  |  |  |  |  |  |  |  |  |
| М11.9 | | Определены ли в документах организации роли, связанные с деятельность по определению/коррекции методики оценки рисков нарушения ИБ / подход к оценке риска нарушения ИБ? | обязательный |  |  |  |  |  |  |  |  |  |
| М11.10 | | Назначены ли ответственные за выполнение ролей, связанных с деятельностью по определению/коррекции методики оценки рисков нарушения ИБ / подход к оценке риска нарушения ИБ? | обязательный |  |  |  |  |  |  |  |  |  |
| М11.11 | | Определены ли в документах организации роли по оценке рисков нарушения ИБ? | обязательный |  |  |  |  |  |  |  |  |  |
| М11.12 | | Назначены ли ответственные за выполнение ролей по оценке рисков нарушения ИБ? | обязательный |  |  |  |  |  |  |  |  |  |
| **Групповой показатель M12 "Разработка планов обработки рисков нарушения ИБ"** | | | | | | | | | | | | |
| Обозначение частного показателя ИБ | | Частный показатель ИБ | Обязательность выполнения | Оценка частного показателя ИБ | | | | | | | | Описание выполненной оценки |
|  | |  |  | документированность | | выполнение | | | | | |  |
|  | |  |  | Да | Нет | 0 | 0,25 | 0,5 | 0,75 | 1 | н/о |  |
| М12.1 | | Определен ли в документах организации по каждому из недопустимых рисков нарушения ИБ план, определяющий один из возможных способов обработки риска:  — перенос риска на сторонние организации (например, путем страхования указанного риска);  — уход от риска (например, путем отказа от деятельности, выполнение которой приводит к появлению риска);  — осознанное принятие риска;  — формирование требований ИБ, снижающих риск до допустимого уровня, и формирование планов по их реализации? | обязательный |  |  |  |  |  |  |  |  |  |
| М12.2 | | Согласованы ли планы обработки рисков нарушения ИБ с руководителем службы ИБ либо лицом, отвечающим в организации за обеспечение ИБ? | обязательный |  |  |  |  |  |  |  |  |  |
| М12.3 | | Утверждены ли руководством организации планы обработки рисков нарушения ИБ? | обязательный |  |  |  |  |  |  |  |  |  |
| М12.4 | | Содержат ли планы реализации требований ИБ последовательность и сроки реализации и внедрения организационных, технических и иных защитных мер? | обязательный |  |  |  |  |  |  |  |  |  |
| М12.5 | | Определены ли в документах организации роли по разработке планов обработки рисков нарушения ИБ? | обязательный |  |  |  |  |  |  |  |  |  |
| М12.6 | | Назначены ли ответственные за выполнение ролей по разработке планов обработки рисков нарушения ИБ? | обязательный |  |  |  |  |  |  |  |  |  |
| **Групповой показатель M13 "Определение/коррекция внутренних документов регламентирующих деятельность в области обеспечения ИБ"** | | | | | | | | | | | | |
| Обозначение частного показателя ИБ | | Частный показатель ИБ | Обязательность выполнения | Оценка частного показателя ИБ | | | | | | | | Описание выполненной оценки |
|  | |  |  | документированность | | выполнение | | | | | |  |
|  | |  |  | Да | Нет | 0 | 0,25 | 0,5 | 0,75 | 1 | н/о |  |
| М13.1 | | Проводится ли разработка и коррекция внутренних документов, регламентирующих деятельность в области обеспечения ИБ в организации, с учетом рекомендаций по стандартизации Банка Абхазии РС БА ИББС-2.0 "Обеспечение информационной безопасности организаций банковской системы Республики Абхазия Методические рекомендации по документации в области обеспечения информационной безопасности в соответствии с требованиями СТО БА ИББС-1.О"? | рекомендуемый |  |  |  |  |  |  |  |  |  |
| М13.2 | | Разработана ли политика ИБ организации? Утверждена ли политика ИБ руководством? | обязательный |  |  |  |  |  |  |  |  |  |
| М13.3 | | Корректируется ли политика ИБ организации? | обязательный |  |  |  |  |  |  |  |  |  |
| М13.4 | | Разработаны ли частные политики ИБ организации? | обязательный |  |  |  |  |  |  |  |  |  |
| М13.5 | | Корректируются ли частные политики ИБ организации? | обязательный |  |  |  |  |  |  |  |  |  |
| М13.6 | | Разработаны ли в организации документы, регламентирующие процедуры выполнения отдельных видов деятельности, связанных с обеспечением ИБ? | обязательный |  |  |  |  |  |  |  |  |  |
| М13.7 | | Корректируются ли в организации документы, регламентирующие процедуры выполнения отдельных видов деятельности, связанных с обеспечением ИБ? | обязательный |  |  |  |  |  |  |  |  |  |
| М13.8 | | Определены ли в организации перечень и формы документов, являющихся свидетельством выполнения деятельности по обеспечению ИБ? | обязательный |  |  |  |  |  |  |  |  |  |
| М13.9 | | Определены ли в политике ИБ (частных политиках ИБ) организации:  — цели и задачи обеспечения ИБ;  — основные области обеспечения ИБ;  — типы основных защищаемых информационных активов;  — модели угроз и нарушителей;  — совокупность правил, требований и руководящих принципов в области ИБ  — основные требования к обеспечению ИБ;  — принципы противодействия угрозам ИБ по отношению к типам основных защищаемых информационных активов;  — основные принципы повышения уровня осознания и осведомленности в области ИБ;  — принципы реализации и контроля выполнения требований политики ИБ? | обязательный |  |  |  |  |  |  |  |  |  |
| М13.10 | | Корректируются ли в политике ИБ (частных политиках ИБ) организации  — цели и задачи обеспечения ИБ;  — основные области обеспечения ИБ;  — типы основных защищаемых информационных активов;  — модели угроз и нарушителей;  — совокупность правил, требований и руководящих принципов в области ИБ  — основные требования к обеспечению ИБ;  — принципы противодействия угрозам ИБ по отношению к типам основных защищаемых информационных активов;  — основные принципы повышения уровня осознания и осведомленности в области ИБ;  — принципы реализации и контроля выполнения требований политики ИБ? | обязательный |  |  |  |  |  |  |  |  |  |
| М13.11 | | Разрабатываются ли внутренние документы, регламентирующие деятельность в области обеспечения ИБ на основе:  — законодательства Республики Абхазия;  — комплекса СТО БА ИББС, в частности требования 7-го и 8-го разделов стандарта СТО БАИББС-1.0;  — нормативных актов и предписаний регулирующих и надзорных органов — договорных требований организации со сторонними организациями  — результатов оценки рисков, выполненной с соответствующей уровню разрабатываемого документа детализацией рассматриваемых информационных активов (типов информационных активов)? | обязательный |  |  |  |  |  |  |  |  |  |
| М13.12 | | Корректируются ли внутренние документы, регламентирующие деятельность в области обеспечения ИБ на основе:  — законодательства Республики Абхазия;  — комплекса СТО БА ИББС, в частности требования 7-го и 8-го разделов стандарта СТО БАИББС-1.0;  — нормативных актов и предписаний регулирующих и надзорных органов  — договорных требований организации со сторонними организациями  — результатов оценки рисков, выполненной с соответствующей уровню разрабатываемого документа детализацией рассматриваемых информационных активов (типов информационных активов)? | обязательный |  |  |  |  |  |  |  |  |  |
| М13.13 | | Содержит ли совокупность внутренних документов, регламентирующих деятельность в области обеспечения ИБ, требования по обеспечению ИБ всех выявленных информационных активов (типов информационных активов), находящихся в области действия СОИБ организации? | обязательный |  |  |  |  |  |  |  |  |  |
| М13.14 | | Не противоречат ли документы, регламентирующие процедуры выполнения отдельных видов деятельности, связанных с обеспечением ИБ, положениям политики ИБ и частных политик ИБ? | обязательный |  |  |  |  |  |  |  |  |  |
| М13.15 | | Детализируют ли документы, регламентирующие процедуры выполнения отдельных видов деятельности, связанных с обеспечением ИБ, положения политики ИБ и частных политик ИБ? | обязательный |  |  |  |  |  |  |  |  |  |
| М13.16 | | Утвержден ли руководством организации порядок взаимодействия (координирования работы) службы ИБ с работниками, ответственными за обеспечение ИБ в структурных подразделениях организации (в случае наличия в структурных подразделениях организации работников, ответственных за обеспечение ИБ)? | обязательный |  |  |  |  |  |  |  |  |  |
| М13.17 | | Определены ли в составе документов, регламентирующих деятельность в области обеспечения ИБ, перечень свидетельств выполнения указанной деятельности и ответственность работников организации за выполнение этой деятельности? | обязательный |  |  |  |  |  |  |  |  |  |
| М13.18 | | Определены ли в документах организации процедуры выделения и распределения ролей в области обеспечения ИБ? | обязательный |  |  |  |  |  |  |  |  |  |
| М13.19 | | Определен ли в документах организации порядок разработки, поддержки, пересмотра и контроля исполнения внутренних документов, регламентирующих деятельность по обеспечению ИБ организации? | обязательный |  |  |  |  |  |  |  |  |  |
| М13.20 | | Определены ли в документах организации роли по разработке, поддержке, пересмотру и контролю исполнения внутренних документов, регламентирующих деятельность по обеспечению ИБ организации? | обязательный |  |  |  |  |  |  |  |  |  |
| М13.21 | | Назначены ли ответственные за выполнение ролей по разработке, поддержке, пересмотру и контролю исполнения внутренних документов, регламентирующих деятельность по обеспечению ИБ организации? | обязательный |  |  |  |  |  |  |  |  |  |
| **Групповой показатель M14 "Принятие руководством организации БС РА решений о реализации и эксплуатации СОИБ"** | | | | | | | | | | | | |
| Обозначение частного показателя ИБ | | Частный показатель ИБ | Обязательность выполнения | Оценка частного показателя ИБ | | | | | | | | Описание выполненной оценки |
|  | |  |  | документированность | | выполнение | | | | | |  |
|  | |  |  | Да | Нет | 0 | 0,25 | 0,5 | 0,75 | 1 | н/о |  |
| М14.1 | | Оформлены ли документально и утверждены ли руководством решения о реализации и эксплуатации СОИБ, в частности решения:  — об анализе и принятии остаточных рисков нарушения ИБ;  — о планировании этапов внедрения СОИБ, в частности требований ИБ, изложенных в 7-м и 8-м разделах СТО БА ИББС-1.0;  — о распределении ролей в области обеспечения ИБ организации;  — о принятии со стороны руководства планов внедрения защитных мер, направленных на реализацию требований 7-го и 8-го разделов СТО БА ИББС-1.0 и снижение рисков ИБ;  — о выделении ресурсов, необходимых для реализации и эксплуатации функционирования СОИБ? | обязательный |  |  |  |  |  |  |  |  |  |
| М14.2 | | Утверждены ли руководством все планы внедрения СОИБ, в частности планы реализаций требований 7-го и 8-го разделов СТО БА ИББС-1.0, планы обработки рисков нарушения ИБ и внедрения защитных мер, в которых документально зафиксированы:  — последовательность выполнения мероприятий в рамках указанных планов;  — сроки начала и окончания запланированных мероприятий;  — должностные лица (подразделения), ответственные за выполнение каждого указанного мероприятия? | обязательный |  |  |  |  |  |  |  |  |  |
| М14.3 | | Определен ли документально порядок разработки, пересмотра и контроля исполнения планов по обеспечению ИБ организации? | обязательный |  |  |  |  |  |  |  |  |  |
| М14.4 | | Оформлены ли документально решения руководства, связанные с назначением и распределением ролей для всех структурных подразделений в соответствии с положениями внутренних документов, регламентирующих деятельность по обеспечению ИБ организации? | обязательный |  |  |  |  |  |  |  |  |  |
| **Групповой показатель M15 "Организация реализации планов внедрения СОИБ"** | | | | | | | | | | | | |
| Обозначение частного показателя ИБ | | Частный показатель ИБ | Обязательность выполнения | Оценка частного показателя ИБ | | | | | | | | Описание выполненной оценки |
|  | |  |  | документированность | | выполнение | | | | | |  |
|  | |  |  | Да | Нет | 0 | 0,25 | 0,5 | 0,75 | 1 | н/о |  |
| М15.1 | | Определены ли в документах организации и выполняются ли проектирование/приобретение/ развертывание, внедрение, эксплуатация, контроль и сопровождение эксплуатации защитных мер (СИБ), предусмотренных планами реализации требований ИБ? | обязательный |  |  |  |  |  |  |  |  |  |
| М15.2 | | Реализуются ли при построении элементов СИБ (применительно к конкретной области или сфере деятельности организации) защитные меры, применяемые к объектам среды, в соответствии с существующими в организации требованиями обеспечения ИБ, сформулированными в политике ИБ и других внутренних документах организации? | обязательный |  |  |  |  |  |  |  |  |  |
| М15.3 | | Определены ли в документах организации роли, связанные с реализацией планов обработки рисков нарушения ИБ и с реализацией требуемых защитных мер? | обязательный |  |  |  |  |  |  |  |  |  |
| М15.4 | | Назначены ли ответственные за выполнение ролей, связанных с реализацией планов обработки рисков нарушения ИБ и с реализацией требуемых защитных мер? | обязательный |  |  |  |  |  |  |  |  |  |
| **Групповой показатель M16 "Разработка и организация реализации программ по обучению и повышению осведомленности в области ИБ"** | | | | | | | | | | | | |
| Обозначение частного показателя ИБ | | Частный показатель ИБ | Обязательность выполнения | Оценка частного показателя ИБ | | | | | | | | Описание выполненной оценки |
|  | |  |  | документированность | | выполнение | | | | | |  |
|  | |  |  | Да | Нет | 0 | 0,25 | 0,5 | 0,75 | 1 | н/о |  |
| М16.1 | | Организована ли документально оформленная работа с персоналом организации в направлении повышения осведомленности и обучения в области ИБ, включая разработку и реализацию планов и программ обучения и повышения осведомленности в области ИБ и контроля результатов выполнения указанных планов? Утверждена ли руководством указанная работа? | обязательный |  |  |  |  |  |  |  |  |  |
| М16.2 | | Установлены ли в планах обучения и повышения осведомленности требования к периодичности обучения и повышения осведомленности? | обязательный |  |  |  |  |  |  |  |  |  |
| М16.3 | | Включена ли в программы обучения и повышения осведомленности информация:  - по существующим политикам ИБ;  - по применяемым в организации защитным мерам;  - по правильному использованию защитных мер в соответствии с внутренними документами организации;  - о значимости и важности деятельности работников для обеспечения ИБ организации? | обязательный |  |  |  |  |  |  |  |  |  |
| М16.4 | | Определен ли в организации перечень документов, являющихся свидетельством выполнения программ обучения и повышения осведомленности в области ИБ, в частности:  - документы (журналы), подтверждающие прохождение руководителями и работниками организации обучения в области ИБ с указанием уровня образования, навыков, опыта и квалификации обучаемых;  - документы, содержащие результаты проверок обучения работников организации;  - документы, содержащие результаты проверок осведомленности в области ИБ в организации? | обязательный |  |  |  |  |  |  |  |  |  |
| М16.5 | | Организуется ли для работника, получившего новую роль, обучение или инструктаж в области ИБ, соответствующий полученной роли? | обязательный |  |  |  |  |  |  |  |  |  |
| М16.6 | | Определены ли в документах организации роли по разработке, реализации планов и программ обучения и повышения осведомленности в области ИБ и по контролю их результатов? | обязательный |  |  |  |  |  |  |  |  |  |
| М16.7 | | Назначены ли ответственные за выполнение ролей по разработке, реализации планов и программ обучения и повышения осведомленности в области ИБ и по контролю их результатов? | обязательный |  |  |  |  |  |  |  |  |  |
| **Групповой показатель M17 "Организация обнаружения и реагирования на инциденты безопасности"** | | | | | | | | | | | | |
| Обозначение частного показателя ИБ | | Частный показатель ИБ | Обязательность выполнения | Оценка частного показателя ИБ | | | | | | | | Описание выполненной оценки |
|  | |  |  | документированность | | выполнение | | | | | |  |
|  | |  |  | Да | Нет | 0 | 0,25 | 0,5 | 0,75 | 1 | н/о |  |
| М17.1 | | Существуют ли в организации документы, регламентирующие процедуры обработки инцидентов, включающие:  — процедуры обнаружения инцидентов ИБ;  — процедуры информирования об инцидентах;  — процедуры классификации инцидентов и оценки ущерба, нанесенного инцидентом ИБ;  — процедуры реагирования на инцидент;  — процедуры анализа причин инцидентов ИБ и оценки результатов реагирования на инциденты ИБ (при необходимости — с участием внешних экспертов в области ИБ)? | обязательный |  |  |  |  |  |  |  |  |  |
| М17.2 | | Сформирована и поддерживается ли в актуальном состоянии централизованная база инцидентов ИБ? | рекомендуемый |  |  |  |  |  |  |  |  |  |
| М17.3 | | Определены ли в документах организации процедуры по хранению информации:  — об инцидентах ИБ;  — о практиках анализа инцидентов ИБ;  — о результатах реагирования на инциденты ИБ? | обязательный |  |  |  |  |  |  |  |  |  |
| М17.4 | | Определены ли в документах организации порядок действий работников организации при обнаружении нетипичных событий, связанных с ИБ, и порядок информирования о данных событиях? | обязательный |  |  |  |  |  |  |  |  |  |
| М17.5 | | Осведомлены ли работники организации о порядке действий при обнаружении нетипичных событий, связанных с ИБ, и порядке информирования о данных событиях? | обязательный |  |  |  |  |  |  |  |  |  |
| М17.6 | | Учитывают ли процедуры расследования инцидентов действующее законодательство Республики Абхазия, положения нормативных актов Банка Абхазии, а также внутренних документов организации в области ИБ? | обязательный |  |  |  |  |  |  |  |  |  |
| М17.7 | | Принимаются и выполняются ли в организации документально оформленные решения по всем выявленным инцидентам ИБ? | обязательный |  |  |  |  |  |  |  |  |  |
| М17.8 | | Определены ли в документах организации роли по обнаружению, классификации, реагированию, анализу и расследованию инцидентов ИБ? | обязательный |  |  |  |  |  |  |  |  |  |
| М17.9 | | Назначены ли ответственные за выполнение ролей по обнаружению, классификации, реагированию, анализу и расследованию инцидентов ИБ? | обязательный |  |  |  |  |  |  |  |  |  |
| **Групповой показатель M18 "Организация обеспечения непрерывности бизнеса и его восстановления после прерываний"** | | | | | | | | | | | | |
| Обозначение частного показателя ИБ | | Частный показатель ИБ | Обязательность выполнения | Оценка частного показателя ИБ | | | | | | | | Описание выполненной оценки |
|  | |  |  | документированность | | выполнение | | | | | |  |
|  | |  |  | Да | Нет | 0 | 0,25 | 0,5 | 0,75 | 1 | н/о |  |
| М18.1 | | Выделены ли в описи защищаемых информационных активов организации активы, существенные для обеспечения непрерывности бизнеса организации | обязательный |  |  |  |  |  |  |  |  |  |
| М18.2 | | Определены ли документально в организации требования обеспечения ИБ, регламентирующие вопросы обеспечения непрерывности бизнеса и его восстановления после прерывания? | обязательный |  |  |  |  |  |  |  |  |  |
| М18.3 | | Определен ли в документах организации план обеспечения непрерывности бизнеса и его восстановления после возможного прерывания, содержащий инструкции и порядок действий работников организации, в состав которого включены:  — условия активизации плана;  — порядок действий, которые должны быть предприняты после инцидента ИБ (инструкции персонала);  — процедуры восстановления;  — процедуры тестирования и проверки плана;  — план обучения и повышения осведомленности работников организации — обязанности работников организации с указанием ответственных за выполнение каждого из положений плана? | обязательный |  |  |  |  |  |  |  |  |  |
| М18.4 | | Основывается ли разработка планов обеспечения непрерывности бизнеса и его восстановления после прерываний на документально оформленных результатах оценки рисков нарушения ИБ организации применительно к информационным активам, существенным для обеспечения непрерывности бизнеса и его восстановления после прерывания? | обязательный |  |  |  |  |  |  |  |  |  |
| М18.5 | | Определены ли документально, реализованы и эксплуатируются ли защитные меры обеспечения непрерывности бизнеса применительно к информационным активам, существенным для обеспечения непрерывности бизнеса и его восстановления после прерывания? | обязательный |  |  |  |  |  |  |  |  |  |
| М18.6 | | Основываются ли реализация и использование защитных мер обеспечения непрерывности бизнеса и его восстановления после прерывания на соответствующих требованиях обеспечения ИБ? | обязательный |  |  |  |  |  |  |  |  |  |
| М18.7 | | Согласован ли план обеспечения непрерывности бизнеса и его восстановления после прерываний с существующими в организации процедурами обработки инцидентов ИБ? | обязательный |  |  |  |  |  |  |  |  |  |
| М18.8 | | Определено ли в документах организации и выполняется ли периодическое тестирование плана обеспечения непрерывности бизнеса и его восстановления после прерывания? | обязательный |  |  |  |  |  |  |  |  |  |
| М18.9 | | Составлен ли сценарий тестирования плана обеспечения непрерывности бизнеса и его восстановления после прерывания с учетом существующей в организации модели угроз и нарушителей, а также результатов оценки рисков? | обязательный |  |  |  |  |  |  |  |  |  |
| М18.10 | | Проводится ли при необходимости корректировка плана обеспечения непрерывности бизнеса и его восстановления после прерывания по результатам тестирования? | обязательный |  |  |  |  |  |  |  |  |  |
| М18.11 | | Реализована ли в организации программа обучения и повышения осведомленности работников в области обеспечения непрерывности бизнеса и его восстановления после прерываний? | обязательный |  |  |  |  |  |  |  |  |  |
| М18.12 | | Определены ли в документах организации и выполняются ли процедуры регулярного пересмотра и обновления плана обеспечения непрерывности бизнеса и его восстановления после прерывания (для обеспечения уверенности в их эффективности), учитывающие изменения в приоритетах, целях и интересах бизнеса организации; пересмотр моделей угроз; оценку рисков нарушения ИБ? | обязательный |  |  |  |  |  |  |  |  |  |
| М18.13 | | Определены ли в документах организации роли по разработке плана обеспечения непрерывности бизнеса и его восстановления после прерывания? | обязательный |  |  |  |  |  |  |  |  |  |
| М18.14 | | Назначены ли ответственные за выполнение ролей по разработке плана обеспечения непрерывности бизнеса и его восстановления после прерывания? | обязательный |  |  |  |  |  |  |  |  |  |
| **Групповой показатель M19 "Мониторинг и контроль защитных мер"** | | | | | | | | | | | | |
| Обозначение частного показателя ИБ | | Частный показатель ИБ | Обязательность выполнения | Оценка частного показателя ИБ | | | | | | | | Описание выполненной оценки |
|  | |  |  | документированность | | выполнение | | | | | |  |
|  | |  |  | Да | Нет | 0 | 0,25 | 0,5 | 0,75 | 1 | н/о |  |
| М19.1 | | Определены ли в документах организации процедуры мониторинга СОИБ и контроля защитных мер, которые охватывают все реализованные и эксплуатируемые защитные меры, входящие в СИБ, проводятся персоналом организации, ответственным за обеспечение ИБ? | обязательный |  |  |  |  |  |  |  |  |  |
| М19.2 | | Фиксируются ли документально результаты выполнения процедур мониторинга СОИБ и контроля защитных мер? | обязательный |  |  |  |  |  |  |  |  |  |
| М19.3 | | Определены ли в документах организации и выполняются ли процедуры сбора и хранения информации о действиях работников организации, событиях и параметрах, имеющих отношение к функционированию защитных мер? | обязательный |  |  |  |  |  |  |  |  |  |
| М19.4 | | Включается ли в базу данных инцидентов информация обо всех инцидентах ИБ, выявленных в процессе мониторинга СОИБ и контроля защитных мер? | обязательный |  |  |  |  |  |  |  |  |  |
| М19.5 | | Подвергаются ли процедуры мониторинга СОИБ и контроля защитных мер регулярным и документально зафиксированным пересмотрам в связи с изменениями в составе и способах использования защитных мер, выявлением новых угроз и уязвимостей ИБ, а также на основе данных об инцидентах ИБ? | обязательный |  |  |  |  |  |  |  |  |  |
| М19.6 | | Определен ли в документах организации порядок пересмотра процедур мониторинга СОИБ и контроля защитных мер? | обязательный |  |  |  |  |  |  |  |  |  |
| М19.7 | | Определены ли в документах организации роли, связанные с выполнением процедур мониторинга СОИБ и контроля защитных мер, а также с пересмотром указанных процедур? | обязательный |  |  |  |  |  |  |  |  |  |
| М19.8 | | Назначены ли ответственные за выполнение ролей, связанных с выполнением процедур мониторинга СОИБ и контроля защитных мер, а также с пересмотром указанных процедур? | обязательный |  |  |  |  |  |  |  |  |  |
| **Групповой показатель M20 "Проведение самооценки ИБ"** | | | | | | | | | | | | |
| Обозначение частного показателя ИБ | | Частный показатель ИБ | Обязательность выполнения | Оценка частного показателя ИБ | | | | | | | | Описание выполненной оценки |
|  | |  |  | документированность | | выполнение | | | | | |  |
|  | |  |  | Да | Нет | 0 | 0,25 | 0,5 | 0,75 | 1 | н/о |  |
| М20.1 | | Проводится ли самооценка ИБ в соответствии с настоящим стандартом? | обязательный |  |  |  |  |  |  |  |  |  |
| М20.2 | | Организован ли порядок проведения самооценки ИБ в соответствии с рекомендациями по стандартизации Банка Абхазии РС БА ИББС-2.1 "Обеспечение информационной безопасности организаций банковской системы Республики Абхазия Руководство по самооценке соответствия информационной безопасности организаций банковской системы Республики Абхазия требованиям СТО БА ИББС-1.0"? | рекомендуемый |  |  |  |  |  |  |  |  |  |
| М20.3 | | Определена ли в документах организации и реализована ли программа самооценок ИБ, содержащая информацию, необходимую для планирования и организации самооценок ИБ, их контроля, анализа и совершенствования, а также обеспечения их ресурсами, необходимыми для эффективного и результативного проведения указанных самооценок ИБ в заданные сроки? | обязательный |  |  |  |  |  |  |  |  |  |
| М:20.4 | | Определены ли в документах организации  — порядок формирования, сбора и хранения свидетельств самооценки ИБ  — периодичность проведения самооценки ИБ;  — порядок хранения и использования результатов самооценки ИБ? | обязательный |  |  |  |  |  |  |  |  |  |
| М20.5 | | Оформлен ли в документах организации для каждой проводимой в организации самооценки ИБ план ее проведения, определяющий:  — цель самооценки ИБ;  — объекты и деятельность, подвергающиеся самооценке ИБ;  — порядок и сроки выполнения мероприятий самооценки ИБ;  — распределение ролей среди работников организации, связанных с проведением самооценки ИБ? | обязательный |  |  |  |  |  |  |  |  |  |
| М20.6 | | Подготавливаются ли по результатам самооценок ИБ отчеты? | обязательный |  |  |  |  |  |  |  |  |  |
| М20.7 | | Доводятся ли результаты самооценок ИБ и соответствующие отчеты до руководства организации? | обязательный |  |  |  |  |  |  |  |  |  |
| М20.8 | | Определены ли в документах организации роли, связанные с выполнением программы самооценок ИБ? | обязательный |  |  |  |  |  |  |  |  |  |
| М20.9 | | Назначены ли ответственные за выполнение ролей, связанных с выполнением программы самооценок ИБ? | обязательный |  |  |  |  |  |  |  |  |  |
| **Групповой показатель M21 "Проведение аудита ИБ"** | | | | | | | | | | | | |
| Обозначение частного показателя ИБ | | Частный показатель ИБ | Обязательность выполнения | Оценка частного показателя ИБ | | | | | | | | Описание выполненной оценки |
|  | |  |  | документированность | | выполнение | | | | | |  |
|  | |  |  | Да | Нет | 0 | 0,25 | 0,5 | 0,75 | 1 | н/о |  |
| М21.1 | | Проводится ли аудит ИБ организации в соответствии с требованиями стандарта Банка Абхазии СТО БА ИББС-1.1 "Обеспечение информационной безопасности организаций банковской системы Республики Абхазия. Аудит информационной безопасности" и настоящего стандарта? | обязательный |  |  |  |  |  |  |  |  |  |
| М21.2 | | Определена ли в документах организации и реализуется ли программа аудитов ИБ, содержащая информацию, необходимую для планирования и организации аудитов ИБ, их контроля, анализа и совершенствования, а также обеспечения их ресурсами, необходимыми для эффективного и результативного проведения указанных аудитов ИБ в заданные сроки? | обязательный |  |  |  |  |  |  |  |  |  |
| М21.3 | | Оформлен ли в документах организации для каждого проводимого в организации аудита ИБ план аудита, определяющий:  - цель аудита ИБ;  - критерии аудита ИБ;  - область аудита ИБ;  - дату и продолжительность проведения аудита ИБ;  - состав аудиторской группы;  - описание деятельности и мероприятий по проведению аудита ИБ;  - распределение ресурсов при проведении аудита ИБ? | обязательный |  |  |  |  |  |  |  |  |  |
| М21.4 | | Оформлены ли договоры с аудиторскими организациями и определены ли в соответствующих документах:  - порядок хранения, доступа и использования материалов, получаемых в процессе проведения аудита ИБ;  - порядок взаимодействия с аудиторской организацией в процессе проведения аудита ИБ;  - порядок взаимодействия аудиторской группы и руководства, позволяющий представителям аудиторской группы при необходимости непосредственно обращаться к руководству;  - порядок организации опроса работников;  - порядок организации наблюдения за деятельностью работников организации со стороны представителей аудиторской организации? | обязательный |  |  |  |  |  |  |  |  |  |
| М21.5 | | Подготавливаются ли по результатам аудитов ИБ отчеты? | обязательный |  |  |  |  |  |  |  |  |  |
| М21.6 | | Доводятся ли результаты аудитов ИБ и соответствующие отчеты до руководства организации? | обязательный |  |  |  |  |  |  |  |  |  |
| М21.7 | | Определен ли в документах организации порядок хранения, доступа и использования материалов, получаемых в процессе проведения аудитов, в частности отчетов аудитов? | обязательный |  |  |  |  |  |  |  |  |  |
| М21.8 | | Определены ли в документах организации роли, связанные с организацией выполнения программ аудитов и планов отдельных аудитов? | обязательный |  |  |  |  |  |  |  |  |  |
| М21.9 | | Назначены ли ответственные за выполнение ролей, связанных с организацией выполнения программ аудитов и планов отдельных внешних аудитов? | обязательный |  |  |  |  |  |  |  |  |  |
| **Групповой показатель M22 "Анализ функционирования СОИБ"** | | | | | | | | | | | | |
| Обозначение частного показателя ИБ | | Частный показатель ИБ | Обязательность выполнения | Оценка частного показателя ИБ | | | | | | | | Описание выполненной оценки |
|  | |  |  | документированность | | выполнение | | | | | |  |
|  | |  |  | Да | Нет | 0 | 0,25 | 0,5 | 0,75 | 1 | н/о |  |
| М22.1 | | Проводится ли в организации анализ функционирования СОИБ, использующий в том числе:  — результаты мониторинга СОИБ и контроля защитных мер;  — сведения об инцидентах ИБ;  — результаты проведения аудитов ИБ, самооценок ИБ;  — данные об угрозах, возможных нарушителях и уязвимостях ИБ;  — данные об изменениях внутри организации, например данные об изменениях в процессах и технологиях, реализуемых в рамках основного процессного потока, изменениях во внутренних документах организации;  — данные об изменениях вне организации, например данные об изменения в законодательстве Республики Абхазия, изменениях в требованиях комплекса БА ИББС, изменениях в договорных обязательствах организации? | обязательный |  |  |  |  |  |  |  |  |  |
| М22.2 | | Проводится ли анализ соответствия комплекса внутренних документов, регламентирующих деятельность по обеспечению ИБ в организации, требованиям законодательства РА, требованиям стандартов Банка Абхазии, контрактным требованиям организации? | обязательный |  |  |  |  |  |  |  |  |  |
| М22.3 | | Проводится ли анализ соответствия внутренних документов нижних уровней иерархии, регламентирующих деятельность по обеспечению ИБ в организации, требованиям политик ИБ организации? | обязательный |  |  |  |  |  |  |  |  |  |
| М22.4 | | Проводится ли оценка рисков в области ИБ организации, включая оценку уровня остаточного и допустимого рисков? | обязательный |  |  |  |  |  |  |  |  |  |
| М22.5 | | Проводится ли проверка адекватности модели угроз организации существующим угрозам ИБ? | обязательный |  |  |  |  |  |  |  |  |  |
| М22.6 | | Проводится ли оценка адекватности используемых защитных мер требованиям внутренних документов организации и результатам оценки рисков? | обязательный |  |  |  |  |  |  |  |  |  |
| М22.7 | | Проводится ли анализ отсутствия разрывов в технологических процессах обеспечения ИБ, а также несогласованности в использовании защитных мер? | обязательный |  |  |  |  |  |  |  |  |  |
| М22.8 | | Документируются ли результаты анализа функционирования СОИБ | обязательный |  |  |  |  |  |  |  |  |  |
| М22.9 | | Определены ли в документах организации роли, связанные с процедурами анализа функционирования СОИБ? | обязательный |  |  |  |  |  |  |  |  |  |
| М22.10 | | Назначены ли ответственные за выполнение ролей, связанных с процедурами анализа функционирования СОИБ? | обязательный |  |  |  |  |  |  |  |  |  |
| **Групповой показатель M23 "Анализ СОИБ со стороны руководства организации БС РА"** | | | | | | | | | | | | |
| Обозначение частного показателя ИБ | | Частный показатель ИБ | Обязательность выполнения | Оценка частного показателя ИБ | | | | | | | | Описание выполненной оценки |
|  | |  |  | документированность | | выполнение | | | | | |  |
|  | |  |  | Да | Нет | 0 | 0,25 | 0,5 | 0,75 | 1 | н/о |  |
| М23.1 | | Утвержден ли в организации перечень документов (данных), необходимых для формирования информации, предоставляемой руководству с целью проведения анализа СОИБ? | обязательный |  |  |  |  |  |  |  |  |  |
| М23.2 | | Входят ли в перечень документов, необходимых для формирования информации, предоставляемой руководству с целью проведения анализа СОИБ, отчеты с результатами:  - мониторинга СОИБ и контроля защитных мер;  - анализа функционирования СОИБ;  - аудитов ИБ;  - самооценок ИБ? | обязательный |  |  |  |  |  |  |  |  |  |
| М23.3 | | Входят ли в перечень документов, необходимых для формирования информации, предоставляемой руководству с целью проведения анализа СОИБ, документы, содержащие информацию:  - о способах и методах защиты, защитных мерах или процедурах их использования, которые могли бы использоваться для улучшения функционирования СОИБ; - о новых выявленных уязвимостях и угрозах ИБ;  - о действиях, предпринятых по итогам предыдущих анализов СОИБ, осуществленных руководством;  - об изменениях, которые могли бы повлиять на организацию СОИБ, например изменения в законодательстве Республики Абхазия и(или) в положениях стандартов Банка Абхазии;  - о выявленных инцидентах ИБ? | обязательный |  |  |  |  |  |  |  |  |  |
| М23.4 | | Входят ли в перечень документов, необходимых для формирования информации, предоставляемой руководству с целью проведения анализа СОИБ, документы, подтверждающие выполнение требуемой деятельности по обеспечению ИБ, например выполнение планов обработки рисков? | обязательный |  |  |  |  |  |  |  |  |  |
| М23.5 | | Входят ли в перечень документов, необходимых для формирования информации, предоставляемой руководству с целью проведения анализа СОИБ, документы, подтверждающие выполнение требований непрерывности бизнеса и его восстановления после прерывания? | обязательный |  |  |  |  |  |  |  |  |  |
| М23.6 | | Определен ли в организации и утвержден ли руководством план выполнения деятельности по контролю и анализу СОИБ, содержащий, в частности, положения по проведению совещаний на уровне руководства, на которых в том числе производятся поиск и анализ проблем ИБ, влияющих на бизнес организации? | обязательный |  |  |  |  |  |  |  |  |  |
| М23.7 | | Определены ли в документах организации роли, связанные с подготовкой информации, необходимой для анализа СОИБ руководством? | обязательный |  |  |  |  |  |  |  |  |  |
| М23.8 | | Назначены ли ответственные за выполнение ролей, связанных с подготовкой информации, необходимой для анализа СОИБ руководством? | обязательный |  |  |  |  |  |  |  |  |  |
| **Групповой показатель M24 "Принятие решений по тактическим улучшениям СОИБ"** | | | | | | | | | | | | |
| Обозначение частного показателя ИБ | | Частный показатель ИБ | Обязательность выполнения | Оценка частного показателя ИБ | | | | | | | | Описание выполненной оценки |
|  | |  |  | документированность | | выполнение | | | | | |  |
|  | |  |  | Да | Нет | 0 | 0,25 | 0,5 | 0,75 | 1 | н/о |  |
| М24.1 | | Рассматриваются ли при принятии решений, связанных с тактическими улучшениями СОИБ, документально оформленные результаты:  — аудитов ИБ;  — самооценок ИБ;  — мониторинга СОИБ и контроля защитных мер;  — анализа функционирования СОИБ;  — обработки инцидентов ИБ;  — выявления новых угроз и уязвимостей ИБ;  — оценки рисков;  — анализа перечня защитных мер, возможных для применения;  — стратегических улучшений СОИБ;  — анализа СОИБ со стороны руководства;  — анализа успешных практик в области ИБ (собственных или других организаций)? | обязательный |  |  |  |  |  |  |  |  |  |
| М24.2 | | Оформляются ли документально решения по тактическим улучшениям СОИБ, содержащие либо выводы об отсутствии необходимости тактических улучшений СОИБ, либо направления тактических улучшений СОИБ? | обязательный |  |  |  |  |  |  |  |  |  |
| М24.3 | | Формируются ли направления тактических улучшений СОИБ в виде корректирующих и превентивных действий? | обязательный |  |  |  |  |  |  |  |  |  |
| М24.4 | | Определены ли в документах организации планы реализации тактических улучшений СОИБ? | обязательный |  |  |  |  |  |  |  |  |  |
| М24.5 | | Существуют ли в организации документы, в которых фиксируются результаты выполнения планов реализации тактических улучшений СОИБ? | обязательный |  |  |  |  |  |  |  |  |  |
| М24.6 | | Санкционирует и контролирует ли руководство службы ИБ организации деятельность, связанную с реализацией тактических улучшений СОИБ? | обязательный |  |  |  |  |  |  |  |  |  |
| М24.7 | | Определены ли в документах организации и выполняются ли процедуры согласования и информирования заинтересованных сторон о тактических улучшениях СОИБ, в частности об изменениях, относящихся к обеспечению ИБ, к ответственности в области ИБ, к требованиям ИБ? Фиксируются ли результаты выполнения указанных процедур? | обязательный |  |  |  |  |  |  |  |  |  |
| М24.8 | | Назначаются ли ответственные за реализацию решений по тактическим улучшениям СОИБ? | обязательный |  |  |  |  |  |  |  |  |  |
| **Групповой показатель M25 "Принятие решений по стратегическим улучшениям СОИБ"** | | | | | | | | | | | | |
| Обозначение частного показателя ИБ | | Частный показатель ИБ | Обязательность выполнения | Оценка частного показателя ИБ | | | | | | | | Описание выполненной оценки |
|  | |  |  | документированность | | выполнение | | | | | |  |
|  | |  |  | Да | Нет | 0 | 0,25 | 0,5 | 0,75 | 1 | н/о |  |
| М25.1 | | Рассматриваются ли при принятии решений, связанных со стратегическими улучшениями СОИБ, документально оформленные результаты:  - аудитов ИБ;  - самооценок ИБ;  - мониторинга СОИБ и контроля защитных мер;  - анализа функционирования СОИБ;  - обработки инцидентов ИБ;  - выявления новых информационных активов организации или их типов  - выявления новых угроз и уязвимостей ИБ;  - оценки рисков;  - пересмотра основных рисков ИБ;  - анализа СОИБ со стороны руководства;  - анализа успешных практик в области ИБ (собственных или других организаций)? | обязательный |  |  |  |  |  |  |  |  |  |
| М25.2 | | Рассматриваются ли при принятии решений, связанных со стратегическими улучшениями СОИБ, изменения интересов, целей и задач бизнеса организации, контрактных обязательств организации, а также изменения в законодательстве РА и нормативных актах Банка Абхазии? | обязательный |  |  |  |  |  |  |  |  |  |
| М25.3 | | Оформляются ли документально решения по стратегическим улучшениям СОИБ, содержащие либо выводы об отсутствии необходимости стратегических улучшений СОИБ, либо направления стратегических улучшений СОИБ? | обязательный |  |  |  |  |  |  |  |  |  |
| М25.4 | | Формируются ли направления стратегических улучшений СОИБ в виде корректирующих или превентивных действий, например:  - уточнение/пересмотр целей и задач обеспечения ИБ, определенных в рамках политики ИБ (частных политик ИБ) организации;  - изменения в области действия СОИБ;  - уточнение описи типов информационных активов;  - пересмотр моделей угроз и нарушителей;  - изменение подходов к оценке рисков ИБ, критериев принятия риска ИБ? | обязательный |  |  |  |  |  |  |  |  |  |
| М25.5 | | Определены ли в документах организации планы реализации стратегических улучшений СОИБ? | обязательный |  |  |  |  |  |  |  |  |  |
| М25.6 | | Существуют ли в организации документы, в которых фиксируются результаты выполнения планов реализации стратегических улучшений СОИБ? | обязательный |  |  |  |  |  |  |  |  |  |
| М25.7 | | Санкционирует и контролирует ли руководство организации деятельность, связанную с реализацией стратегических улучшений СОИБ? | обязательный |  |  |  |  |  |  |  |  |  |
| М25.8 | | В случае стратегических улучшений СОИБ выполняется ли деятельность по реализации соответствующих тактических улучшений СОИБ для всех необходимых процедур обеспечения ИБ, используемых защитных мер и соответствующих внутренних документов, в частности, выполняются ли:  - выработка планов тактических улучшений СОИБ;  - уточнение планов обработки рисков;  - уточнение программы внедрения защитных мер;  - уточнение процедур использования защитных мер? | обязательный |  |  |  |  |  |  |  |  |  |
| М25.9 | | Определены ли в документах организации и выполняются ли процедуры согласования и информирования заинтересованных сторон о стратегических улучшениях СОИБ, в частности об изменениях, относящихся к обеспечению ИБ, к ответственности в области ИБ, к требованиям ИБ? Фиксируются ли документально результаты выполнения указанных процедур? | обязательный |  |  |  |  |  |  |  |  |  |
| М25.10 | | Назначаются ли ответственные за реализацию решений по стратегическим улучшениям СОИБ? | обязательный |  |  |  |  |  |  |  |  |  |

|  |  |  |  |
| --- | --- | --- | --- |
|  |  | | |
|  | Подпись руководителя организации | | |
|  |  | | |
|  |  |  |
|  | дата |  |