РЕКОМЕНДАЦИИ
В ОБЛАСТИ СТАНДАРТИЗАЦИИ БАНКА АБХАЗИИ

РС БА ИББС-2.2-2013

ОБЕСПЕЧЕНИЕ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ ОРГАНИЗАЦИЙ БАНКОВСКОЙ СИСТЕМЫ РЕСПУБЛИКИ АБХАЗИЯ

МЕТОДИКА
ОЦЕНКИ РИСКОВ НАРУШЕНИЯ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ

Введение

Действующим стандартом Банка Абхазии "Обеспечение информационной безопасности организаций банковской системы Республики Абхазия. Общие положения" (далее - СТО БА ИББС-1.0-2009) с целью создания и поддержания на должном уровне системы обеспечения информационной безопасности (СОИБ) организаций банковской системы (БС) Республики Абхазия (РА) определено требование проведения оценки рисков нарушения информационной безопасности (ИБ).

Настоящая методика устанавливает рекомендуемые способы и порядок проведения оценки рисков нарушения ИБ организации БС РА, являющейся составной частью системы менеджмента ИБ (СМИБ) организации БС РА.

Положения настоящей методики могут быть использованы для целей внутреннего контроля организаций БС РА.

Периодичность проведения оценки рисков нарушения ИБ, в том числе с использованием положений настоящей методики, определяется организацией БС РА самостоятельно.

1. Область применения

Настоящая методика распространяется на организации БС РА, проводящие оценку рисков нарушения ИБ в рамках построения/совершенствования системы обеспечения информационной безопасности (СОИБ) в соответствии с требованиями СТО БА ИББС-1.0-2009.

Настоящая методика рекомендована для применения путем использования устанавливаемых в ней положений при проведении оценки рисков нарушения ИБ и использовании результатов оценки рисков нарушения ИБ, а также путем включения ссылок на нее и (или) прямого использования содержащихся в ней положений во внутренних документах организации БС РА.

В конкретной организации БС РА для проведения оценки рисков нарушения ИБ могут использоваться иные методики. Результаты использования настоящей методики и иных методик оценки рисков нарушения ИБ имеют равное значение при построении СОИБ организации БС РА.

2. Нормативные ссылки

В настоящей методике использованы нормативные ссылки на стандарт СТО БА ИББС-1.0-2009.

3. Термины и определения

В настоящей методике применены термины по СТО БА ИББС-1.0-2009, в том числе следующие термины (в алфавитном порядке) с соответствующими определениями:

3.1. Априорные защитные меры: защитные меры, эксплуатация которых сокращает качественно или количественно существующие уязвимости объектов защиты информационных активов, тем самым снижая вероятность реализации соответствующих угроз ИБ (например, средства защиты от несанкционированного доступа).

3.2. Апостериорные защитные меры: защитные меры, эксплуатация которых сокращает степень тяжести последствий нарушения свойств ИБ информационных активов (например, средства резервного копирования и восстановления информации).

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

3.4. Информационный актив: информация с реквизитами, позволяющими ее идентифицировать; имеющая ценность для организации БС РА; находящаяся в распоряжении организации БС РА и представленная на любом материальном носителе в пригодной для ее обработки, хранения или передачи форме.

3.5. Источник угрозы информационной безопасности; источник угрозы ИБ: объект или субъект, реализующий угрозы ИБ путем воздействия на объекты среды информационных активов организации БС РА.

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

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

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

3.9. Остаточный риск нарушения информационной безопасности: риск, остающийся после обработки риска нарушения ИБ.

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

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

3.12. Риск нарушения информационной безопасности; риск нарушения ИБ[*]: риск, связанный с угрозой ИБ.

3.13. Угроза информационной безопасности; угроза ИБ: угроза нарушения свойств ИБ - доступности, целостности или конфиденциальности информационных активов организации БС РА.

3.14. Ущерб: утрата активов, повреждение (утрата свойств) активов и (или) инфраструктуры организации или другой вред активам и (или) инфраструктуре организации БС РА, наступивший в результате реализации угроз ИБ через уязвимости ИБ.

4. Общий подход к оценке рисков нарушения ИБ

4.1. Информационные активы организации БС РА рассматриваются в совокупности с соответствующими им объектами среды. При этом обеспечение свойств ИБ для информа-

[*] Риски нарушения ИБ заключаются в возможности утраты свойств ИБ информационных активов в результате реализации угроз ИБ, вследствие чего организации БС РА может быть нанесен ущерб.

ционных активов выражается в создании необходимой защиты соответствующих им объектов среды.

4.2. Угрозы ИБ реализуются их источниками (источниками угроз ИБ), которые могут воздействовать на объекты среды информационных активов организации БС РА. В случае успешной реализации угрозы ИБ информационные активы теряют часть или все свойства ИБ.

4.3. Оценка рисков нарушения ИБ проводится для типов информационных активов (типов информации), входящих в предварительно определенную область оценки. Для оценки рисков нарушения ИБ предварительно определяются и документально оформляются:

- полный перечень типов информационных активов, входящих в область оценки;
- полный перечень типов объектов среды, соответствующих каждому из типов информационных активов области оценки;
- модель угроз ИБ, описывающую угрозы ИБ для всех выделенных в организации БС РА типов объектов среды на всех уровнях иерархии информационной инфраструктуры организации БС РА.

Формирование перечня источников угроз и моделей угроз рекомендуется проводить с учетом положений СТО БА ИББС-1.0, а также перечня основных источников угроз ИБ, приведенных в приложении 1.

4.4. Перечень типов информационных активов формируется на основе результатов выполнения в организации БС РА классификации информационных активов. Состав перечня типов информационных активов (классификация информации) не должен противоречить нормам законодательства РА, в том числе нормативных актов Банка Абхазии.

В качестве примера используется следующий перечень типов информационных активов в организации БС РА:

- информация ограниченного доступа:
- информация, содержащая сведения, составляющие банковскую тайну:
- платежная информация (информация, предназначенная для проведения расчетных, кассовых и других банковских операций и учетных операций);
- информация, содержащая сведения, составляющие коммерческую тайну;
- персональные данные;
- управляющая информация платежных, информационных и телекоммуникационных систем (информация, используемая для технической настройки программно-аппаратных комплексов обработки, хранения и передачи информации);
- открытая (общедоступная) информация.

В конкретной организации БС РА указанный перечень может быть изменен в соответствии с принятыми в ней подходами к классификации информационных активов и уровнем детализации типов информационных активов при проведении оценки рисков нарушения ИБ.

4.5. Формирование перечней типов объектов среды выполняется в соответствии с иерархией уровней информационной инфраструктуры организации БС РА, определенной в СТО БА ИББС-1.0. В частности, указанные перечни могут содержать следующие типы объектов среды:

- линии связи и сети передачи данных;
- сетевые программные и аппаратные средства, в том числе сетевые серверы;
- файлы данных, базы данных, хранилища данных;
- носители информации, в том числе бумажные носители;
- прикладные и общесистемные программные средства;
- программно-технические компоненты автоматизированных систем;
- помещения, здания, сооружения;
- платежные и информационные технологические процессы.

4.6. Риск нарушения ИБ определяется на основании качественных оценок:

- степени возможности реализации угроз ИБ (далее - СВР угроз ИБ) выявленными и (или) предполагаемыми источниками угроз ИБ в результате их воздействия на объекты среды рассматриваемых типов информационных активов;
- степени тяжести последствий от потери свойств ИБ для рассматриваемых типов информационных активов (далее - СТП нарушения ИБ).

4.7. Оценка СВР угроз ИБ и СТП нарушения ИБ базируется на экспертной оценке, выполняемой сотрудниками службы ИБ организации БС РА с привлечением сотрудников подразделений информатизации. Для оценки СТП нарушения ИБ дополнительно привлекаются сотрудники профильных подразделений, использующих рассматриваемые типы информационных активов. Взаимодействие сотрудников указанных подразделений осуществляется в рамках постоянно действующей или создаваемой на время проведения оценки рисков нарушения ИБ рабочей группы.

4.8. К экспертной оценке СВР угроз ИБ и СТП нарушения ИБ привлекаются сотрудники организации БС РА, обладающие необходимыми знаниями, образованием и опытом работы.

4.8.1. Рекомендуется, чтобы эксперты, привлекаемые для оценки СВР угроз ИБ и СТП нарушения ИБ из числа сотрудников службы ИБ или подразделения информатизации организации БС РА, имели:

- знания законодательства РА в области обеспечения информационной безопасности;
- знания международных и национальных стандартов в области обеспечения информационной безопасности;
- знания нормативных актов и предписаний регулирующих и надзорных органов в области обеспечения информационной безопасности;
- знания внутренних документов организации БС РА, регламентирующих деятельность в области обеспечения информационной безопасности;
- знания о современных средствах вычислительной и телекоммуникационной техники, операционных системах, системах управления базами данных, а также о конкретных способах обеспечения информационной безопасности в них;
- знания о возможных источниках угроз ИБ, способах реализации угроз ИБ, частоте реализации угроз ИБ в прошлом;
- знания о способах обеспечения информационной безопасности в платежных, информационных и телекоммуникационных системах организации БС РА;
- понимание различных подходов к обеспечению информационной безопасности, знания защитных мер, свойственных им ограничений.

4.8.2. Рекомендуется, чтобы эксперты, привлекаемые для оценки СТП нарушения ИБ из числа сотрудников профильных подразделений, имели:

- знания законодательства РА в области своей профессиональной деятельности;
- знания нормативных актов и предписаний регулирующих и надзорных органов в области своей профессиональной деятельности;
- знания внутренних документов организации БС РА, регламентирующих их профессиональную деятельность;
- знания бизнес-процессов организации БС РА, а также организации платежных и информационных технологических процессов в области своей профессиональной деятельности;
- понимание степени влияния возможных инцидентов ИБ на функционирование бизнес-процессов организации БС РА в области своей профессиональной деятельности;
- знания о платежных, информационных и телекоммуникационных системах организации БС РА в области своей профессиональной деятельности.

4.8.3. Рекомендуется, чтобы каждый эксперт, привлекаемый для оценки рисков нарушения ИБ, соответствовал следующим характеристикам:

- имел высшее образование;

- четырехлетний опыт постоянной работы в своей профессиональной области;
- поддерживал и совершенствовал собственные знания;
- имел способность идентифицировать в организации БС РА людей, которые могут предоставить необходимую информацию;
- обладал навыками делового и управленческого взаимодействия.

4.8.4. Если работники организации БС РА не обладают необходимыми знаниями и опытом для оценки СВР угроз ИБ, рекомендуется привлекать консультантов или экспертов, которые не являются работниками организации БС РА.

5. Процедуры оценки рисков нарушения ИБ

5.1. Исходными данными для оценки рисков нарушения ИБ является информация, определенная в п. 4.4 настоящей методики.

5.2. Для проведения оценки рисков нарушения ИБ выполняются следующие процедуры.

Процедура 1. Определение перечня типов информационных активов, для которых выполняются процедуры оценки рисков нарушения ИБ (далее - область оценки рисков нарушения ИБ).

Процедура 2. Определение перечня типов объектов среды, соответствующих каждому из типов информационных активов области оценки рисков нарушения ИБ.

Процедура 3. Определение источников угроз для каждого из типов объектов среды, определенных в рамках выполнения процедуры 2.

Процедура 4. Определение СВР угроз ИБ применительно к типам объектов среды, определенных в рамках выполнения процедуры 2.3.

Процедура 5. Определение СТП нарушения ИБ для типов информационных активов области оценки рисков нарушения ИБ.

Процедура 6. Оценка рисков нарушения ИБ.

5.3. Процедура 1. Область оценки рисков нарушения ИБ может быть определена как:

- перечень типов информационных активов организации БС РА в целом;
- перечень типов информационных активов подразделения организации БС РА;
- перечень типов информационных активов, соответствующих отдельным процессам деятельности организации БС РА в целом или подразделения организации БС РА.

5.3.1. Для каждого из типов информационных активов определяется перечень свойств ИБ, поддержание которых необходимо обеспечивать в рамках СОИБ организации БС РА.

Основными свойствами ИБ в рамках настоящей методики являются:

- конфиденциальность;
- целостность;
- доступность.

При необходимости для конкретных типов информационных активов в организации БС РА могут определяться другие (дополнительные) свойства ИБ.

5.3.2. Перечень типов информационных активов области оценки рисков нарушения ИБ и их свойства ИБ документально фиксируются, для чего рекомендуется использовать примерную форму, приведенную в приложении 2.

5.4. Процедура 2. Для каждого из выделенных в рамках выполнения процедуры 1 типов информационных активов составляется перечень типов объектов среды. При составлении данного перечня рассматриваемые типы объектов среды разделяются по уровням информационной инфраструктуры организации БС РА.

Перечень типов объектов среды документально фиксируется, для чего рекомендуется использовать примерную форму, приведенную в приложении 3.

5.5. Процедура 3. Для каждого из определенных в рамках выполнения процедуры 2 типов объектов среды составляется перечень источников угроз, воздействие которых может привести к потере свойств ИБ соответствующих типов информационных активов.

Типы объектов среды и выявляемые для них источники угроз должны соответствовать друг другу в рамках иерархии информационной инфраструктуры организации БС РА.

Перечень источников угроз формируется на основе модели угроз организации БС РА. При этом возможно расширение первоначального перечня источников угроз, зафиксированных в модели угроз организации БС РА (или же его дополнительная структуризация путем составления новых моделей угроз для некоторых из выделенных типов объектов среды или отдельных объектов среды).

При формировании перечня источников угроз рекомендуется рассматривать возможные способы их воздействия на объекты среды, в результате чего возможна потеря свойств ИБ соответствующих типов информационных активов (способы реализации угроз ИБ). Степень детализации и порядок группировки для рассмотрения способов реализации угроз ИБ определяются организацией БС РА.

5.5.1. Результаты выполнения процедуры 3 документально фиксируются, для чего рекомендуется использовать примерную форму документирования данных и результатов оценки СВР угроз ИБ, приведенную в приложении 4 (заполнению подлежат поля: "Тип информационного актива", "Тип объекта среды", "Источник угроз ИБ", "Свойства ИБ типа информационного актива", "Способ реализации угроз ИБ").

5.6. Процедура 4. Для выполнения оценки СВР угроз ИБ используются результаты выполнения процедур 1, 2, 3 настоящей методики и проводится анализ возможности потери каждого из свойств ИБ для каждого из типов информационных активов в результате воздействия на соответствующие им типы объектов среды выделенных источников угроз.

5.6.1. Основными факторами для оценки СВР угроз ИБ являются:

- информация соответствующих моделей угроз, в частности:
- данные о расположении источника угрозы относительно соответствующих типов объектов среды;
- информация о мотивации источника угрозы (для источников угроз антропогенного характера);
- предположения о квалификации и (или) ресурсах источника угрозы;
- статистические данные о частоте реализации угрозы ее источником в прошлом;
- информация о способах реализации угроз ИБ;
- информация о сложности обнаружения реализации угрозы рассматриваемым источником;
- данные о наличии у рассматриваемых типов объектов среды организационных, технических и прочих априорных защитных мер.

5.6.2. Для оценки СВР угроз ИБ используется следующая качественная шкала степеней:

- нереализуемая;
- минимальная;
- средняя;
- высокая;
- критическая.

При привлечении к оценке отдельных СВР угроз ИБ нескольких экспертов и получении разных экспертных оценок рекомендуется итоговую, обобщенную оценку СВР угроз ИБ принимать равной экспертной оценке, определяющей наибольшую СВР угрозы ИБ.

5.6.3. Данные, на основании которых проводится оценка СВР угроз ИБ, и ее результаты документируются, для чего рекомендуется использовать примерную форму документирования данных и результатов оценки СВР угроз ИБ, приведенную в приложении 4 (заполнению подлежат поля: "Используемые априорные защитные меры", "Прочие данные, определяющие СВР угроз ИБ", "Оценка СВР угроз ИБ").

5.7. Процедура 5. Для выполнения оценки СТП нарушения ИБ используются результаты выполнения процедур 1, 2, 3 настоящей методики и проводится анализ последствий потери каждого из свойств ИБ для каждого из типов информационных активов в результа-

те воздействия на соответствующие им типы объектов среды выделенных источников угроз.

5.7.1. Основными факторами для оценки СТП нарушения ИБ являются:

- степень влияния на непрерывность деятельности организации БС РА;
- степень влияния на деловую репутацию;
- объем финансовых и материальных потерь;
- объем финансовых и материальных затрат, необходимых для восстановления свойств ИБ для информационных активов рассматриваемого типа и ликвидации последствий нарушения ИБ;
- объем людских ресурсов, необходимых для восстановления свойств ИБ для информационных активов рассматриваемого типа и ликвидации последствий нарушения ИБ;
- объем временных затрат, необходимых для восстановления свойств ИБ для информационных активов рассматриваемого типа и ликвидации последствий нарушения ИБ;
- степень нарушения законодательных требований и (или) договорных обязательств организации БС РА;
- степень нарушения требований регулирующих и контролирующих (надзорных) органов в области ИБ, а также требований нормативных актов Банка Абхазии;
- объем хранимой, передаваемой, обрабатываемой, уничтожаемой информации, соответствующей рассматриваемому типу объекта среды;
- данные о наличии у рассматриваемых типов объектов среды организационных, технических и прочих апостериорных защитных мер.

5.7.2. Для оценки СТП нарушения ИБ вследствие реализации угроз ИБ используется следующая качественная шкала степеней:

- минимальная;
- средняя;
- высокая;
- критическая.

При привлечении к оценке отдельных СТП нарушения ИБ нескольких экспертов и получении разных экспертных оценок рекомендуется итоговую, обобщенную оценку СТП нарушения ИБ принимать равной экспертной оценке, определяющей наибольшую СТП нарушения ИБ.

5.7.3. Данные, на основании которых проводится оценка СТП нарушения ИБ, и ее результаты документируются, для чего рекомендуется использовать примерную форму документирования данных и результатов оценки СТП нарушения ИБ, приведенную в приложении 5.

5.8. Процедура 6. Оценка рисков нарушения ИБ проводится на основании сопоставления оценок СВР угроз ИБ и оценок СТП нарушения ИБ вследствие реализации соответствующих угроз.

Оценка рисков проводится для всех свойств ИБ выделенных типов информационных активов и всех соответствующих им комбинаций типов объектов среды и воздействующих на них источников угроз.

Для выполнения оценки рисков нарушения ИБ необходимо использовать результаты выполнения процедур 4 и 5 настоящей методики.

5.8.1. Для оценки рисков нарушения ИБ используется следующая качественная шкала:

- допустимый;
- недопустимый.

5.8.2. Для сопоставления оценок СВР угроз ИБ и оценок СТП нарушения ИБ заполняется таблица допустимых/недопустимых рисков нарушения ИБ. Рекомендуемый пример ее заполнения приведен в таблице 1. Оценка рисков нарушения ИБ проводится с учетом данных указанной таблицы.

Таблица 1.

Допустимые/недопустимые риски нарушения информационной безопасности

СВР угроз ИБ	СТП нарушения ИБ			
	минимальная	средняя	высокая	критическая
нереализуемая	допустимый	допустимый	допустимый	допустимый
минимальная	допустимый	допустимый	допустимый	недопустимый
средняя	допустимый	допустимый	недопустимый	недопустимый
высокая	допустимый	недопустимый	недопустимый	недопустимый
критическая	недопустимый	недопустимый	недопустимый	недопустимый

5.8.3. Результаты оценки рисков нарушения ИБ документально фиксируются, для чего рекомендуется использовать примерную форму, приведенную в приложении 6.

6. Оценка рисков нарушения ИБ в количественной (денежной) форме

6.1. Риски нарушения ИБ могут быть оценены в количественной (денежной) форме. Оценка рисков нарушения ИБ в количественной форме проводится с целью формирования резервов на возможные потери, связанные с инцидентами ИБ, и определяется на основании количественных оценок:

- СВР угроз ИБ, выраженной в количественной форме (процентах) (далее - СВР $_{кол}$ угроз ИБ);
- СТП нарушения ИБ, выраженной в количественной (денежной) форме (далее – СТП $_{кол}$ нарушения ИБ).

6.2. Оценки СВР $_{кол}$ угроз ИБ формируются экспертно путем перевода качественных оценок СВР угроз ИБ, полученных в рамках выполнения процедуры 4, в количественную форму в соответствии со следующей рекомендуемой шкалой:

Таблица 2.

Рекомендуемая шкала соответствия СВР угроз ИБ и СВР $_{кол}$ угроз ИБ

Величина СВР угроз ИБ	Величина СВР $_{кол}$ угроз ИБ
Нереализуемая	0%
Минимальная	От 1 до 20%
Средняя	От 21 до 50%
Высокая	От 51 до 100%
Критическая	100%

6.3. Данные, на основании которых проводится оценка СВР $_{кол}$ угроз ИБ, и ее результаты документируются, для чего рекомендуется использовать примерную форму документирования данных и результатов оценки СВР $_{кол}$ угроз ИБ, приведенную в приложении 7.

6.4. Оценки СТП $_{кол}$ нарушения ИБ формируются экспертно путем перевода качественных оценок СТП нарушения ИБ, полученных в рамках выполнения процедуры 5, в количественную форму в соответствии со следующей рекомендуемой шкалой:

Таблица 3.

Рекомендуемая шкала соответствия СТП нарушения ИБ и СТП $_{кол}$ нарушения ИБ

Величина СТП нарушения ИБ	Величина СТП $_{кол}$ нарушения ИБ
Минимальная	До 0,5% от величины капитала организации БС РА
Средняя	От 0,5 до 1,5% от величины капитала организации БС РА
Высокая	От 1,5 до 3,0% от величины капитала организации БС РА
Критическая	Более 3,0% от величины капитала организации БС РА

6.5. Данные, на основании которых проводится оценка СТП $_{кол}$ нарушения ИБ, и ее результаты документируются, для чего рекомендуется использовать примерную форму документирования данных и результатов оценки СТП $_{кол}$ нарушения ИБ, приведенную в приложении 8.

6.6. Количественные оценки рисков нарушения ИБ вычисляются для всех свойств ИБ выделенных типов информационных активов и всех соответствующих им комбинаций объектов среды и воздействующих на них источников угроз путем перемножения оценок СВР $_{кол}$ угроз ИБ и СТП $_{кол}$ нарушения ИБ.

6.7. Результаты количественной оценки рисков нарушения ИБ документально фиксируются, для чего рекомендуется использовать примерную форму, приведенную в приложении 9.

6.8. Суммарная количественная оценка риска нарушения ИБ организации БС РА вычисляется как сумма количественных оценок по всем отдельным рискам нарушения ИБ. Размер резерва на возможные потери, связанные с инцидентами ИБ, рекомендуется принимать равным суммарной количественной оценке риска нарушения ИБ.

7. Заключительные положения

7.1. Настоящие Рекомендации в области стандартизации Банка Абхазии подлежат опубликованию.

7.1. Настоящие Рекомендации в области стандартизации Банка Абхазии вступают в силу с 08.10.2013г.

Председатель
Национального банка
Республики Абхазия **И.Ш. Аргун**

Приложение 1

РЕКОМЕНДУЕМЫЙ ПЕРЕЧЕНЬ
КЛАССОВ, ОСНОВНЫХ ИСТОЧНИКОВ УГРОЗ ИБ И ИХ ОПИСАНИЕ.

Источник угрозы ИБ	Описание
Класс 1. Источники угроз ИБ, связанные с неблагоприятными событиями природного, техногенного и социального характера	
Пожар	Неконтролируемый процесс горения, сопровождающийся уничтожением материальных ценностей и создающий опасность для жизни людей. Возможные причины: поджог, самовозгорание, природное явление
Природные катастрофы, чрезвычайные ситуации и стихийные бедствия	Природные явления разрушительного характера (наводнения, землетрясения, извержения вулканов, ураганы, смерчи, тайфуны, цунами и т.д.).
Техногенные катастрофы	Разрушительный процесс, развивающийся в результате нарушения нормального взаимодействия технологических объектов между собой или с компонентами окружающей природной среды, приводящий к гибели людей, разрушению и повреждению объектов экономики и компонентов окружающей природной среды.
Нарушение внутриклиматических условий	Негативное изменение климатических условий в помещениях, где расположены технические средства и/или находится персонал: значительные изменения температуры и влажности, повышение содержания углекислого газа, пыли и т.п. Возможные последствия: сбои, отказы и аварии технических средств, снижение работоспособности и нанесение ущерба здоровью персонала, нарушение непрерывности выполнения процессов, снижение качества информационных услуг (сервисов)
Нарушение электропитания	Нарушение или снижение качества электропитания. Возможные причины: техногенная катастрофа, стихийное бедствие, природное явление, террористический акт, пожар и т.п. Возможные последствия: сбои и отказы технических средств
Нарушение функционирования систем жизнеобеспечения	Сбои и аварии в системах водоснабжения, канализации, отопления
Угроза здоровью персонала	Угроза здоровью персонала в результате радиационных, биологических, механических, термических, химических и иных воздействий со стороны окружающей среды, объектов инженерной инфраструктуры, технических средств, пищевые отравления, производственный травматизм. Возможные причины: техногенные или природные катастрофы, аварии объектов инженерной инфраструктуры, неисправность оборудования, несоблюдение правил техники безопасности и охраны труда, санитарных правил и т.д. Возможные последствия: нехватка персонала, денежные выплаты, судебные разбирательства
Класс 2. Источники угроз ИБ, связанные с деятельностью террористов и лиц, совершающих преступления и правонарушения	

Нарушения общественного порядка, вандализм, массовые беспорядки, политическая нестабильность	Уничтожение или повреждение имущества организации БС РА
Террористические действия	Совершение взрыва, поджога или иных действий, устрашающих население и создающих опасность гибели людей, причинения значительного имущественного ущерба либо наступления иных тяжких последствий, в целях воздействия на принятие решения организацией БС РА, а также угроза совершения указанных действий в тех же целях
Промышленный шпионаж	Передача, собирание, похищение или хранение информационных активов организации БС РА для использования их в ущерб организации БС РА
Запугивание и шантаж	Принуждение персонала организации БС РА к осуществлению несанкционированных действий, заключающееся в угрозе разоблачения, физической расправы или расправы с близкими
Социальный инжиниринг	Умышленные действия сторонних лиц, преследующих мошеннические цели, реализуемые посредством обмана, введения в заблуждение работников организации БС РА. Возможные последствия: ошибки работников, нарушение свойств, утрата информационных активов, нарушение непрерывности процессов, снижение качества информационных услуг (сервисов)
Класс 3. Источники угроз ИБ, связанные с деятельностью поставщиков/провайдеров/партнеров	
Зависимость от партнеров/клиентов	Зависимость от партнеров заставляет организацию полагаться на их информационную безопасность, организация должна быть уверена, что партнер сможет обеспечить должный уровень безопасности либо учитывать данный источник угроз
Ошибки, допущенные при заключении контрактов с провайдерами внешних услуг	Неточности и неопределенности в договоре с провайдером внешних услуг, которые могут создавать проблемы в работе заказчика
Нарушения договорных обязательств сторонними (третьими) лицами	Невыполнение со стороны третьих лиц взятых на себя обязательств по качеству, составу, содержанию и/или порядку оказания услуг, поставки продукции и т.д. Например, невыполнение требований разработчиками, поставщиками программно-технических средств и услуг или внешними пользователями
Ошибки в обеспечении безопасности информационных систем на стадиях жизненного цикла	Ошибки в обеспечении безопасности при разработке, эксплуатации, сопровождении и выводе из эксплуатации информационных систем
Разработка и использование некачественной документации	Некачественное выполнение документированного описания технологических процессов обработки, хранения, передачи данных, руководств для персонала, участвующего в этих технологических процессах, а также описания средств обеспечения ИБ и руководств по их использованию

Использование программных средств и информации без гарантии источника	Использование в информационной системе организации непроверенных данных или нелицензионного программного обеспечения
Класс 4. Источники угроз ИБ, связанные со сбоями, отказами, разрушениями/повреждениями программных и технических средств	
Превышение допустимой нагрузки	Неумышленное превышение допустимой нагрузки на вычислительные, сетевые ресурсы системы. Выполнение работниками объема операций большего, чем это допускается психофизиологическими нормами. Возможные причины: малая вычислительная и/или пропускная мощность, неправильная организация бизнес-процессов. Возможные последствия: сбои и отказы технических средств, нарушение доступности технических средств, ошибки персонала, нанесение вреда здоровью
Разрушение/повреждение, аварии технических средств и каналов связи	Физическое разрушение/повреждение технических средств (канала связи) или определенное сочетание отказов его элементов, приводящее к нарушениям функционирования, сопряженным с особо значительными техническими потерями, делающее невозможным функционирование технического средства (канала связи) в целом в течение значительного периода времени. Возможные причины: действие внешних (физический несанкционированный доступ, террористический акт, техногенная катастрофа, стихийное бедствие, природное явление, массовые беспорядки) и/или внутренних (значительные отказы элементов технических средств) факторов. Возможные последствия: нарушение свойств информационных активов, их утрата, нарушение непрерывности выполнения процессов, снижение качества информационных услуг (сервисов)
Сбои и отказы программных средств	Нарушение работоспособности программных средств. Возможные причины: недопустимое изменение параметров или свойств программных средств под влиянием внутренних процессов (ошибок) и/или внешних воздействий со стороны вредоносных программ, оператора и технических средств. Возможные последствия: нарушение свойств информационных активов, нарушение непрерывности выполнения процессов, снижение качества информационных услуг (сервисов)
Сбои и отказы технических средств и каналов связи	Прерывание работоспособности технических средств или невозможность выполнения ими своих функций в заранее установленных границах. Возможные причины: недопустимое изменение характеристик технических средств под влиянием внутренних процессов, сложность технических средств, нехватка персонала, недостаточное техническое обслуживание. Возможные последствия: сбои, отказы программных средств, аварии систем, нарушение доступности информационных активов, нарушение непрерывности выполнения процессов, снижение качества информационных услуг (сервисов)

Нарушения функциональности криптографической системы	Случайное или намеренное неправильное управление криптографическими ключами, криптографическими протоколами и алгоритмами, программно-аппаратными средствами систем криптографической защиты информации, приводящее к потере конфиденциальности, целостности и доступности информации, нарушению неотказуемости приема-передачи информации, блокировке функционирования платежных и информационных систем организации БС РА
Нарушения функциональности архивной системы	Нарушение конфиденциальности и целостности архивных данных и/или непредоставление услуг архивной системой (нарушение доступности) вследствие случайных ошибок пользователей или неправильного управления архивной системой, а также вследствие физических воздействий на компоненты архивной системы
Класс 5. Источники угроз ИБ, связанные с деятельностью внутренних нарушителей ИБ	
Недобросовестное исполнение обязанностей	Сознательное неисполнение работниками определенных обязанностей или небрежное их исполнение
Халатность	Неисполнение или ненадлежащее исполнение должностным лицом своих обязанностей вследствие недобросовестного или небрежного отношения к службе
Причинение имущественного ущерба	Умышленное нанесение персоналом вреда информационным активам. В первую очередь вредительство может быть направлено на технические и программные средства, а также на информационные активы. Возможные последствия: ущерб, вызванный нарушением свойств активов, включая их разрушение и уничтожение
Ошибка персонала	Любые не соответствующие установленному регламенту или сложившимся практикам действия персонала, совершаемые без злого умысла. Возможные причины: недостаточно четко определенные обязанности, халатность, недостаточное обучение или квалификация персонала. Возникновению ошибок способствуют отсутствие дисциплинарного процесса и документирования процессов, предоставление избыточных полномочий, умышленное использование методов социального инжиниринга по отношению к персоналу. Возможные последствия: нарушение конфиденциальности и целостности информации, утрата информационных активов, нарушение непрерывности выполнения процессов, снижение качества информационных услуг (сервисов), сбои и отказы технических и программных средств
Хищение	Совершенное с корыстной целью противоправное безвозмездное изъятие и/или обращение имущества организации БС РА, причинившие ущерб собственнику или иному владельцу этого имущества

Выполнение вредоносных программ	Внедрение в систему и выполнение вредоносных программ: программных закладок, "троянских коней", программных "вирусов" и "червей" и т.п. Возможные причины: беспечность, халатность, низкая квалификация персонала (пользователей), наличие уязвимостей используемых программных средств. Возможные последствия: несанкционированный доступ к информационным активам, нарушение их свойств, сбои, отказы и уничтожение программных средств, нарушение непрерывности выполнения процессов, снижение качества информационных услуг (сервисов)
Использование информационных активов не по назначению	Умышленное использование информационных активов организации в целях, отличных от целей организации. Возможные причины: отсутствие контроля персонала. Возможные последствия: нехватка вычислительных, сетевых или людских ресурсов, прямой ущерб организации
Нарушения персоналом организационных мер по обеспечению ИБ	Несоблюдение персоналом требований внутренних документов, регламентирующих деятельность по ИБ
Ошибки кадровой работы	Ошибки кадровой работы заключаются в приеме на работу неквалифицированных сотрудников, увольнении/перемещении сотрудников без проведения сопутствующих процедур по обеспечению ИБ, непроведении или нерегулярном проведении тренингов и проверок персонала
Класс 6. Источники угроз ИБ, связанные с деятельностью внешних нарушителей ИБ	
Действия неавторизованного субъекта	Умышленные действия со стороны субъекта из внешней по отношению к области обеспечения ИБ среды. Возможные последствия: разрушение и уничтожение технических и программных средств, внедрение и выполнение вредоносных программ, нарушение свойств, утрата информационных активов и сервисов
Ложное сообщение об угрозе	Ложное сообщение об угрозе, такой как: пожар, террористический акт, техногенная катастрофа, гражданские беспорядки и т.д. Возможные последствия: нарушение свойств информационных активов, их утрата, нарушение непрерывности выполнения процессов, снижение качества информационных услуг (сервисов)
Неконтролируемое уничтожение информационного актива	Неумышленное уничтожение информационных активов. Возможные причины: сбои оборудования, природные факторы и техногенные катастрофы. Возможные последствия: прямой ущерб организации
Неконтролируемая модификация информационного актива	Неумышленное изменение информационных активов. Возможные причины: сбои оборудования, природные факторы и техногенные катастрофы. Возможные последствия: нарушение непрерывности выполнения процессов, прямой ущерб организации

Несанкционированный логический доступ	Несанкционированный логический доступ неавторизованных субъектов к компонентам подразделения и информационным активам. Возможные причины: компрометация пароля, предоставление пользователям/администраторам избыточных прав доступа, недостатки (отсутствие) механизмов аутентификации пользователей и администраторов, ошибки администрирования, оставление без присмотра программно-технических средств. Одним из путей получения несанкционированного доступа к системе является умышленное внедрение вредоносных программ с целью хищения пароля для входа в систему или получения прав доступа. Возможные последствия: нарушение свойств информационных активов, сбои, отказы и аварии программных и технических средств, нарушение непрерывности процессов и/или снижение качества информационных услуг (сервисов)
Несанкционированный физический доступ	Физический несанкционированный доступ неавторизованных лиц в контролируемую зону расположения технических средств и/или информационных активов. Возможные причины: может осуществляться путем обхода средств контроля физического доступа или использования утраченных/похищенных средств обеспечения доступа. Возможные последствия: разрушение и уничтожение технических и программных средств, нарушение конфиденциальности, целостности, доступности информационных активов, нарушение непрерывности процессов и/или снижение качества информационных услуг (сервисов)
Класс 7. Источники угроз ИБ, связанные с несоответствием требованиям надзорных и регулирующих органов, действующему законодательству	
Несоответствие внутренних документов действующему законодательству	Несоответствие деятельности может привести к административным и уголовным санкциям со стороны судебных, надзорных и регулирующих органов в отношении должностных лиц подразделения, вызвать остановку отдельных видов деятельности
Изменчивость и несогласованность требований надзорных и регулирующих органов, вышестоящих инстанций	Непостоянство, различия и коллизии в содержании требований и/или порядке их выполнения способны дезорганизовать деятельность подразделения или его отдельных служб, снизить ее эффективность и качество, а при определенных обстоятельствах - затруднить ее осуществление. Способствует "размыванию" или пересечению зон ответственности исполнителей и служб, манипуляции со стороны ответственных лиц и служб своими правами и обязанностями в ущерб общей деятельности. Приводит к перераспределению ресурсов в пользу той деятельности (зачастую не основной), за несоблюдение требований к которой наказание наиболее ощутимо для организации (должностного лица)

Приложение 2

ПРИМЕРНАЯ ФОРМА
ДОКУМЕНТИРОВАНИЯ ПЕРЕЧНЯ ТИПОВ ИНФОРМАЦИОННЫХ АКТИВОВ ОБЛАСТИ ОЦЕНКИ РИСКОВ НАРУШЕНИЯ ИБ И ИХ СВОЙСТВ ИБ

На примере заполнения:

тип информационного актива - "Информация ограниченного доступа" (далее - "ДСП информация").

Тип информационного актива	Свойства информационной безопасности			
	конфиденциальность	целостность	доступность	другие свойства ИБ (при необходимости)
"ДСП информация"	+	+	+	-
...				
...				

Примечание.

Свойства ИБ, поддержание которых необходимо обеспечивать в рамках СОИБ организации БС РА для типа информационного актива, обозначаются знаком "+", остальные свойства ИБ - знаком "-".

Приложение 3

ПРИМЕРНАЯ ФОРМА
ДОКУМЕНТИРОВАНИЯ ПЕРЕЧНЯ ТИПОВ ОБЪЕКТОВ СРЕДЫ

На примере заполнения:
тип информационного актива - "ДСП информация".

Тип информационного актива	Уровни иерархии информационной инфраструктуры	Типы объектов среды
"ДСП информация"	Физический уровень	Линии связи, аппаратные и технические средства, физические носители информации
	Сетевой уровень	Маршрутизаторы, коммутаторы, концентраторы
	Уровень сетевых приложений и сервисов	Программные компоненты передачи данных по компьютерным сетям (сетевые сервисы)
	Уровень операционных систем	Файлы данных с "ДСП информацией"
	Уровень систем управления базами данных	Базы данных с "ДСП информацией"
	Уровень банковских технологических приложений и сервисов	Прикладные программы доступа и обработки "ДСП информации", бумажные носители
...		

Приложение 4

ПРИМЕРНАЯ ФОРМА
ДОКУМЕНТИРОВАНИЯ ДАННЫХ И РЕЗУЛЬТАТОВ ОЦЕНКИ СВР УГРОЗ ИБ

На примере заполнения:

тип информационного актива - "ДСП информация";

свойство ИБ - "Конфиденциальность";

способ реализации угрозы - "Несанкционированное копирование";

тип объекта среды - "Файлы данных с ДСП информацией";

источники угроз - "Внутренний нарушитель" и "Внешний нарушитель".

Тип информационного актива	Тип объекта среды	Источник угрозы ИБ	Свойства ИБ типа информационного актива	Способ реализации угроз ИБ*	Используемые априорные защитные меры	Прочие данные, определяющие СВР угроз ИБ	Оценка СВР угроз ИБ
"ДСП информация"	Файлы данных с "ДСП информацией"	Внутренний нарушитель	Конфиденциальность	Несанкционированное копирование	Проведение кадровой работы. Мониторинг и протоколирование доступа к файлам данных. Использование антивирусной защиты	Пользователь, имеющий право доступа к файлам данных имеет возможность совершить противоправное действие	высокая
		...					
		Внешний нарушитель	Конфиденциальность	Несанкционированное копирование	Контроль и протоколирование доступа к файлам данных. Организация физической защиты зданий и помещений. Использование антивирусной защиты	Нет данных	минимальная

Примечание.

В ячейках "Оценка СВР угроз ИБ" требуется указать значение из следующего перечня: нереализуемая; минимальная; средняя; высокая; критическая.

---

* Степень детализации и порядок группировки для рассмотрения способов реализации угроз ИБ определяется организацией БС РА.

Приложение 5

ПРИМЕРНАЯ ФОРМА
ДОКУМЕНТИРОВАНИЯ ДАННЫХ И РЕЗУЛЬТАТОВ ОЦЕНКИ СТП НАРУШЕНИЯ ИБ

На примере заполнения:

тип информационного актива - "ДСП информация";

тип объекта среды - "Файлы данных с ДСП информацией";

источники угроз - "Внутренний нарушитель" и "Внешний нарушитель".

Тип информационного актива	Тип объекта среды	Источник угрозы ИБ	Свойства ИБ типа информационного актива	Используемые апостериорные защитные меры	Прочие данные, определяющие СТП нарушения ИБ	Оценка СТП нарушения ИБ
"ДСП информация"	Файлы данных с "ДСП информацией"	Внутренний нарушитель	Конфиденциальность	Не используются	Нет данных	высокая
			Целостность	Резервирование и контрольное суммирование файлов данных	Нет данных	средняя
			Доступность	Резервирование файлов данных	Нет данных	средняя
			Другие свойства ИБ (при необходимости)			
		...				
		Внешний нарушитель	Конфиденциальность	Не используются	Нет данных	высокая
			Целостность	Резервирование и контрольное суммирование файлов данных	Нет данных	средняя
			Доступность	Резервирование файлов данных	Нет данных	минимальная
			Другие свойства ИБ (при необходимости)			

Примечание.

В ячейках "Оценка СТП нарушения ИБ" требуется указать значение из следующего перечня: минимальная; средняя; высокая; критическая.

Приложение 6

ПРИМЕРНАЯ ФОРМА
ДОКУМЕНТИРОВАНИЯ РЕЗУЛЬТАТОВ ОЦЕНКИ РИСКОВ НАРУШЕНИЯ ИБ

На примере заполнения:

тип информационного актива - "ДСП информация";
свойство ИБ - "Конфиденциальность";
способ реализации угрозы - "Несанкционированное копирование";
тип объекта среды - "Файлы данных с ДСП информацией";
источники угроз - "Внутренний нарушитель" и "Внешний нарушитель".

Тип информационного актива	Тип объекта среды	Источник угрозы ИБ	Свойства ИБ типа информационного актива	Способ реализации угроз ИБ	Оценка СВР угроз ИБ	Оценка СТП нарушения ИБ	Оценка рисков нарушения ИБ
"ДСП информация"	Файлы данных с "ДСП информацией"	Внутренний нарушитель	Конфиденциальность	Несанкционированное копирование	высокая	высокая	недопустимый
		...					
		Внешний нарушитель	Конфиденциальность	Несанкционированное копирование	минимальная	высокая	допустимый

Примечание.

В ячейках "Оценка рисков нарушения ИБ" требуется указать значение из следующего перечня: допустимый; недопустимый.

Приложение 7

ПРИМЕРНАЯ ФОРМА
ДОКУМЕНТИРОВАНИЯ ДАННЫХ И РЕЗУЛЬТАТОВ ОЦЕНКИ СВР $_{кол}$ УГРОЗ ИБ

На примере заполнения:
тип информационного актива - "ДСП информация";
Свойство ИБ - "Конфиденциальность";
способ реализации угрозы - "Несанкционированное копирование";
тип объекта среды - "Файлы данных с ДСП информацией";
источники угроз - "Внутренний нарушитель" и "Внешний нарушитель".

Тип информационного актива	Тип объекта среды	Источник угрозы ИБ	Свойства ИБ типа информационного актива	Способ реализации угроз ИБ	Используемые априорные защитные меры	Прочие данные, определяющие СВР $_{кол}$ угроз ИБ	Оценка СВР $_{кол}$ угроз ИБ
"ДСП информация"	Файлы данных с "ДСП информацией"	Внутренний нарушитель	Конфиденциальность	Несанкционированное копирование	Проведение кадровой работы. Мониторинг и протоколирование доступа к файлам данных. использование антивирусной защиты.	Пользователь, имеющий право доступа к файлам данных, имеет возможность совершить противоправное действие	56%
		Внешний нарушитель	Конфиденциальность	Несанкционированное копирование	Контроль и протоколирование доступа к файлам данных. организация физической защиты зданий и помещений. использование антивирусной защиты.	Нет данных	15%

Приложение 8

ПРИМЕРНАЯ ФОРМА
ДОКУМЕНТИРОВАНИЯ ДАННЫХ И РЕЗУЛЬТАТОВ ОЦЕНКИ
СТП $_{кол}$ НАРУШЕНИЯ ИБ

На примере заполнения:
тип информационного актива - "ДСП информация";
тип объекта среды - "Файлы данных с ДСП информацией";
источники угроз - "Внутренний нарушитель" и "Внешний нарушитель".

Тип информационного актива	Тип объекта среды	Источник угрозы ИБ	Свойства ИБ типа информационного актива	Используемые априорные защитные меры	Прочие данные, определяющие СВР $_{кол}$ угроз ИБ	Оценка СТП $_{кол}$ нарушения ИБ (рубли)
"ДСП информация"	Файлы данных с "ДСП информацией"	Внутренний нарушитель	Конфиденциальность	Не используются	Нет данных	7 млн.
			Целостность	Резервирование и контрольное суммирование файлов данных	Нет данных	4 млн.
			Доступность	Резервирование файлов данных	Нет данных	3 млн.
			Другие свойства ИБ (при необходимости)		Нет данных	
		Внешний нарушитель	Конфиденциальность	Не используются	Нет данных	9 млн.
			Целостность	Резервирование и контрольное суммирование файлов данных	Нет данных	4 млн.
			Доступность	Резервирование файлов данных	Нет данных	0,5 млн.

Приложение 9

ПРИМЕРНАЯ ФОРМА
ДОКУМЕНТИРОВАНИЯ РЕЗУЛЬТАТОВ КОЛИЧЕСТВЕННОЙ ОЦЕНКИ РИСКОВ НАРУШЕНИЯ ИБ

На примере заполнения:

тип информационного актива - "ДСП информация";
свойство ИБ - "Конфиденциальность";
способ реализации угрозы - "Несанкционированное копирование";
тип объекта среды - "Файлы данных с ДСП информацией";
источники угроз - "Внутренний нарушитель" и "Внешний нарушитель".

Тип информационного актива	Тип объекта среды	Источник угрозы ИБ	Свойства ИБ типа информационного актива	Способ реализации угроз ИБ	Оценка СТП $_{кол}$ нарушения ИБ (рубли)	Оценка СВР $_{кол}$ угроз ИБ	Оценка рисков нарушения ИБ
"ДСП информация"	Файлы данных с "ДСП информацией"	Внутренний нарушитель	Конфиденциальность	Несанкционированное копирование	7 млн.	56%	3,92 млн.
		Внешний нарушитель	Конфиденциальность	Несанкционированное копирование	9 млн.	15%	1,35 млн.