РЕКОМЕНДАЦИИ В ОБЛАСТИ
СТАНДАРТИЗАЦИИ
БАНКА РОССИИ

РС БР ИББС-2.5-2014

ОБЕСПЕЧЕНИЕ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ ОРГАНИЗАЦИЙ БАНКОВСКОЙ СИСТЕМЫ РОССИЙСКОЙ ФЕДЕРАЦИИ

МЕНЕДЖМЕНТ ИНЦИДЕНТОВ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ

Дата введения: 2014-06-01

Издание официальное

Москва
2014

Предисловие

1. ПРИНЯТЫ И ВВЕДЕНЫ в действие Распоряжением Банка России от 17 мая 2014 года № Р-400.

Содержание

Введение

Действующим стандартом Банка России “Обеспечение информационной безопасности организаций банковской системы Российской Федерации. Общие положения” (далее — СТО БР ИББС-1.0) с целью создания и поддержания на должном уровне системы обеспечения информационной безопасности (далее — СОИБ) организаций банковской системы (далее — БС) Российской Федерации (далее — РФ) и снижения степени тяжести последствий от нарушений ИБ определены требования к организации обнаружения и реагирования на инциденты информационной безопасности (далее — ИБ).

Настоящие рекомендации в области стандартизации Банка России устанавливают подходы к реализации организацией БС РФ процесса обнаружения и реагирования на инциденты ИБ, являющегося составной частью системы менеджмента ИБ (СМИБ) организации БС РФ.

РЕКОМЕНДАЦИИ В ОБЛАСТИ СТАНДАРТИЗАЦИИ БАНКА РОССИИ

ОБЕСПЕЧЕНИЕ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ ОРГАНИЗАЦИЙ БАНКОВСКОЙ СИСТЕМЫ РОССИЙСКОЙ ФЕДЕРАЦИИ

МЕНЕДЖМЕНТ ИНЦИДЕНТОВ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ

Дата введения: 2014-06-01

1. Область применения

Настоящие рекомендации в области стандартизации Банка России распространяются на организации БС РФ, проводящие деятельность по обнаружению инцидентов ИБ и реагированию на инциденты ИБ в рамках реализации СОИБ в соответствии с требованиями СТО БР ИББС-1.0.

Настоящие рекомендации в области стандартизации Банка России рекомендованы для применения путем прямого использования устанавливаемых в них положений при проведении деятельности по обнаружению инцидентов ИБ и реагированию на инциденты ИБ, а также путем включения ссылок на них и (или) прямого использования содержащихся в них положений во внутренних документах организации БС РФ.

Положения настоящих рекомендаций в области стандартизации Банка России применяются на добровольной основе. В конкретной организации БС РФ для проведения деятельности по обнаружению инцидентов ИБ и реагированию на инциденты ИБ могут использоваться иные рекомендации и (или) требования.

2. Нормативные ссылки

В настоящих рекомендациях в области стандартизации Банка России использованы нормативные ссылки на СТО БР ИББС-1.0.

3. Термины и определения

В настоящих рекомендациях в области стандартизации Банка России применяются термины и определения, установленные СТО БР ИББС-1.0, а также следующие термины и соответствующие определения:

3.1. **Инцидент ИБ** — событие ИБ или их комбинация, указывающие на свершившуюся, предпринимаемую или вероятную реализацию угрозы ИБ, результатом которой являются:

- нарушение в СОИБ организации БС РФ, включая нарушение работы средств защиты информации;
- нарушение требований законодательства Российской Федерации, нормативных актов и предписаний регулирующих и надзорных органов, внутренних документов организации БС РФ в области обеспечения ИБ, нарушение в выполнении процессов СМИБ организации БС РФ;
- нарушение в выполнении банковских технологических процессов организации БС РФ;
- нанесение ущерба организации БС РФ и (или) ее клиентам.

3.2. **Событие ИБ** — изменение состояния объекта или области мониторинга ИБ, действия работников организации БС РФ и (или) иных лиц, которые указывают на возможный инцидент ИБ.

3.3. **Журнал регистрации событий ИБ** — электронный журнал, содержащий записи о событиях ИБ, в том числе о действиях пользователей и эксплуатирующего персонала автоматизированной банковской системы (далее — АБС).

3.4. **Менеджмент инцидентов ИБ** — деятельность по своевременному обнаружению инцидентов ИБ, адекватному и оперативному реагированию на них, направленная на минимизацию и (или) ликвидацию негативных последствий от инцидентов ИБ для организации БС РФ и (или) ее клиентов.

3.5. **Закрытие инцидента ИБ** — действия работников организации БС РФ в рамках реагирования на инцидент ИБ, результатом которых являются:

- устранение нарушений в СОИБ организации БС РФ, реализованных в результате инцидента ИБ;
- устранение последствий угрозы (угроз) ИБ, реализованн(ой)ых в составе инцидента ИБ;
- выяснение причин нетипичного поведения работников организации БС РФ и (или) иных лиц, нештатного функционирования АБС и иных объектов среды информационных активов организации БС РФ, а также нетипичных событий в выполнении банковских технологических процессов.

3.6. **Группа реагирования на инциденты ИБ** (далее — ГРИИБ) — действующая на постоянной основе группа работников организации БС РФ, которая выполняет установленные в организации БС РФ процедуры реагирования на инциденты ИБ.

3.7. **Классификатор инцидентов ИБ** — документ, определяющий способ описания инцидентов ИБ с помощью набора атрибутов — параметров инцидента ИБ.

3.8. **Запись об инциденте ИБ** — элемент централизованной базы данных об инцидентах ИБ, содержащий описание конкретного инцидента ИБ в соответствии с классификатором инцидентов ИБ.

3.9. **Администратор ИБ** — работник организации БС РФ, на которого возложены обязанности по мониторингу ИБ и контролю защитных мер в АБС, аудиту прав и контролю действий пользователей и эксплуатирующего персонала АБС.

3.10. **Распорядитель доступа информационного актива** — руководитель структурного подразделения организации БС РФ или работник организации БС РФ, осуществляющий распоряжение доступом к информационному активу в пределах полномочий, предоставленных организацией БС РФ.

4. Обозначения и сокращения

АБС — автоматизированная банковская система;
БС РФ — банковская система Российской Федерации;
ГРИИБ — группа реагирования на инциденты ИБ;
ИБ — информационная безопасность;
СОИБ — система обеспечения информационной безопасности;
СМИБ — система менеджмента информационной безопасности.

5. Общие положения

5.1. Для реализации, эксплуатации, контроля и поддержания на должном уровне менеджмента инцидентов ИБ организации БС РФ рекомендуется реализовать ряд процессов системы менеджмента инцидентов ИБ, сгруппированных в виде циклической модели Деминга: "...— планирование — реализация — проверка — совершенствование — планирование — ...".

5.2. Планирование в рамках системы менеджмента инцидентов ИБ включает выполнение следующих основных мероприятий:

- разработка и документирование политики менеджмента инцидентов ИБ организации БС РФ;
- определение организационной структуры и ролей процессов реагирования на инциденты ИБ;
- установление и документирование регламентов обнаружения инцидентов ИБ и реагирования на инциденты ИБ;
- выбор технических средств, включая средства защиты информации, необходимых для использования в рамках процессов обнаружения инцидентов ИБ и реагирования на инциденты ИБ, и определение во внутренних документах организации БС РФ порядка эксплуатации указанных технических средств;
- определение порядка осуществления контроля за выполнением процессов обнаружения инцидентов ИБ и реагирования на инциденты ИБ.

5.3. Реализация в рамках системы менеджмента инцидентов ИБ включает выполнение следующих основных мероприятий:

- выделение необходимых ресурсов и назначение ролей для выполнения процессов реагирования на инциденты ИБ;

— проведение мероприятий по обучению и повышению осведомленности работников организации БС РФ, представителей внешних организаций и клиентов организации БС РФ, использующих информационную инфраструктуру организации БС РФ в области обнаружения инцидентов ИБ и реагирования на инциденты ИБ;
— выполнение деятельности по обнаружению инцидентов ИБ и реагированию на инциденты ИБ.

5.4. Анализ в рамках системы менеджмента инцидентов ИБ включает выполнение следующих основных мероприятий:

— анализ действий работников организации БС РФ при выполнении процессов реагирования на инцидент ИБ;
— определение направлений и методов совершенствования СОИБ организации БС РФ на основе результатов выполнения процессов менеджмента инцидентов ИБ;
— определение направлений и методов улучшения процессов менеджмента инцидентов ИБ.

5.5. Совершенствование в рамках системы менеджмента инцидентов ИБ включает выполнение следующих основных мероприятий:

— принятие решений и инициирование совершенствования процессов менеджмента инцидентов ИБ;
— принятие решений и инициирование улучшений в СОИБ организации БС РФ.

Непосредственное выполнение деятельности по совершенствованию процессов менеджмента инцидентов ИБ осуществляется путем планирования и реализации в рамках системы менеджмента инцидентов ИБ.

Выполнение решений по совершенствованию СОИБ организации БС РФ реализуется в рамках тактических и стратегических улучшений, требования к выполнению которых установлены СТО БР ИББС-1.0.

6. Рекомендации по планированию в рамках системы менеджмента инцидентов ИБ

6.1. Рекомендации по разработке и документированию политики менеджмента инцидентов ИБ организации БС РФ

6.1.1. Политика менеджмента инцидентов ИБ организации БС РФ является внутренним документом организации БС РФ, устанавливающим принципы и основные положения, регламентирующие деятельность по менеджменту инцидентов ИБ организации БС РФ.

Политика менеджмента инцидентов ИБ организации БС РФ разрабатывается службой ИБ организации БС РФ совместно и (или) по согласованию с подразделением информатизации организации БС РФ, юридической службой организации БС РФ, подразделениями организации БС РФ, в зоне компетенции которых находятся вопросы обеспечения непрерывности выполнения банковских технологических процессов организации БС РФ, службой персонала (кадров) организации БС РФ и утверждается руководством организации БС РФ.

6.1.2. В политике менеджмента инцидентов ИБ организации БС РФ рекомендуется установить следующие положения:

1. Цель и задачи менеджмента инцидентов ИБ.

Основные цели менеджмента инцидентов ИБ, устанавливаемые политикой менеджмента инцидентов ИБ организации БС РФ, должны определять:

— создание условий для осуществления своевременного обнаружения и оперативного реагирования на инциденты ИБ, в том числе их закрытия;
— предотвращение и (или) снижение негативного влияния инцидентов ИБ на выполнение банковских технологических процессов организации БС РФ и (или) ее клиентов;
— оперативное совершенствование СОИБ организации БС РФ.

Основные задачи, устанавливаемые политикой менеджмента инцидентов ИБ организации БС РФ и решаемые в рамках менеджмента инцидентов ИБ, должны обеспечивать достижение установленных целей менеджмента инцидентов ИБ путем:

— своевременного обнаружения инцидентов ИБ;
— оперативного реагирования на инциденты ИБ в соответствии с требованиями законодательства РФ, нормативных актов Банка России и регламентами, установленными внутренними документами организации БС РФ;
— координации деятельности работников структурных подразделений организации БС РФ в рамках процессов реагирования на инциденты ИБ, в том числе их закрытия;

— ведения базы данных зарегистрированных событий ИБ и обнаруженных инцидентов ИБ;
— накопления и повторного использования знаний по обнаружению инцидентов ИБ и реагированию на них;
— анализа, оценки эффективности и совершенствования процессов менеджмента инцидентов ИБ организации БС РФ;
— предоставления руководству организации БС РФ информации и отчетов по результатам выполнения процессов менеджмента инцидентов ИБ, в том числе информации о фактах обнаружения инцидентов ИБ и результатах реагирования на них.

2. Общее описание состава событий ИБ и критериев классификации событий ИБ как инцидентов ИБ. Описание событий ИБ рекомендуется производить путем формирования перечня типов событий ИБ для каждого из уровней информационной инфраструктуры организации БС РФ, определенных СТО БР ИББС-1.0.

3. Общее описание стадий обнаружения инцидентов ИБ и реагирования на инциденты ИБ, ролей работников организации БС РФ, задействованных на стадиях реагирования на инциденты ИБ, с указанием подразделений организации БС РФ, работникам которых назначаются указанные роли.

Рекомендуется рассматривать следующие стадии обнаружения инцидентов ИБ и реагирования на инциденты ИБ:

— стадия обнаружения, оповещения и оценки, на которой путем анализа события ИБ и установленных в организации БС РФ критериев выявляется инцидент ИБ, производится оповещение уполномоченных работников организации БС РФ, оценка инцидента ИБ, принятие решений о дальнейшем реагировании на инцидент ИБ;
— стадия сбора и фиксации информации, относящейся к инциденту ИБ;
— стадия закрытия инцидента ИБ, в том числе локализации (предотвращение распространения) и восстановления штатного выполнения банковских технологических процессов организации БС РФ, на которой происходит устранение негативных последствий от реализации инцидента ИБ (при их наличии);
— стадия анализа собранной информации, относящейся к инциденту ИБ, и принятие управленческих решений по результатам реагирования на инцидент ИБ.

Стадии сбора и фиксации информации, закрытия инцидента ИБ, анализа информации и принятия управленческих решений в рамках настоящих рекомендаций объединяются общим термином “реагирование на инцидент ИБ”.

4. Общее описание организационной структуры процессов реагирования на инциденты ИБ с указанием:

— состава структурных подразделений организации БС РФ, работникам которых назначаются роли, связанные с реагированием на инциденты ИБ;
— требований к ГРИИБ, в том числе к составу лиц, включаемых в ГРИИБ;
— состава ролей участников процессов реагирования на инциденты ИБ;
— принципов и способов взаимодействия ГРИИБ и работников организации БС РФ в рамках реализации процесса реагирования на инциденты ИБ.

6.2. Рекомендации к определению организационной структуры реагирования на инциденты ИБ

6.2.1. Организационная структура реагирования на инциденты ИБ должна обеспечивать достижение установленных целей менеджмента инцидентов ИБ и решение задач менеджмента инцидентов ИБ во всех структурных подразделениях организации БС РФ. Для этого рекомендуется выделение двухуровневой организационной структуры реагирования на инциденты ИБ — центральной и филиальной (региональной).

6.2.2. На центральном уровне реагирования на инциденты ИБ реализуется выполнение следующих основных задач:

— планирование процессов реагирования на инциденты ИБ организации БС РФ;
— установление регламентов реагирования на инциденты ИБ;
— контроль реализации процессов реагирования на инциденты ИБ организации БС РФ;
— планирование, контроль и координация совместной деятельности ГРИИБ разных уровней;
— обобщенный анализ результатов реагирования на инциденты ИБ;
— выработка предложений по принятию управленческих решений по результатам реагирования на инциденты ИБ;
— выработка предложений по совершенствованию и контроль совершенствования процессов менеджмента инцидентов ИБ;

— обнаружение инцидентов ИБ, реагирование на инциденты ИБ головного (центрального) структурного подразделения организации БС РФ, а также реагирование на инциденты ИБ, которые эскалированы с регионального уровня, в соответствии с установленными в организации БС РФ критериями.

6.2.3. На филиальном (региональном) уровне реагирования на инциденты ИБ реализуется выполнение следующих основных задач:

— планирование мероприятий по реагированию на инциденты ИБ на филиальном (региональном) уровне;
— контроль соблюдения установленных регламентов реагирования на инциденты ИБ на филиальном (региональном) уровне;
— обнаружение инцидентов ИБ, реагирование на инциденты ИБ филиального (регионального) уровня, а также эскалация инцидентов ИБ на центральный уровень в соответствии с установленными в организации БС РФ критериями.

Основу организационной структуры реагирования на инциденты ИБ на каждом из уровней составляет ГРИИБ, создаваемая для каждого из уровней.

6.2.4. ГРИИБ центрального уровня координирует и осуществляет реагирование на инциденты ИБ головного (центрального) структурного подразделения организации БС РФ, координирует и контролирует реагирование на инциденты ИБ регионального уровня в случае их эскалации на центральный уровень. Основу ГРИИБ центрального уровня рекомендуется формировать из представителей службы ИБ организации БС РФ и подразделений информатизации организации БС РФ, обладающих необходимыми полномочиями по выделению работников указанных подразделений для осуществления деятельности по реагированию на инциденты ИБ. Организационную структуру, состав, обязанности и полномочия ГРИИБ центрального уровня рекомендуется определять Положением о ГРИИБ.

6.2.5. ГРИИБ филиального (регионального) уровня координирует и осуществляет реагирование на инциденты ИБ в пределах соответствующего филиала (региона), а в случае отсутствия возможности их обработки с привлечением собственных ресурсов и установленными в организации БС РФ критериями осуществляет их эскалацию в ГРИИБ центрального уровня. Основу ГРИИБ регионального уровня рекомендуется формировать из представителей службы ИБ и подразделений информатизации, обладающих необходимыми компетенциями для реагирования на инциденты ИБ.

Типовую организационную структуру, состав, обязанности и полномочия ГРИИБ регионального уровня рекомендуется определять на центральном уровне типовым Положением о ГРИИБ регионального уровня.

6.3. Рекомендации к определению ролей процесса реагирования на инциденты ИБ

6.3.1. В организации БС РФ рекомендуется определить роли работников, связанные с реагированием на инциденты ИБ, и назначить ответственных за их выполнение. Среди прочего, рекомендуется определить роли, связанные с выполнением деятельности на следующих стадиях:

— стадия оповещения и оценки;
— стадия сбора и фиксации информации;
— стадия закрытия инцидента ИБ;
— стадия анализа и принятие управленческих решений по результатам реагирования на инцидент ИБ.

6.3.2. Ответственных за выполнение ролей в рамках реагирования на инциденты ИБ рекомендуется включать в ГРИИБ. При необходимости ГРИИБ может дополняться внешними экспертами, привлекаемыми на временной основе.

Действия членов ГРИИБ в рамках процесса обработки инцидента ИБ рекомендуется определить соответствующими регламентами реагирования на инциденты ИБ.

6.3.3. Рекомендуется установить следующий состав ролей ГРИИБ:

1. Роль куратора ГРИИБ, который организует и курирует выполнение процессов реагирования на инциденты ИБ, работу ГРИИБ, а также обеспечивает общий контроль достаточности и своевременности выполнения деятельности в организации БС РФ по реагированию на инциденты ИБ.

Среди прочего, куратор ГРИИБ:

— инициирует принятие управленческих решений по результатам реагирования на инциденты ИБ;
— информирует руководство организации БС РФ об обнаруженных инцидентах ИБ и результатах реагирования на них;

— принимает решение о проведении расследований по фактам инцидентов ИБ, а также о необходимости взаимодействия со сторонними организациями и правоохранительными органами в рамках расследования инцидентов ИБ.

Рекомендуется назначать куратора ГРИИБ из числа руководства организации БС РФ.

2. Роль руководителя ГРИИБ, который обеспечивает оперативное руководство реагированием на инциденты ИБ.

Руководителя ГРИИБ рекомендуется наделять административными полномочиями, позволяющими обеспечивать управление и координацию участников процесса реагирования на инциденты ИБ в соответствии с установленными регламентами. В обязанности руководителя ГРИИБ входят:

— инициализация реагирования на инцидент ИБ в ГРИИБ;
— назначение ответственного исполнителя ГРИИБ для реагирования на обнаруженный и зарегистрированный инцидент ИБ;
— координирование деятельности членов ГРИИБ при реагировании на инцидент ИБ;
— привлечение необходимой компетенции в рамках ГРИИБ для реагирования на инцидент ИБ;
— контроль соблюдения требований регламентирующих документов в ходе реагирования на инцидент ИБ;
— принятие решения о возможности закрытия инцидента ИБ;
— предоставление консультаций и рекомендаций участникам процесса реагирования на инциденты ИБ.

Кроме того, к обязанностям руководителя ГРИИБ рекомендуется относить формирование предложений по совершенствованию процессов реагирования на инциденты ИБ и пересмотру соответствующих регламентов.

Руководитель ГРИИБ является основным ответственным за исполнение процесса реагирования на инцидент ИБ, а также за результат исполнения данного процесса.

Рекомендуется назначать руководителя ГРИИБ из числа руководства службы ИБ организации БС РФ.

3. Роль оператора-диспетчера ГРИИБ, который в качестве единой точки входа обеспечивает сбор информации о событиях ИБ и инцидентах ИБ, обнаруженных и (или) имевших место в организации БС РФ.

В обязанности оператора-диспетчера ГРИИБ входят:

— отслеживание (мониторинг) событий ИБ с использованием технических средств мониторинга ИБ;
— сбор информации о событиях ИБ и (или) нетипичных событиях, потенциально имеющих отношение к ИБ, от работников организации БС РФ;
— проведение первичной оценки событий ИБ с целью определения, является ли событие ИБ инцидентом ИБ;
— обеспечение и контроль ведения записей о событиях ИБ;
— в случае классификации событий ИБ в качестве инцидента ИБ регистрация инцидента ИБ и информирование руководителя ГРИИБ и (или) членов ГРИИБ.

4. Роль аналитика ГРИИБ, который обладает необходимой компетенцией и назначается ответственным исполнителем ГРИИБ для реагирования на обнаруженный и зарегистрированный инцидент ИБ.

Аналитик ГРИИБ выполняет следующие основные функции:

— проведение вторичной оценки события ИБ с целью подтвердить, что событие ИБ является инцидентом ИБ, и, в случае такого подтверждения, проведение мероприятий по реагированию на инцидент ИБ и расследованию инцидента ИБ, в том числе сбор и фиксация информации, координирование и контроль закрытия инцидента ИБ;
— оповещение работников организации БС РФ об инциденте ИБ в соответствии с установленными регламентами;
— взаимодействие с оператором-диспетчером ГРИИБ, руководителем ГРИИБ по вопросам реагирования на инцидент ИБ;
— выдвижение предложений о необходимости взаимодействия в рамках расследования инцидентов ИБ со сторонними организациями и правоохранительными органами;
— выдвижение предложений по результатам реагирования на инцидент ИБ, в том числе предложений по совершенствованию СОИБ организации БС РФ, совершенствованию процессов менеджмента инцидентов ИБ, регламентов реагирования на инциденты ИБ, внутренних документов организации БС РФ, связанных с инцидентами ИБ.

Рекомендуется объединять аналитиков ГРИИБ в функциональные группы для решения задач по реагированию на инциденты ИБ определенного вида, например инциденты ИБ, связанные с воздействием вредоносного кода, или инциденты ИБ при осуществлении дистанционного банковского обслуживания.

Рекомендуется назначать аналитиков ГРИИБ из числа работников службы ИБ или работников подразделения информатизации организации БС РФ.

5. Роль секретаря ГРИИБ, основной задачей которого является сбор и анализ информации с целью формирования и предоставления руководителю ГРИИБ и куратору ГРИИБ аналитических отчетов материалов, включая:

— сбор и обобщение сведений об инцидентах ИБ, в том числе событиях ИБ, ошибочно признанных инцидентами ИБ;
— подготовку отчетов о зафиксированных инцидентах ИБ, в том числе событиях ИБ, ошибочно признанных инцидентами ИБ;
— подготовку отчетов о результатах реагирования на инциденты ИБ и расследования инцидентов ИБ.

Ограничений на назначение одному работнику нескольких ролей ГРИИБ в рамках настоящих рекомендаций не устанавливается. В то же время не рекомендуется совмещение в одном лице ролей ГРИИБ и ролей, связанных с разработкой, модернизацией и непосредственной эксплуатацией АБС.

6.3.4. При определении состава ГРИИБ, а также экспертов, привлекаемых к реагированию на инциденты ИБ на временной основе, рекомендуется предусмотреть включение представителей следующих структурных подразделений организации БС РФ:

— служба ИБ организации БС РФ, представители которой участвуют на всех этапах реагирования на инцидент ИБ;
— подразделения информатизации, привлечение представителей которых рекомендуется для оценки влияния (воздействия) инцидентов ИБ на предоставление ИТ-услуг организации БС РФ и для выработки решений по поддержанию и восстановлению ИТ-услуг организации БС РФ в ходе реагирования на инциденты ИБ;
— юридическая служба, привлечение представителей которой следует обеспечить, если есть основания полагать, что инцидент ИБ может иметь правовые последствия, в том числе для участия в сборе доказательной базы, подготовки материалов для правоохранительных органов или для передачи в суд;
— подразделение по связям с общественностью и со средствами массовой информации, привлечение представителей которого следует обеспечить, если есть основания полагать, что возникнет необходимость информирования средств массовой информации и общественности;
— подразделения организации БС РФ, в зоне компетенции которых находятся вопросы обеспечения непрерывности выполнения банковских технологических процессов организации БС РФ, работники которых должны быть осведомлены об инцидентах ИБ и их последствиях. Кроме того, компетенция работников указанных подразделений в минимизации тяжести последствий от нарушений выполнения банковских технологических процессов организации БС РФ при различных обстоятельствах должна быть учтена при планировании действий по реагированию на инциденты ИБ. Необходимо, чтобы регламенты реагирования на инциденты ИБ и регламенты восстановления выполнения банковских технологических процессов организации БС РФ были согласованы и учитывали возможность привлечения работников указанных подразделений к деятельности по реагированию на инциденты ИБ;
— подразделения, в зоне компетенции которых находятся вопросы обеспечения физической безопасности и контроля доступом в здания и помещения организации БС РФ, привлечение представителей которых следует обеспечить, если есть основания полагать, что возникли нарушения физической безопасности или инцидент ИБ включает скоординированные несанкционированные действия по логическому и физическому доступу к защищаемым ресурсам. Кроме того, во время выполнения процедур реагирования на инциденты ИБ членам ГРИИБ может потребоваться предоставление доступа в здания и помещения, для которых установлен отдельный режим доступа;
— служба персонала (кадров) организации БС РФ, привлечение представителей которой следует обеспечить, если есть основания полагать, что в процессе реагирования на инцидент ИБ потребуется применение дисциплинарных мер к работнику организации БС РФ, действия которого привели к реализации инцидента ИБ.

6.4. Рекомендации по установлению и документированию регламентов обнаружения инцидентов ИБ и реагирования на инциденты ИБ

6.4.1. В организации БС РФ рекомендуется установить и документировать регламенты выполнения деятельности на следующих этапах:

— стадия обнаружения и оповещения о событиях ИБ;
— стадия оценки событий ИБ, обнаружения инцидента ИБ и оповещения об инциденте ИБ;
— стадия сбора и фиксации информации об инциденте ИБ;
— стадия закрытия инцидента ИБ.

Указанные регламенты разрабатываются службой ИБ организации БС РФ совместно и (или) по согласованию с подразделением информатизации организации БС РФ, юридической службой организации БС РФ, подразделениями организации БС РФ, в зоне компетенции которых находятся вопросы обеспечения непрерывности выполнения бизнес-процессов организации БС РФ, службой персонала (кадров) организации БС РФ и утверждаются руководством организации БС РФ, например куратором ГРИИБ.

6.4.2. В регламенты обнаружения и оповещения о событиях ИБ рекомендуется включать:

— детальный перечень событий ИБ, при обнаружении которых работники организации БС РФ осуществляют оповещение оператора-диспетчера ГРИИБ;
— детальное описание способов первичного документирования информации о событиях ИБ работниками организации БС РФ, выявившими событие ИБ;
— детальное описание процедур оповещения оператора-диспетчера ГРИИБ и передачи оператору-диспетчеру ГРИИБ документов, содержащих информацию об обнаруженных событиях ИБ;
— детальное описание процедур регистрации оператором-диспетчером ГРИИБ информации об обнаруженном событии ИБ;
— описание порядка хранения информации о событиях ИБ, в том числе в электронном виде.

6.4.3. При формировании перечня событий ИБ рекомендуется осуществлять группирование событий ИБ по уровням информационной инфраструктуры организации БС РФ.

Основными источниками событий ИБ являются:

— технические и программные средства мониторинга ИБ и контроля эксплуатации применяемых защитных мер;
— работники организации БС РФ, выявляющие события ИБ;
— клиенты и партнеры организации БС РФ, включая работников сторонних организаций, имеющих доступ к информационным активам, находящихся под управлением (в распоряжении) организации БС РФ.

6.4.4. В качестве источников информации о событиях ИБ организации БС РФ, формируемых техническими и программными средствами мониторинга ИБ и контроля эксплуатации применяемых защитных мер, рекомендуется использовать:

— регистрационные журналы систем управления, контроля и мониторинга ИБ;
— системные журналы операционных систем;
— системные журналы систем управления базами данных;
— регистрационные журналы прикладного программного обеспечения;
— регистрационные журналы активного сетевого оборудования;
— регистрационные журналы применяемых средств защиты информации, в том числе средств защиты информации от несанкционированного доступа, средств защиты от воздействия вредоносного кода, регистрационные журналы специализированных программно-технических средств обнаружения вторжений и сетевых атак, программного обеспечения проверки целостности файлов;
— информацию специализированных устройств контроля физического доступа, в том числе телевизионных систем охранного наблюдения, систем контроля и управления доступом и охранной сигнализации.

6.4.5. Перечень событий ИБ, выявляемых работниками организации БС РФ, клиентами и партнерами организации БС РФ, составляется экспертным методом и регулярно пересматривается и корректируется, в том числе в связи с возможным появлением новых угроз ИБ, информационных активов, видов деятельности.

Для определения перечня событий ИБ может быть использован примерный перечень типов событий ИБ, приведенный в Приложении 1 к настоящему документу, который рекомендуется скорректировать применительно к специфике деятельности конкретной организации БС РФ.

6.4.6. Способы первичного документирования информации о событиях ИБ должны обеспечивать придание юридической значимости собираемой информации, для чего рекомендуется руководствоваться следующими принципами:

— хранение собранной информации о событиях ИБ должно осуществляться безопасным образом на носителях “только для чтения”;
— при сборе информации о событиях ИБ должны присутствовать не менее двух лиц, действия которых должны протоколироваться;
— необходимо документировать и хранить вместе с собранной информацией описания сервисных команд, использованных для выполнения сбора информации о событиях ИБ;
— целесообразно осуществлять сбор и анализ данных смежных АБС, сервисов и (или) сетей, например, сетевого оборудования и межсетевых экранов.

6.4.7. Рекомендуется определить единую точку входа для информации о событиях ИБ, происходящих в организации БС РФ, которой является оператор-диспетчер ГРИИБ.

Все работники организации БС РФ должны быть ознакомлены с процедурой оповещения о событиях ИБ. Кроме того, в организации БС РФ должны быть определены и выполняться процедуры информирования клиентов и партнеров организации БС РФ о способах оповещения организации БС РФ об обнаруженных событиях ИБ, имеющих отношение к деятельности организации БС РФ.

Все события ИБ, выявляемые работниками организации БС РФ, клиентами и партнерами организации БС РФ, рекомендуется регистрировать с присвоением каждому событию ИБ уникального идентификационного номера.

6.4.8. Рекомендуется обеспечить следующие сроки хранения информации об обнаруженных событиях ИБ:

— событиях ИБ, обнаруженных в рамках банковских платежных технологических процессов, — не менее 5 лет;
— иных событиях ИБ — не менее 3 лет.

6.4.9. В регламенты оценки событий ИБ, обнаружения инцидента ИБ и оповещения об инциденте ИБ рекомендуется включать:

— порядок первичной оценки и критерии классификации событий ИБ в качестве инцидента ИБ;
— порядок использования классификатора инцидентов ИБ и первичной классификации инцидента ИБ;
— порядок оповещения руководителя и членов ГРИИБ об обнаруженном инциденте ИБ;
— порядок и критерии необходимости эскалации инцидента ИБ на центральный уровень реагирования на инциденты ИБ.

6.4.10. Первичная оценка события ИБ и его классификация в качестве инцидента ИБ осуществляется оператором-диспетчером ГРИИБ на основе установленных организацией БС РФ критериев, а также на основе компетентного суждения оператора-диспетчера ГРИИБ.

Вынесение суждения о классификации события ИБ в качестве инцидента ИБ рекомендуется в следующих случаях:

— событие ИБ указывает на нарушение требований законодательства РФ, нормативных актов Банка России, правил платежной системы, внутренних документов организации БС РФ;
— событие ИБ указывает на несанкционированные и (или) нерегламентированные действия в отношении информационных активов организации БС РФ;
— событие ИБ указывает на возможные нарушения в выполнении банковских технологических процессов организации БС РФ;
— событие ИБ указывает на возможное хищение денежных средств и (или) осуществление несанкционированного перевода денежных средств.

6.4.11. Для использования в процессе реагирования на инцидент ИБ рекомендуется определить единую для всех инцидентов ИБ систему их классификации. В случае классификации события ИБ как инцидента ИБ определяются его атрибуты, и далее они используются для управления процессом реагирования на инцидент ИБ и его контроля посредством ведения записи об инциденте ИБ. Порядок определения атрибутов инцидентов ИБ должен быть описан в документе, регламентирующем использование классификатора инцидентов ИБ.

6.4.12. Для оператора-диспетчера ГРИИБ рекомендуется определить детальные и конкретные инструкции оповещения руководителя и членов ГРИИБ об обнаруженном инциденте ИБ, а также эскалации инцидента ИБ на центральный уровень реагирования на инциденты ИБ.

6.4.13. При регламентировании действий целесообразно предусмотреть назначение в каждый момент времени выполнения процесса реагирования на инцидент ИБ ответственного за выполнение соответствующей операции по реагированию из числа членов ГРИИБ.

6.4.14. В регламенты сбора и фиксации информации об инциденте ИБ рекомендуется включать:

— детальное описание источников информации об инциденте ИБ, которые необходимо использовать для сбора информации;
— порядок использования классификатора инцидентов ИБ членами ГРИИБ;
— детальное описание способов документирования и хранения информации об инцидентах ИБ членами ГРИИБ.

6.4.15. Описание источников информации об инциденте ИБ рекомендуется определять для каждого уровня информационной инфраструктуры организации БС РФ на основе перечня источников событий ИБ организации БС РФ, рекомендации к которым установлены в пп. 6.4.3, пп. 6.4.4 настоящих рекомендаций.

6.4.16. Способы документирования информации об инциденте ИБ должны обеспечивать придание юридической значимости собираемой информации, для чего рекомендуется руководствоваться принципами, установленными в пп. 6.4.5 настоящих рекомендаций.

Рекомендуется обеспечить сроки хранения информации об инцидентах ИБ в соответствии с рекомендациями, установленными пп. 6.4.7 настоящих рекомендаций.

6.4.17. В регламенты закрытия инцидента ИБ рекомендуется включать:

— порядок и условия функциональной эскалации инцидента ИБ и (или) привлечения дополнительной компетенции;
— порядок взаимодействия членов ГРИИБ и лиц, привлекаемых к закрытию инцидента ИБ;
— детальное описание способов документирования и хранения информации о результатах реагирования на инцидент ИБ, в том числе закрытия инцидентах ИБ, а также результатах анализа причин инцидента ИБ;
— порядок информирования руководства организации БС РФ о результатах анализа инцидента ИБ;
— порядок подготовки и направления информации об инциденте ИБ, связанном с осуществлением переводов денежных средств, в адрес оператора платежной системы в соответствии с правилами платежной системы и в адрес Банка России в соответствии с требованиями нормативных актов Банка России.

6.5. Рекомендации по выбору технических средств по обнаружению и реагированию на инциденты ИБ и определению порядка их эксплуатации

6.5.1. В состав технических, в том числе программных, средств, используемых в рамках деятельности по обнаружению и реагированию на инциденты ИБ (далее — технические средства), рекомендуется включить:

— технические средства формирования данных, являющихся источниками информации о событиях ИБ и об инцидентах ИБ, в соответствии с рекомендациями, установленными пп. 6.4.4 настоящего документа;
— технические средства централизованного сбора информации о событиях ИБ, корреляции информации о событиях ИБ и обнаружения на основе установленных правил инцидентов ИБ (далее — средства мониторинга ИБ);
— технические средства контроля применяемых в организации БС РФ защитных мер;
— технические средства автоматизации процессов реагирования на инциденты ИБ, включая хранение информации о событиях ИБ и инцидентах ИБ.

6.5.2. Средства мониторинга ИБ и контроля защитных мер должны выполнять следующие основные функции:

— отслеживание и регистрацию событий ИБ в целях обнаружения инцидентов ИБ;
— агрегирование полученной информации о событиях ИБ, корреляцию информации о событиях ИБ, обнаружение инцидентов ИБ на основе установленных в организации БС РФ критериев и правил;
— текущий контроль функционирования применяемых средств защиты информации и обнаружение отклонений в их работе от штатного режима;
— текущий контроль действий пользователей и эксплуатирующего персонала и обнаружение нарушений в эксплуатации технических средств.

6.5.3. Требования к представлению информации о событиях ИБ со стороны компонент информационной инфраструктуры организации БС РФ для ее использования в рамках системы мониторинга ИБ и контроля защитных мер целесообразно формировать на стадии их создания и (или) модернизации.

Для случаев, когда приобретаемое организацией БС РФ прикладное программное обеспечение не обладает функциональными возможностями ведения регистрационных журналов событий ИБ и его доработка не предусмотрена поставщиком, рекомендуется рассмотреть возможность применения компенсирующих функций по формированию информации о событиях ИБ, реализуемых иными компонентами информационной инфраструктуры организации БС РФ, например операционными системами или системами управления базами данных.

6.5.4. Технические средства автоматизации процессов реагирования на инциденты ИБ должны обеспечивать реализацию следующих функций:

— хранение и защиту информации о событиях ИБ и инцидентах ИБ;
— проведение классификации инцидентов ИБ, определение атрибутов инцидентов ИБ в соответствии с применяемым в организации БС РФ классификатором инцидентов ИБ;
— реализацию ролевого доступа к информации об инцидентах ИБ членов ГРИИБ в соответствии с установленными для них ролями в рамках ГРИИБ;
— отслеживание и контроль выполнения этапов реагирования на инцидент ИБ и контроль выполнения членами ГРИИБ установленных регламентов реагирования на инциденты ИБ.

6.5.5. Порядок эксплуатации технических средств должен предусматривать:

— описание состава (количество), мест установки, параметров настроек технических средств;
— описание состава и требований к реализации организационных мер, необходимых для обеспечения эксплуатации технических средств;
— описание правил и процедур эксплуатации технических средств, включая правила и процедуры обновления программного обеспечения технических средств, управления и контроля (мониторинга) параметров их настройки;
— описание ролей и состава функций эксплуатирующего персонала и персонала, осуществляющего контроль эксплуатации технических средств;
— инструкции пользователей и эксплуатирующего персонала, в том числе персонала, осуществляющего контроль эксплуатации технических средств;
— описание правил и процедур контроля доступа эксплуатационного персонала к техническим средствам;
— требования к составу и содержанию организационно-распорядительных документов, необходимых для обеспечения эксплуатации технических средств;
— требования к составу и содержанию организационных мероприятий, необходимых для обеспечения эксплуатации технических средств, в том числе мероприятий по назначению ролей эксплуатирующего персонала, обучению, информированию и повышению осведомленности эксплуатирующего персонала и пользователей;
— описание правил и процедур по обеспечению информационной безопасности при выводе из эксплуатации АБС или по окончании обработки информации.

6.5.6. В организации БС РФ рекомендуется реализовать процедуры контроля соответствия фактических настроек технических средств заданным в эксплуатационной документации. Не рекомендуется наличие субъектов доступа, обладающих единоличными и бесконтрольными возможностями по изменению настроек технических средств. Все действия по изменению настроек технических средств рекомендуется протоколировать и осуществлять под контролем работников службы ИБ по предварительно согласованной программе.

Доступ к информации протоколов изменений настроек технических средств осуществляется только эксплуатирующим персоналом (только чтение), администраторами ИБ и (или) работниками службы ИБ.

6.5.7. В организации БС РФ рекомендуется реализовать процедуры контроля доступа к журналам, содержащим информацию о событиях ИБ и инцидентах ИБ, используемым в соответствии с рекомендациями, установленными пп. 6.4.4 настоящего документа. Управление указанными журналами должно осуществляться уполномоченными работниками службы ИБ.

6.5.8. В организации БС РФ рекомендуется реализовать процедуры обеспечения целостности журналов, содержащих информацию о событиях ИБ и инцидентах ИБ, используемых в соответствии с рекомендациями, установленными пп. 6.4.4 настоящего документа, на случай возможных сбоев в работе и отказов технических и (или) программных средств.

6.5.9. Полный доступ к данным средств мониторинга ИБ предоставляется только уполномоченным членам ГРИИБ и (или) работникам службы ИБ.

6.5.10. С целью обеспечения ИБ при использовании технических средств рекомендуется реализовать:

— запрет несанкционированного доступа к техническим средствам;
— защиту от несанкционированного отключения технических средств;

— защиту от несанкционированного изменения списка событий ИБ, подлежащих регистрации;
— ведения архива файлов с записями информации мониторинга ИБ и журналов регистрации событий ИБ;
— защиту от несанкционированного редактирования или удаления файлов с записями информации мониторинга ИБ и журналов регистрации событий ИБ.

Периодичность архивирования и резервного копирования рекомендуется устанавливать службе ИБ организации БС РФ по согласованию с подразделением информатизации организации БС РФ.

6.5.11. Обязанности по эксплуатации и контролю эксплуатации технических средств рекомендуется отражать в должностных инструкциях работников организации БС РФ.

6.6. Рекомендации по определению порядка осуществления контроля за выполнением процессов обнаружения инцидентов ИБ и реагирования на инциденты ИБ

6.6.1. В организации БС РФ рекомендуется определить регламенты периодического контроля по следующим направлениям:
— контроль выполнения регламентов обнаружения и своевременного оповещения о событиях ИБ;
— контроль актуальности перечня событий ИБ;
— контроль соблюдения принципов первичного документирования информации о событиях ИБ;
— контроль выполнения своевременной оценки событий ИБ, классификации инцидентов ИБ и оповещения об инцидентах ИБ;
— контроль использования классификатора инцидентов ИБ;
— контроль соблюдения регламентов сбора и фиксации информации об инциденте ИБ;
— контроль своевременности принятия мер по закрытию инцидента ИБ, в том числе своевременности эскалации инцидента ИБ и (или) привлечения дополнительной компетенции;
— контроль осведомленности работников организации БС РФ по вопросам обнаружения и реагирования на инциденты ИБ, в том числе осведомленности членов ГРИИБ;
— контроль эксплуатации технических средств.

6.6.2. Организацию контроля за выполнением процессов обнаружения инцидентов ИБ реагирования на инциденты ИБ рекомендуется возложить на куратора ГРИИБ, а непосредственное выполнение контрольных мероприятий на службу ИБ с привлечением работников организации БС РФ — членов ГРИИБ.

7. Рекомендации по реализации в рамках системы менеджмента инцидентов ИБ

7.1. Рекомендации по выделению необходимых ресурсов и назначению ролей в рамках процессов реагирования на инциденты ИБ

7.1.1. В организации БС РФ должно быть организовано назначение следующих ролей:
— ролей, связанных с выполнением задач центрального уровня реагирования на инциденты ИБ;
— ролей, связанных с выполнением задач регионального уровня реагирования на инциденты ИБ;
— ролей членов ГРИИБ;
— ролей работников организации БС РФ, привлекаемых для закрытия инцидентов ИБ;
— ролей работников организации БС РФ, выполняющих функции по эксплуатации технических средств;
— ролей, связанных с выполнением функций по контролю за выполнением процессов обнаружения инцидентов ИБ и реагирования на инциденты ИБ.

7.1.2. Назначение ролей в рамках процессов реагирования на инциденты ИБ рекомендуется осуществлять под общим управлением куратора ГРИИБ.

7.1.3. При распределении и назначении ролей в процессе реагирования на инциденты ИБ рекомендуется учитывать, что для достижения большей эффективности использования персонала необходимо использовать менее квалифицированный персонал для идентификации и

фильтрации ложных сигналов тревоги, обеспечивая при этом привлечение квалифицированного персонала для тех процессов, где требуются его навыки, и только на той стадии процесса, где его содействие необходимо.

7.1.4. Роли должны быть обеспечены всеми необходимыми ресурсами для их выполнения, в том числе:

— регламентами выполнения соответствующей деятельности;
— необходимыми техническими средствами;
— временными и материальными ресурсами, включая помещения, оргтехнику, рабочие места.

7.1.5. Назначение ролей и полномочий для выполнения ролей рекомендуется осуществлять распорядительным актом организации БС РФ, а права доступа к АБС, необходимые для исполнения ролей, предоставлять в соответствии с заявками, утвержденными соответствующими распорядителями доступа к информационным активам.

7.1.6. Взаимодействие структурных подразделений организаций БС РФ в ходе реагирования на инцидент ИБ осуществляется в виде включения представителей структурных подразделений в ГРИИБ, а также путем их привлечения к процессу реагирования на инциденты ИБ. Порядок привлечения работников организации БС РФ к процессу реагирования на инциденты ИБ, включая полномочия привлекаемых работников, должен быть регламентирован.

7.1.7. Взаимодействие структурных подразделений организаций БС РФ в ходе обработки и расследования инцидентов ИБ организует руководитель ГРИИБ, который должен иметь необходимые полномочия.

7.2. Рекомендации по проведению мероприятий по обучению и повышению осведомленности в области обнаружения инцидентов ИБ и реагирования на инциденты ИБ

7.2.1. В организации БС РФ рекомендуется внедрить программу регулярного обучения и повышения осведомленности по следующим основным направлениям:

— повышение осведомленности работников организации БС РФ по вопросам исполнения регламента обнаружения событий ИБ и оповещения о них, в том числе по составу событий ИБ;
— повышение осведомленности представителей внешних организаций и клиентов организации БС РФ, использующих информационную инфраструктуру организации БС РФ, о порядке и процедурах информирования организации БС РФ об обнаруженных инцидентах ИБ;
— обучение и повышение осведомленности членов ГРИИБ и работников организации БС РФ, привлекаемых к реагированию на инциденты ИБ, по вопросам сбора, фиксации и документирования информации об инцидентах ИБ, использования классификатора инцидентов ИБ;
— обучение и повышение осведомленности членов ГРИИБ и работников организации БС РФ, привлекаемых к реагированию на инциденты ИБ, с целью приобретения знаний по технической эксплуатации информационной инфраструктуры организации БС РФ, позволяющих осуществить оперативное закрытие инцидентов ИБ;
— обучение работников подразделений информатизации организации БС РФ по вопросам эксплуатации технических средств;
— обучение работников службы ИБ организации БС РФ по вопросам контроля эксплуатации технических средств.

7.2.2. Рекомендуется ознакомление работников организации БС РФ с процедурой информирования о событиях ИБ, а также о необходимости незамедлительного сообщения об обнаруженных событиях ИБ оператору-диспетчеру ГРИИБ. В процедуры ознакомления рекомендуется включать:

— перечень или описание событий ИБ, о которых требуется сообщать;
— форму сообщения о событиях ИБ, включая детали, существенные для классификации инцидента ИБ, и описание действий по реагированию (например, о типе несоответствия или нарушения, возникновениях неправильных срабатываний, появлении сообщений на экране, нетипичном поведении);
— способы первичного документирования информации о событиях ИБ;
— рекомендации по поведению в случае явных нарушений ИБ, например о выполнении или, наоборот, запрете каких-либо действий, кроме немедленного оповещения оператора-диспетчера ГРИИБ.

7.3. Рекомендации по выполнению деятельности по обнаружению инцидентов ИБ и реагированию на инциденты ИБ

7.3.1. Рекомендуется организовать деятельность по обнаружению и реагированию на инциденты ИБ в соответствии со следующим общим алгоритмом:

- обнаружение событий ИБ, выполняемое работниками организации БС РФ и (или) техническими средствами. Работник организации БС РФ осуществляет первичное документирование информации об обнаруженном событии ИБ и оповещение оператора-диспетчера ГРИИБ в соответствии с установленным регламентом. Для обнаружения событий ИБ работники организации БС РФ используют доведенный до них перечень событий ИБ. Технические средства эксплуатируются в соответствии с документацией, согласованной со службой ИБ организации БС РФ. Информацию о событиях ИБ, выявляемых клиентами и партнерами организации БС РФ, рекомендуется также доводить до оператора-диспетчера ГРИИБ;
- регистрация информации о событиях ИБ, включая сбор информации, связанной с событием ИБ, первичную оценку собранной информации, выполняемые оператором-диспетчером ГРИИБ. Основная задача при первичной оценке — определение, является ли событие ИБ инцидентом ИБ, в частности, произошло ли нарушение ИБ или требований к обеспечению ИБ, установленных для организации БС РФ. Рекомендуется использование технических средств мониторинга ИБ, осуществляющих автоматическое обнаружение инцидентов ИБ из потока информации о событиях ИБ в соответствии с установленными правилами корреляции событий ИБ;
- оповещение членов и (или) руководителя ГРИИБ об инциденте ИБ, выполняемое оператором-диспетчером ГРИИБ. В зависимости от характера инцидента ИБ на основе критериев, установленных в регламенте работы оператора-диспетчера ГРИИБ, оповещается определенный аналитик ГРИИБ, руководитель определенной функциональной группы ГРИИБ и (или) руководитель ГРИИБ;
- вторичная оценка инцидента ИБ, выполняемая аналитиком ГРИИБ с целью подтвердить или опровергнуть то, что обнаруженное событие ИБ является инцидентом ИБ;
- в случае подтверждения того, что обнаруженное событие ИБ является инцидентом ИБ, принятие конкретных мер по закрытию инцидента ИБ, в том числе принятие решения об эскалации инцидента ИБ, устранение нарушения в СОИБ организации БС РФ, прекращение воздействия реализовавшейся угрозы (угроз) ИБ, восстановление выполнения банковских технологических процессов организации БС РФ;
- эскалация инцидента ИБ и привлечение дополнительной компетенции для его обработки. Необходимость эскалации определяет руководитель ГРИИБ и в случае необходимости обращается к куратору ГРИИБ. Эскалация может быть иерархической — если полномочий руководителя ГРИИБ недостаточно для выполнения действий в рамках реагирования на инциденты ИБ, которые, по его мнению, необходимо осуществить (например, прекратить выполнение определенных банковских технологических процессов), а также функциональной — если требуется привлечение специалистов, не входящих в состав ГРИИБ. К иерархической эскалации относится также обращение в ГРИИБ центрального уровня в случае невозможности закрытия инцидента ИБ силами ГРИИБ филиала организации БС РФ или при других обстоятельствах, например в случае невозможности закрытия инцидента ИБ силами ГРИИБ филиала организации БС РФ в установленный срок;
- в случае если инцидент ИБ может привести к судебному разбирательству против лица или организации, а также для проведения дисциплинарных процедур в организации БС РФ вся информация, относящаяся к данному инциденту ИБ, должна быть собрана, сохранена и представлена с целью проведения дальнейшего анализа и возможного принятия судом в качестве доказательства. В зависимости от характера инцидента ИБ желательно максимально полное дублирование журналов о событиях ИБ и об инцидентах ИБ с учетом возможности сохранения необходимости указанных действий и после закрытия инцидента ИБ;
- принятие решения о закрытии инцидента, утверждаемое руководителем ГРИИБ, осуществляемое только после полного восстановления нарушений в СОИБ организации БС РФ, выполнения банковских технологических процессов организации БС РФ, последствий реализации угрозы ИБ, выяснения причин всех проявлений нештатного выполнения бизнес-процессов организации БС РФ и нетипичного поведения работников организации БС РФ.

7.3.2. Управление процессом реагирования на инцидент ИБ, фиксация информации в рамках процесса реагирования на инцидент ИБ осуществляются путем использования классификатора инцидентов ИБ. Классификатор инцидентов ИБ используется для определения и фиксации работниками организации БС РФ, задействованными в деятельности по реагированию на инцидент ИБ, информации об инциденте ИБ (атрибутов инцидента ИБ), выявляемой в процессе реагирования на инцидент ИБ.

7.3.3. Классификатор инцидентов ИБ используется для формализации процесса формирования записи об инциденте ИБ централизованной базы данных об инцидентах ИБ (определения атрибутов инцидента ИБ) на этапах обнаружения инцидента ИБ и реагирования на инцидент ИБ, в том числе при выполнении следующих видов деятельности:

- первичная оценка события ИБ, которая проводится путем определения значений выделенных атрибутов (признаков) инцидента ИБ. Значения этих атрибутов заносятся в создаваемую запись об инциденте ИБ;
- управление процессом оповещения конкретных членов ГРИИБ и руководителя ГРИИБ в зависимости от определенных атрибутов инцидента ИБ;
- принятие решения об эскалации инцидента ИБ в зависимости от определенных атрибутов инцидента ИБ;
- определение значений атрибутов инцидента ИБ работниками организации БС РФ, осуществляющими реагирование на инцидент ИБ;
- определение значений атрибутов инцидента ИБ по результатам закрытия инцидента ИБ;
- фиксация фактов о некорректной (ложной) классификации события ИБ в качестве инцидента ИБ.

7.3.4. При регламентации действий членов ГРИИБ и других работников организации БС РФ, участвующих в реагировании на инциденты ИБ, рекомендуется увязывать эти действия со значениями отдельных атрибутов инцидента ИБ в записи о нем, а также предусматривать ведение записи об инциденте ИБ в соответствии с действующим классификатором инцидентов ИБ.

8. Рекомендации по анализу в рамках системы менеджмента инцидентов ИБ

8.1. В организации БС РФ рекомендуется установить и выполнять процедуры анализа процессов обнаружения инцидентов ИБ и реагирования на инциденты ИБ. Выполнение указанных процедур рекомендуется осуществлять под общим руководством куратора ГРИИБ работникам службы ИБ организации БС РФ.

8.2. Выполнение процедур анализа следует осуществлять на основе:

- результатов проведения контроля за выполнением процессов обнаружения инцидентов ИБ и реагирования на инциденты ИБ;
- анализа статистической отчетности по обнаружению инцидентов ИБ и реагированию на инциденты ИБ;
- анализа записей об инцидентах ИБ, содержащих информацию о нарушениях ИБ, затронутых инцидентом ИБ информационных активах, АБС, степени тяжести последствий от обнаруженных инцидентов ИБ.

8.3. В результате анализа рекомендуется определять наиболее проблемные с точки зрения подверженности инцидентам ИБ сегменты и компоненты информационной инфраструктуры организации БС РФ, наиболее существенные уязвимости и недостатки в обеспечении ИБ, оценивать достаточность принятых мер и выделенных ресурсов для реагирования на инциденты ИБ.

Кроме того, рекомендуется анализировать наличие тенденций, которые могут указывать на потребности в совершенствовании СОИБ организации БС РФ.

8.4. Дополнительному анализу подлежат действия работников организации БС РФ, осуществляемые при реагировании на инциденты ИБ. Целью проведения анализа является формирование (инициирование) совершенствований в части:

- корректировки установленных регламентов обнаружения инцидентов ИБ и реагирования на инциденты ИБ;
- изменения состава ГРИИБ и корректировка состава лиц, привлекаемых к реагированию на инциденты ИБ;
- изменения требований к квалификации членов ГРИИБ;
- корректировки порядка взаимодействия лиц, осуществляющих реагирование на инциденты ИБ;
- корректировки порядка эксплуатации технических средств.

8.5. Результаты анализа обнаружения инцидентов ИБ и реагирования на инциденты ИБ целесообразно использовать в качестве основы для инициирования и реализации процесса проведения тактических и стратегических улучшений СОИБ организации БС РФ, требования к выполнению которого установлены СТО БР ИИБС-1.0.

8.6. Для определения направлений и способов улучшения процессов менеджмента инцидентов ИБ рекомендуется на основе анализа документов и отчетов по инцидентам ИБ провести анализ эффективности применяемых процедур обнаружения инцидентов ИБ и реагирования на инциденты ИБ, в частности:

— оценить адекватность применяемого состава регистрируемых событий ИБ и потребность в его корректировке;
— оценить адекватность используемого классификатора инцидентов ИБ и потребность в его корректировке;
— оценить эффективность используемых процедур мониторинга ИБ;
— оценить адекватность регламентов реагирования на инциденты ИБ.

8.7. При выработке предложений по совершенствованию процессов менеджмента инцидентов ИБ рекомендуется учитывать:

— доступные сведения о соответствующем опыте сторонних организаций;
— изменения в законодательстве РФ, требованиях нормативных актов Банка России, правил платежной системы, внутренних документов организации БС РФ.

8.8. В организации БС РФ рекомендуется установить процедуры информирования руководства организации БС РФ о результатах анализа процессов менеджмента инцидентов ИБ, а также о значимых инцидентах ИБ, оказывающих существенное негативное влияние на выполнение бизнес-процессов организации БС РФ.

9. Рекомендации к классификации инцидентов ИБ и использованию классификатора инцидентов ИБ в процессе их обработки

9.1. Основной целью проведения классификации инцидентов ИБ является повышение степени системности и минимизация субъективности при реализации процессов реагирования на инциденты ИБ, осуществляемые путем определения и фиксации атрибутов инцидента ИБ для дальнейшего их использования в ходе реагирования на инцидент ИБ, а также при анализе системы менеджмента инцидентов ИБ.

9.2. При проведении классификации ИБ рекомендуется осуществлять описание инцидентов ИБ с помощью предварительно установленного набора признаков (атрибутов), при этом значения атрибутов должны задаваться максимально конкретно по определенным правилам.

9.3. Используемый организацией БС РФ классификатор инцидентов ИБ должен давать возможность его адаптации, дополнения, расширения, для чего структура классификатора инцидентов ИБ должна позволять:

— введение дополнительных атрибутов или значений атрибутов;
— проведение классификации вновь обнаруженных инцидентов ИБ без нарушения целостности и изменения установленных процессов классификации.

9.4. Для классификации инцидентов ИБ необходимо определить набор атрибутов, характеризующих инцидент ИБ, для каждого атрибута — значения, которые он может принимать.

Процедура классификации инцидента ИБ состоит в присвоении для конкретного инцидента ИБ соответствующих значений классификационным атрибутам. При этом для конкретного инцидента ИБ могут быть использованы не все атрибуты или значения некоторых атрибутов инцидента ИБ могут определяться постепенно по мере выполнения деятельности по реагированию на него.

9.5. Набор значений атрибутов для конкретного инцидента ИБ представляет собой запись об инциденте ИБ, которая вносится в централизованную базу инцидентов ИБ. Рекомендуется сформировать и поддерживать в актуальном состоянии централизованную базу данных инцидентов ИБ, структуру записей которой рекомендуется задавать на основе классификатора инцидентов ИБ.

9.6. Роли по классификации инцидентов ИБ назначаются членам ГРИИБ и работникам, привлекаемым к реагированию на инциденты ИБ.

9.7. Инциденты ИБ рекомендуется классифицировать по следующим признакам:

— по степени тяжести последствий для деятельности организации БС РФ (в денежном выражении, в балльной шкале);

— по степени вероятности повторного возникновения инцидента ИБ;
— по видам источников угроз ИБ, вызывающих инциденты ИБ;
— по преднамеренности возникновения инцидента ИБ (случайный, намеренный, ошибочный);
— по видам объектов информационной инфраструктуры, задействованных (пораженных) при реализации инцидента ИБ;
— по уровню информационной инфраструктуры, на котором происходит инцидент ИБ;
— по нарушенным свойствам информационной безопасности (конфиденциальность, целостность, доступность);
— по типу инцидента ИБ (свершившийся инцидент ИБ, попытка осуществления инцидента ИБ, подозрение на инцидент ИБ);
— по области распространения и действия инцидента ИБ (в пределах одной АБС, в пределах отдельного структурного подразделения организации БС РФ, в организации БС РФ в целом, выходящий за пределы организации БС РФ);
— по сложности обнаружения инцидента ИБ;
— по сложности закрытия инцидента ИБ;
— по другим признакам, устанавливаемым организацией БС РФ.

9.8. Признаки классификации инцидентов ИБ рекомендуется определять с учетом формирования на основе результатов классификации инцидентов ИБ отчетных форм, представляемых организацией БС РФ в соответствии с требованиями законодательства РФ, нормативных актов Банка России и правилами платежных систем.

9.9. Классификатор инцидентов ИБ рекомендуется использовать на всех этапах обнаружения инцидента ИБ и реагирования на инцидент ИБ. Рекомендуется установить состав атрибутов инцидентов ИБ, возможных для заполнения на каждом из этапов реагирования на инцидент ИБ.

9.10. В Приложении 2 к настоящему документу содержится примерный классификатор инцидентов ИБ.

Приложение 1. Примерный перечень типов событий ИБ

Физический уровень информационной инфраструктуры:

- физический доступ работников организации БС РФ и иных лиц в здания и помещения организации БС РФ;
- физический доступ работников организации БС РФ и иных лиц к средствам вычислительной техники и использование указанными субъектами средств вычислительной техники;
- использование работниками организации БС РФ и иными лицами устройств копирования и многофункциональных устройств;
- использование работниками организации БС РФ и иными лица аппаратов факсимильной связи;
- изменение параметров настроек средств вычислительной техники, телекоммуникационного оборудования;
- изменение параметров настроек оборудования, обеспечивающего функционирование средств вычислительной техники;
- сбои и отказы в работе средств вычислительной техники, телекоммуникационного оборудования;
- сбои и отказы в работе оборудования, обеспечивающего функционирование средств вычислительной техники;
- сбои и отказы в работе средств защиты информации;
- сбои и отказы в работе сети телефонной связи;
- отказы в работе сетей передачи данных;
- физическое воздействие на средства вычислительной техники, телекоммуникационное оборудование, средства защиты информации и сети передачи данных;
- изменения климатических режимов помещений, в которых расположены средства вычислительной техники, телекоммуникационное оборудование;
- изменения параметров функционирования сетей передачи данных;
- замена и (или) модификация программных и (или) аппаратных частей средств вычислительной техники, телекоммуникационного оборудования;
- осуществление действий с носителями информации, в том числе вынос за пределы территории объектов организации БС РФ носителей информации;
- вынос за пределы организации БС РФ переносных средств вычислительной техники;
- использование переносных средств вычислительной техники на территории объектов организации БС РФ;
- передача средств вычислительной техники между подразделениями организации БС РФ;
- передача средств вычислительной техники во внешние организации;
- проведение работниками организации БС РФ и иными лицами фото- и (или) видеосъемки в зданиях или помещениях организации БС РФ;
- проведение мероприятий по доступу к телевизионным системам охранного наблюдения, охранной сигнализации, системам контроля и управления доступом;
- события, формируемые телевизионными системами охранного наблюдения, охранной сигнализации, системами контроля и управления доступом;
- осуществление действий с носителями информации и системами, позволяющими осуществить физический доступ в здания и помещения организации БС РФ.

Уровень сетевого оборудования:

- изменение параметров настроек сетевого оборудования и программного обеспечения сетевого оборудования;
- изменение состава и версий программного обеспечения сетевого оборудования;
- обнаружение аномальной сетевой активности;
- аутентификация и завершение сеанса работы на сетевом оборудовании;
- обнаружение вредоносного кода и его проявлений;
- изменение топологии вычислительных сетей;
- подключение оборудования к вычислительным сетям;
- сбои в работе программного обеспечения сетевого оборудования;
- обновление программного обеспечения сетевого оборудования;
- выполнение операций по техническому обслуживанию сетевого оборудования;
- использование средств анализа уязвимостей сетевого оборудования;
- отключение/перезагрузка сетевого оборудования;
- обнаружение атак типа “отказ в обслуживании”;

— смена и (или) компрометация аутентификационных данных, используемых для доступа к сетевому оборудованию;
— сбои в работе средств защиты информации;
— изменение параметров работы средств защиты информации;
— запуск средств анализа топологии вычислительной сети.

Уровень сетевых приложений и сервисов:

— идентификация, аутентификация, авторизация и завершение сеанса работников организации БС РФ и иных лиц;
— изменение параметров настроек, состава и версий программного обеспечения;
— обнаружение вредоносного кода и его проявлений;
— установление соединений и обработка запросов, в том числе удаленных, на уровне сетевых приложений и сервисов;
— сбои и отказы в работе сетевых приложений и сервисов;
— выполнение операций, связанных с эксплуатацией и администрированием сетевых приложений и сервисов;
— обнаружение нетипичных (аномальных) запросов на уровне сетевых приложений и сервисов;
— отключение/перезагрузка или приостановление работы сетевых приложений и сервисов;
— выполнение операций по предоставлению доступа к использованию сетевых приложений и сервисов, в том числе использованию электронной почты и сети Интернет;
— выполнение операции по архивированию данных сетевых приложений и сервисов, в том числе данных электронной почты;
— осуществление операций по обмену сообщениями, в том числе обмену платежными сообщениями;
— сбои в осуществлении обменом сообщениями, в том числе в обмене платежными сообщениями;
— искажение, модификация сообщений, в том числе платежных сообщений;
— аутентификация сообщений, в том числе платежных сообщений;
— аутентификация автоматизированных рабочих мест — участников обмена сообщениями, в том числе платежными сообщениями;
— завершение/приостановка выполнения сетевых приложений и сервисов по ошибке;
— распространение и (или) сбор информации с использованием сетевых приложений и сервисов;
— выполнение операций со списками рассылки и адресными книгами;
— наделение работников организации БС РФ и (или) иных лиц правами пользователя конкретного пакета сервисов, в том числе сервисов и ресурсов сети Интернет;
— использование средств анализа уязвимостей сетевых приложений и сервисов;
— смена и (или) компрометация аутентификационных данных, используемых для осуществления доступа к сетевым приложениям и сервисам;
— сбои в работе средств защиты информации;
— переадресация сообщений, в том числе платежных сообщений;
— распространение информации, побуждающей клиента сообщать информацию, необходимую для осуществления действий от его имени;
— внешние воздействия из сети Интернет, в том числе сетевые атаки;
— выполнение операций со средствами криптографической защиты информации и ключевой информацией.

Уровень операционных систем:

— аутентификация и завершение работы работников организации БС РФ и иных лиц, в том числе на уровне системного программного обеспечения, систем управления базами данных и прикладного программного обеспечения, программного обеспечения АБС (далее — программное обеспечение уровня операционных систем);
— изменение параметров конфигурации, состава и версий программного обеспечения уровня операционных систем;
— запуск, остановка и (или) отключение/перезагрузка программного обеспечения уровня операционных систем;
— обнаружение вредоносного кода и его проявлений;
— установление соединений и обработка запросов с использованием программного обеспечения уровня операционных систем;

- сбои в работе программного обеспечения уровня операционных систем;
- выполнение операций, связанных с эксплуатацией и администрированием программного обеспечения уровня операционных систем;
- обнаружение нетипичных запросов с использованием программного обеспечения уровня операционных систем;
- сбои и отказы в работе средств защиты информации;
- изменение параметров конфигурации средств защиты информации;
- выполнение операций по предоставлению доступа к программному обеспечению уровня операционных систем и информационным ресурсам, обрабатываемым с использованием программного обеспечения уровня операционных систем;
- выполнение операций по архивированию, резервированию и восстановлению информации;
- завершение/приостановка работы программного обеспечения уровня операционных систем по ошибке;
- использование средств анализа уязвимостей программного обеспечения уровня операционных систем;
- смена и (или) компрометация аутентификационных данных, используемых для доступа к программному обеспечению уровня операционных систем, и информационным ресурсам, обрабатываемым с использованием программного обеспечения уровня операционных систем;
- изменение параметров конфигурации средств защиты информации;
- внешние воздействие из сети Интернет на программное обеспечение уровня операционных систем;
- создание, авторизация, уничтожение или изменение платежной информации;
- создание, уничтожение или изменение информационных ресурсов, баз данных и (или) иных массивов информации;
- компрометация аутентификационных данных и ключевой информации;
- выполнение операций со средствами криптографической защиты информации и ключевой информацией.

Уровень технологических процессов и приложений и уровень бизнес-процессов организации БС РФ:

- выполнение отдельных операций или процедур в рамках банковских платежных и информационных технологических процессов;
- контроль выполнения операций или процедур в рамках банковских платежных и информационных технологических процессов;
- осуществление операций или процедур в рамках банковских платежных и информационных технологических процессов с использованием средств криптографической защиты информации;
- выполнение отдельных этапов жизненного цикла АБС;
- контроль выполнения отдельных этапов жизненного цикла АБС;
- выделение и назначение ролей, в том числе ролей, связанных с обеспечением ИБ.

Приложение 2. Примерный классификатор инцидентов ИБ

Атрибут инцидента ИБ	Описание значений атрибута инцидента ИБ
Группа 1. Атрибуты регистрации	
1.1. Уникальный идентификатор инцидента ИБ	номер или иной идентификатор, позволяющий ссылаться на инцидент ИБ
1.2. Дата и время обнаружения инцидента ИБ	
1.3. Источник информации об инциденте ИБ	работник организации БС РФ или техническое средство
1.4. Фамилия, имя, отчество работника организации БС РФ, выявившего инцидент ИБ	
1.5. Подразделение работника организации БС РФ, выявившего инцидент ИБ	
1.6. Должность работника организации БС РФ, выявившего инцидент ИБ	
1.7. Роль работника организации БС РФ, выявившего инцидент ИБ	(пользователь, администратор АБС, администратор ИБ, работник службы ИБ)
1.8. Контактная информация работника организации БС РФ, выявившего инцидент ИБ	данные, позволяющие связаться с работником
1.9. Наименование технического средства, с использованием которого обнаружен инцидент ИБ	
1.10. Описание инцидента ИБ	сообщение работника или информация, выданная ТС
Группа 2. Атрибуты, описывающие содержание инцидента ИБ	
2.1. Факт нарушения требований к обеспечению ИБ	– “нет”; – “реквизиты документа, пункт документа”
2.2. Данные о нарушителе требований к обеспечению ИБ	– “нет”; – “Фамилия И.О., должность нарушителя”
2.3. Факт нарушения работы средств защиты информации (далее – СЗИ)	– “нет”; – “выход из строя СЗИ”; – “сбой СЗИ”; – “недоступность критичной для выполнения функций СЗИ информации (например, выход из строя носителей ключевой информации)”; – “нарушение целостности программного обеспечения СЗИ”; – “отклонение параметров настроек СЗИ”; – “снижение функциональных характеристик (параметров) СЗИ”
2.4. Факт реализации угрозы ИБ	– “нет”; – “идентификатор источника угрозы согласно модели угроз или действующему перечню актуальных угроз ИБ”
2.5. Факт нарушения свойств безопасности	– “нет”; – “Конфиденциальность”; – “Целостность”; – “Доступность”; – “Иные свойства”
2.6. Факт нестандартного (несанкционированного) поведения	– “нет”; – “нарушение установленного порядка и режима дня”; – “отклонение от сложившегося порядка и режима использования информационных ресурсов”
2.7. Факт преднамеренности возникновения инцидента ИБ	– “случайный”; – “намеренный”; – “ошибочный”
2.8. Тип инцидента ИБ	– “свершившийся”; – “попытка осуществления инцидента ИБ”; – “подозрение на инцидент ИБ”
2.9. Степень сложности обнаружения инцидента ИБ	– “Обычная”; – “Высокая”

Атрибут инцидента ИБ	Описание значений атрибута инцидента ИБ
Группа 3. Атрибуты, описывающие воздействие объекты информационной инфраструктуры	
3.1. Тип информационных активов, затронутых инцидентом ИБ	– “нет” (информационные активы не затронуты); – “платежная информация”; – “финансово-аналитическая информация”; – “служебная информация”; – “управляющая информация общего и специального назначения”; – “справочная информация”; – “информация операционной и телекоммуникационной среды”
3.2. Затронутые объекты информационной инфраструктуры	– “нет”; – “линии и сети передачи данных”; – “сетевые программные и аппаратные средства”; – “прочие технические средства”; – “файлы данных, базы данных”; – “носители информации (в том числе бумажные носители)”; – “прикладные и общесистемные программные средства”; – “программно-технические компоненты автоматизированных систем”; – “помещения, здания, сооружения, инженерные сети и коммуникации”; – “автоматизированные рабочие места”
3.3. Характеристика банковских технологических процессов	– “нет” (нет информационно-технологических процессов, затронутых инцидентом ИБ); – “платежные технологические процессы”; – “информационные технологические процессы”
3.4. Уровень инцидента ИБ	– “физический”; – “сетевой”; – “операционных систем”; – “систем управления базами данных”; – “банковских технологических процессов и приложений”; –”бизнес-процессов организации”
3.5. Степень тяжести последствий	– “нет”; – “минимальная”; – “средняя”; – “высокая”; – “критическая”
3.6. Степень вероятности повторного возникновения инцидента ИБ	– “нет”; – “минимальная”; – “средняя”; – “высокая”; – “критическая”
3.7. Область распространения и действия инцидента ИБ	– “пределы одной АБС”; – “пределы отдельного структурного подразделения организации БС РФ”; – “организации БС РФ в целом”; – “выходящий за пределы организации БС РФ”
Группа 4. Атрибуты, отражающие значимость инцидента ИБ	
4.1. Приоритет инцидента ИБ	– “0 (Наивысший)”; – “1 (Высокий)”; – “2 (Повышенный)”; – “3 (Средний)”; – “4 (Низкий)”; – “5 (Минимальный)”
4.2. Срочность реагирования на инцидент ИБ	– “Обычная”; – “Высокая”
Группа 5. Атрибуты, связанные с реагированием на инцидент ИБ	
5.1. Доклад о возникновении инцидента ИБ	– “нет”; – “время доклада и кому доложено”
5.2. Доклад об устранении инцидента ИБ	– “нет”; – “время доклада и кому доложено”
5.3. Эскалация инцидента ИБ	– “нет”; – “да”
5.4. Функциональная группа	– “нет”; – “наименование функциональной группы специалистов, которой поручено реагирование на инцидент ИБ”

Атрибут инцидента ИБ	Описание значений атрибута инцидента ИБ
5.5. Время назначения функциональной группы	– “нет”; – “время, когда была назначена функциональная группа, ответственная за реагирование на инцидент ИБ”
5.6. Назначение специалиста – члена ГРИИБ	– “нет”; – “фамилия специалиста, ответственного за реагирование на инцидент ИБ”
5.7. Статус инцидента ИБ	– “Зарегистрирован; – “Назначен”; – “В работе”; – “Закрыт”
5.8. Этап реагирования на инцидент ИБ	
5.9. Установленный срок закрытия инцидента ИБ	– “нет”; – “установленный срок закрытия инцидента ИБ”
5.10. Применение иных мероприятий:	– “нет”; – “описание мероприятий по закрытию инцидента ИБ”
5.11. Необходимость информирования об инциденте ИБ структурных подразделений организации БС РФ.	– “нет”; – “перечень подразделений”.
Группа 6. Атрибуты, связанные с закрытием инцидента ИБ	
6.1. Дата и время закрытия инцидента ИБ	– “нет”; – дата и время.
6.2. Последствия (ущерб) для организации БС РФ от воздействия инцидента ИБ	– “нет”; – “описание ущерба (последствий) в текстовой форме”
6.3. Степень сложности закрытия инцидента ИБ	– “Обычная”; – “Высокая”
6.4. Необходимость информирования о закрытии инцидента ИБ структурных подразделений организации БС РФ	– “нет”; – “перечень подразделений”

Библиография

1. Рекомендации в области стандартизации Банка России РС БР ИББС-2.2-2009 “Обеспечение информационной безопасности организаций банковской системы Российской Федерации. Методика оценки рисков нарушения информационной безопасности”.
2. ГОСТ Р ИСО/МЭК ТО 18044-2007 “Информационная технология. Методы и средства обеспечения безопасности. Менеджмент инцидентов информационной безопасности”.

Ключевые слова: банковская система Российской Федерации, система менеджмента информационной безопасности, политика информационной безопасности, инциденты информационной безопасности, менеджмент инцидентов информационной безопасности.