НЕБАНКОВСКАЯ КРЕДИТНАЯ ОРГАНИЗАЦИЯ
«ОБЪЕДИНЕННАЯ РАСЧЕТНАЯ СИСТЕМА»
(открытое акционерное общество)

УТВЕРЖДЕН
Советом Директоров
Протокол № б/н от 17.07.2015 г.

ПОРЯДОК
управления инцидентами информационной безопасности в платежных системах

Оглавление

1. Общие положения

1.1. Порядок управления инцидентами информационной безопасности в платежных системах (далее ПС) определяет основные цели, этапы и задачи управления инцидентами информационной безопасности (далее ИБ) в НКО «ОРС» (ОАО) (далее НКО) являющейся оператором Платежной системы «ОБЪЕДИНЕННАЯ РАСЧЕТНАЯ СИСТЕМА» (далее – ПС ОРС), оператором по переводу денежных средств, оператором услуг платежной инфраструктуры, в том числе в иных платежных системах, устанавливает категории инцидентов информационной безопасности, регламентирует порядок и процедуры управления инцидентами ИБ.

1.2. Настоящий Порядок определяет действия сотрудников НКО по управлению инцидентами ИБ ПС ОРС. Действия участников ПС ОРС по управлению инцидентами ИБ определяются в Операционных правилах Платежной системы «ОБЪЕДИНЕННАЯ РАСЧЕТНАЯ СИСТЕМА» (раздел 10).

1.3. Настоящий Порядок разработан в соответствии с требованиями Положения Банка России от 09.06.2012 № 382-П «О требованиях к обеспечению защиты информации при осуществлении переводов денежных средств и о порядке осуществления Банком России контроля за соблюдением требований к обеспечению защиты информации при осуществлении переводов денежных средств», требованиями Указания Банка России от 11.06.2014 № 3280-У «О порядке информирования оператором платежной системы Банка России, участников платежной системы о случаях и причинах приостановления (прекращения) оказания услуг платежной инфраструктуры», требованиями Указания Банка России от 09.06.2012 № 2831-У «Об отчетности по обеспечению защиты информации при осуществлении переводов денежных средств операторов платежных систем, операторов услуг платежной инфраструктуры, операторов по переводу денежных средств» и рекомендациями Стандарта Банка России РС БР ИББС-2.5-2014 от 01.06.2014 «Менеджмент инцидентов информационной безопасности».

2. Термины и сокращения

2.1. Применяемые сокращения:

- **АБС —** автоматизированная банковская система;
- **ГРИИБ —** группа реагирования на инциденты ИБ;
- **ИА —** информационный актив;
- **ИБ —** информационная безопасность;
- **ПС ОРС —** Платежная система «ОБЪЕДИНЕННАЯ РАСЧЕТНАЯ СИСТЕМА»;
- **СОИБ —** система обеспечения информационной безопасности;
- **СМИБ —** система менеджмента информационной безопасности.

2.2. Используемые термины:

- **Банковский технологический процесс:** технологический процесс, содержащий операции по изменению и (или) определению состояния банковской информации, используемой при функционировании НКО или необходимой для реализации банковских услуг.
- **Информационная безопасность:** состояние защищенности интересов и целей НКО в условиях наличия угроз в отношении ее ИА.
- **Информационный актив:** информация с реквизитами, позволяющими ее идентифицировать; имеющая ценность для НКО, находящаяся в распоряжении НКО и представленная на любом материальном носителе в пригодной для ее обработки, хранения или передачи форме.
- **Инцидент ИБ ПС**: события, которые возникли вследствие нарушения требований к обеспечению защиты информации при осуществлении переводов денежных средств и (или) условий перевода денежных средств, которые:

- привели к несвоевременности (к нарушению сроков) осуществления переводов денежных средств;
- привели или могут привести к осуществлению переводов денежных средств по распоряжению лиц, не обладающих правом распоряжения этими денежными средствами;
- привели к осуществлению переводов денежных средств с использованием искаженной информации, содержащейся в распоряжениях участников платежной системы, распоряжениях клирингового центра.

- **Событие ИБ**: изменение состояния объекта или области мониторинга ИБ, действия сотрудников НКО и (или) иных лиц, которые указывают на возможный инцидент ИБ.
- **Журнал регистрации событий ИБ**: электронный журнал, содержащий записи о событиях ИБ ПС ОРС.
- **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 ПС.
- **Закрытие инцидента ИБ**: действия сотрудников НКО в рамках реагирования на инцидент ИБ, результатом которых являются:
  - устранение нарушений в СОИБ ПС, реализованных в результате инцидента ИБ ПС;
  - устранение последствий угроз ИБ, реализованных в составе инцидента ИБ ПС;
  - выяснение причин нетипичного поведения сотрудников НКО и (или) иных лиц, нештатного функционирования АБС и иных объектов среды информационных активов НКО, а также нетипичных событий в выполнении банковских технологических процессов.
- **Группа реагирования на инциденты ИБ**: действующая на постоянной основе группа сотрудников НКО, которая выполняет установленные в НКО процедуры реагирования на инциденты ИБ.
- **Классификатор инцидентов ИБ**: документ, определяющий способ описания инцидентов ИБ с помощью набора атрибутов – параметров инцидента ИБ (Приложение № 1).
- **Запись об инциденте ИБ**: элемент централизованной базы данных об инцидентах ИБ, содержащий описание конкретного инцидента ИБ в соответствии с классификатором инцидентов ИБ.

3. Цели, этапы и задачи управления инцидентами ИБ

3.1. Целями управления инцидентами ИБ являются:

- минимизация операционных рисков и негативного влияния инцидентов ИБ на деятельность НКО и ПС, включая ПС ОРС;
- восстановление нормальной работоспособности НКО и ПС, включая ПС ОРС, в максимально короткие сроки;
- обеспечение выработки превентивных защитных мер по предотвращению реализации угроз ИБ НКО и ПС, включая ПС ОРС.

3.2. Процесс управления инцидентами ИБ подразделяется на следующие четыре этапа, в рамках которых решаются соответствующие задачи:

- этап «Планирование»;
- этап «Реализация»;
- этап «Анализ»;

- этап «Совершенствование».

3.2.1. «Планирование» включает выполнение следующих основных мероприятий:
- разработка и утверждение нормативных документов по управлению инцидентами ИБ;
- определение организационной структуры и ролей при реагировании 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 НКО порядка эксплуатации указанных технических средств;
- определение порядка осуществления контроля за выполнением процессов обнаружения инцидентов ИБ и реагирования на инциденты ИБ.

3.2.2. «Реализация» включает выполнение следующих мероприятий:
- проведение ознакомления сотрудников НКО с настоящим Порядком для повышения осведомленности в области управления инцидентами ИБ;
- выявление событий ИБ и оповещение (информирование) о них;
- оценка и принятие решения: является ли выявленное событие инцидентом ИБ;
- реагирование на инциденты ИБ.

3.2.3. «Анализ» включает выполнение следующих мероприятий:
- анализ действий сотрудников НКО при выполнении процессов реагирования на инцидент ИБ;
- анализ статистической отчетности по выявлению инцидентов ИБ и реагированию на инциденты ИБ от участников ПС ОРС;
- анализ записей об инцидентах ИБ, содержащих информацию о нарушениях ИБ, затронутых инцидентом ИБ информационных активах, АБС, степени тяжести последствий от обнаруженных инцидентов ИБ;
- определение направлений и методов совершенствования СОИБ НКО на основе результатов выполнения процессов управления инцидентами ИБ;
- определение направлений и методов улучшения самих процессов управления инцидентами ИБ.

3.2.4. «Совершенствование» включает выполнение следующих мероприятий:
- принятие решений и инициирование совершенствования процессов управления инцидентами ИБ;
- принятие решений и инициирование улучшений в СОИБ НКО;
- разработка дополнительных регламентов и инструкций для работы сотрудников НКО.

4. Организационная структура по управлению инцидентами ИБ

4.1. Группа реагирования на инциденты ИБ.

Организацию деятельности по управлению инцидентами ИБ осуществляет ГРИИБ.

В НКО в ГРИИБ входят:

- Технический директор;

- Служба информационной безопасности;
- Служба информационных технологий (далее Служба ИТ).

На ГРИИБ возлагаются следующие функции:

- планирование процессов реагирования на инциденты ИБ НКО;
- установление регламентов реагирования на инциденты ИБ;
- контроль реализации процессов реагирования на инциденты ИБ НКО;
- обнаружение инцидентов ИБ, реагирование на инциденты ИБ НКО;
- регистрация инцидентов ИБ в журнале регистрации;
- реагирование на инциденты ИБ, о которых проинформировали участники ПС ОРС, если требуется вмешательство НКО;
- закрытие инцидентов ИБ;
- обобщенный анализ результатов реагирования на инциденты ИБ;
- выработка предложений по принятию управленческих решений по результатам реагирования на инциденты ИБ;
- выработка предложений и инициирование улучшений в СОИБ НКО;
- выработка предложений по совершенствованию и контроль совершенствования процессов управления инцидентами ИБ.

5. Классификация инцидентов ИБ

5.1. Инциденты ИБ могут быть преднамеренными или случайными и могут быть вызваны как техническими, так и нетехническими средствами.

5.2. Источниками информации о событиях и инцидентах ИБ могут быть:

- сообщения непосредственно от сотрудников НКО (Управление расчетов, Управление по работе с клиентами);
- сообщения от Службы ИТ НКО;
- системные журналы и оповещения АБС;
- участники ПС, включая ПС ОРС, операторы ПС и их операционные центры.

5.3. В НКО выделяются следующие основные **категории** инцидентов ИБ:

- несвоевременность переводов денежных средств;
- несанкционированный перевод денежных средств или угроза такого события;
- перевод денежных средств с использованием искаженной информации, содержащейся в распоряжениях участников ПС.

5.4. Инциденты ИБ внутри категорий **классифицируются** по следующим признакам:

- по степени тяжести последствий для деятельности ПС, включая ПС ОРС, (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);

- по области распространения и действия инцидента ИБ (в пределах АБС НКО, в пределах операционного центра ПС, включая ПС ОРС, в пределах одного участника ПС, включая ПС ОРС, в пределах всей ПС, включая ОРС);
- по сложности обнаружения инцидента ИБ;
- по сложности закрытия инцидента ИБ.

6. Порядок управления инцидентами ИБ ПС, включая ПС ОРС

6.1. Процедуры управления инцидентами ИБ

6.1.1. Процесс управления инцидентами ИБ осуществляется на основе выполнения следующих процедур;
- обеспечение осведомленности сотрудников в области управления инцидентами ИБ;
- обнаружение и оповещение (информирование) о событии (инциденте) ИБ;
- регистрация и сбор данных о событии (инциденте) ИБ;
- оценка инцидента ИБ и нанесенного им ущерба;
- реагирование на инцидент ИБ;
- анализ инцидента ИБ и оценка результатов реагирования на него;
- реализация улучшений системы управления инцидентами ИБ.

6.2. Обеспечение осведомленности Сотрудников в области ИБ ПС ОРС

6.2.1. Осведомленность персонала НКО по управлению инцидентами ИБ обеспечивается ознакомлением под роспись с настоящим Порядком после его разработки, а также после его пересмотра.

6.3. Обнаружение и оповещение о событии ИБ ПС, включая ПС ОРС

6.3.1. События ИБ ПС, включая ПС ОРС, могут быть обнаружены сотрудником НКО, сотрудником участника ПС, включая ПС ОРС, сотрудником операционного центра ПС, включая ПС ОРС. Технические события ИБ могут обнаруживаться автоматически: устройствами анализа записей аудита, межсетевыми экранами, системами обнаружения вторжений, антивирусными программами.

6.3.2. Сотрудник НКО, обнаружив событие, попадающее под категорию событий ИБ ПС, включая ПС ОРС, (5.3 настоящего Порядка), оповещает членов ГРИИБ по электронной почте, подробно описав событие в свободной форме. Также, сотрудник НКО, получивший информацию о событии ИБ ПС, включая ПС ОРС, от участника или операционного центра ПС, включая ПС ОРС, оповещает членов ГРИИБ по электронной почте.

6.4. Регистрация и сбор данных о событии (инциденте) ИБ

Руководитель ГРИИБ оперативно анализирует зарегистрированное событие ИБ, а затем должен получить любые уточнения у сотрудника, приславшего сообщение о событии ИБ, и собрать и сохранить требуемую дополнительную информацию, являющуюся доступной. В ходе сбора дополнительной информации может также задокументировать следующие сведения:
- проведенные мероприятия, включая использованные средства;
- способ верификации свидетельств (если применимо);
- места хранения свидетельств наличия события ИБ;
- детали хранения материалов и последующего доступа к ним.

Информация и другие свидетельства, собранные и сохраненные на этом этапе, могут потребоваться в будущем для дисциплинарного или судебного разбирательства.

6.5. Оценка инцидента ИБ и нанесенного им ущерба ПС, включая ПС ОРС

Подтверждение и оценка инцидента ИБ входят в обязанности членов ГРИИБ и должна быть выполнена в возможно кратчайшие сроки.

Если по результатам рассмотрения имеющейся информации событие ИБ определяется членами ГРИИБ как ложная тревога, то об этом Руководитель ГРИИБ информирует сотрудника, сообщившего о событии ИБ, по электронной почте.

Если члены ГРИИБ рассматривают обнаруженное событие ИБ как реальный инцидент ИБ, то ими в максимально сжатые сроки осуществляется дальнейшая оценка инцидента ИБ ПС, включая ПС ОРС:

- инцидент ИБ ПС классифицируется по критериям 5.4;
- атрибуты классификации заносятся в БД инцидентов.

6.6. Реагирование на инцидент ИБ

6.6.1. Немедленные действия, в случае если инцидент ИБ произошел в НКО

После подтверждения инцидента ИБ члены ГРИИБ обеспечивают выполнение действий по немедленному реагированию на инцидент ИБ, регистрации подробностей в БД инцидентов ИБ и уведомлению сотрудников о требуемых действиях по инциденту ИБ.

Если критичность инцидента ИБ признается высокой, то руководитель ГРИИБ незамедлительно уведомляет об инциденте ИБ непосредственно Председателя Правления НКО.

В случае выявления чрезвычайной ситуации, руководителем ГРИИБ принимаются меры по активации «Плана действий, направленных на обеспечение непрерывности деятельности и (или) восстановление деятельности НКО «ОРС» (ОАО) в случае возникновения нестандартных и чрезвычайных ситуаций» (далее по тексту - План ОНиВД).

При выполнении действий по немедленному реагированию членам ГРИИБ необходимо учитывать следующие факторы:

- при принятии соответствующего решения необходимо оценить техническую возможность быстро и надежно отключить атакованную АБС, сервис и (или) сеть;
- предотвращение повторного появления инцидента ИБ является приоритетной задачей, поскольку нарушитель выявил слабое место, которое необходимо оперативно устранить;
- необходимость обеспечить сохранность и должное оформление доказательств;
- при проведении исследования источников информации нужно обеспечить неизменность доказательств, следует работать только с их копиями и хранить всю собранную информацию на носителях, доступных только для чтения.

Когда инцидент ИБ разрешен, то обновляется запись об инциденте в БД (журнале) инцидентов ИБ.

6.6.2. Дополнительные действия

При определении членами ГРИИБ реальности инцидента ИБ их дополнительными действиями также могут быть:

- проведение правовой экспертизы;

Если была определена необходимость правовой экспертизы в целях оценки инцидента ИБ, то вся собранная информация передается руководителем ГРИИБ в Юридическую службу НКО.

6.6.3. Информирование Банка России об инцидентах ИБ ПС, включая ПС ОРС

НКО информирует Банк России в лице его территориального учреждения, осуществляющего надзор за его деятельностью (далее - уполномоченное учреждение Банка России), о случаях и причинах приостановления (прекращения) оказания услуг платежной инфраструктуры посредством направления сообщения на бумажном носителе или электронного сообщения, снабженного кодом аутентификации, в течение двух рабочих дней со дня приостановления (прекращения) оказания услуг платежной инфраструктуры. При этом НКО в день приостановления (прекращения) оказания услуг платежной инфраструктуры незамедлительно должна направить в уполномоченное учреждение Банка России уведомление о приостановлении (прекращении) оказания услуг платежной инфраструктуры с использованием способа связи, информация о котором доведена до него уполномоченным учреждением Банка России.

Обо всех инцидентах ИБ ПС, включая ПС ОРС, направляется в территориальное учреждение Банка России отчетность по форме 0403203 «Сведения о выявлении инцидентов, связанных с нарушением требований к обеспечению защиты информации при осуществлении переводов денежных средств» в порядке и сроки, определенные в нормативных документах Банка России,

6.6.4. Информирование участников и операционных центров ПС ОРС об инцидентах ИБ ПС ОРС.

В случае если инцидент ИБ ПС ОРС затрагивает всех участников и операционные центры ПС ОРС, информация об инциденте ИБ размещается на сайте ПС ОРС.

В случае если инцидент ИБ ПС ОРС затрагивает часть участников и операционных центров ПС ОРС, НКО информирует указанных субъектов ПС ОРС по электронной почте.

6.6.5. Информирование Руководства НКО об инцидентах ИБ ПС, включая ПС ОРС

О произошедших инцидентах ИБ, их последствиях и предлагаемых мерах по совершенствованию СОИБ НКО по результатам анализа инцидентов ИБ начальник Службы ИБ докладывает Председателю Правления НКО в составе ежеквартального Отчета по состоянию СОИБ НКО.

6.6.6. Информирование операторов иных ПС об инцидентах ИБ в НКО

В случае если инцидент ИБ в НКО затрагивает иную ПС, НКО информирует иную ПС в соответствии с правилами иной ПС.

6.7. Анализ инцидентов ИБ

6.7.1. Общие положения

После принятия решения о закрытии инцидента ИБ необходимо провести дальнейшую правовую экспертизу и анализ с целью определения извлеченных уроков и потенциальных улучшений ИБ и системы управления инцидентами ИБ.

6.7.2. Дальнейшая правовая экспертиза

В случае необходимости проведения дополнительной правовой экспертизы инцидента ИБ после его закрытия, ГРИИБ организует ее проведение в соответствии с положениями п. 6.6.2 настоящего Порядка.

6.7.3. Извлеченные уроки

После завершения инцидента ИБ важно быстро идентифицировать уроки, извлеченные из его обработки, и предпринять соответствующие действия, которые могут рассматриваться с точки зрения:

- новых или изменившихся требований к мерам защиты для обеспечения ИБ;

- изменений в системе управления инцидентами ИБ и ее процедурах, формах отчета и БД инцидентов ИБ.

6.7.4. Определение улучшений безопасности

В процессе анализа, проведенного после разрешения инцидента ИБ, могут быть определены новые необходимые защитные меры. Выработанные рекомендации и соответствующие им требования к защитным мерам реализуются на основе планов мероприятий по совершенствованию СОИБ.

Если инцидент ИБ имел высокую критичность или являлся ЧС, то Руководитель ГРИИБ после его разрешения проводит совещание всех заинтересованных лиц, владеющих информацией о нем. На совещании рассматриваются следующие вопросы:

- работали ли должным образом процедуры, принятые в системе управления инцидентами ИБ;
- существуют ли процедуры или методы, которые способствовали бы обнаружению инцидентов ИБ;
- были ли определены процедуры или средства, которые использовались бы в процессе реагирования;
- применялись ли процедуры, помогающие восстановлению АБС после идентификации инцидента ИБ;
- была ли передача информации об инциденте ИБ всех причастных сторон эффективной в процессе обнаружения, информирования и реагирования.

Результаты совещания документируются и учитываются при подготовке Плана мероприятий по совершенствованию СОИБ.

6.8. Реализация улучшений системы управления инцидентами ИБ

Этап улучшения системы управления инцидентами ИБ основывается на рекомендациях, сформированных в ходе этапа анализа инцидентов ИБ.

В зависимости от серьезности инцидента ИБ и степени его воздействия при оценке результатов анализа рисков ИБ и системы управления инцидентами ИБ, возможно, придется учитываться новые угрозы и уязвимости. В результате завершения анализа рисков ИБ и системы управления инцидентами ИБ может потребоваться внести изменения в существующие или применить новые защитные меры.

Следуя рекомендациям, сделанным в процессе анализа инцидента ИБ, Руководитель ГРИИБ инициирует и организует процесс внедрения обновленных и (или) новых защитных мер в соответствии с утвержденным Председателем Правления НКО Планом мероприятий по совершенствованию СОИБ.

7. Контроль соблюдения требований Порядка

7.1. Контроль соблюдения настоящего Порядка осуществляет Руководитель ГРИИБ на основе проведения анализа и оценки состояния обеспечения ИБ в НКО, а также в рамках иных контрольных мероприятий.

8. Порядок внесения изменений в Порядок

8.1. Ответственность за поддержание настоящего Порядка в актуальном состоянии, создание, внедрение, координацию и внесение изменений в процессы управления инцидентами ИБ ПС**,** включая ПС ОРС, возлагается на Службу информационной безопасности.

8.2. В случае изменения законодательства Российской Федерации, требований регулирующих органов Порядок должен быть пересмотрен. (Пересмотр Порядка не обязательно влечет за собой внесение изменений).

Приложение № 1

к Порядку управления инцидентами информационной безопасности ПС ОРС

Классификатор инцидентов ИБ ПС ОРС

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	
1.3. Источник информации об инциденте ИБ	работник НКО, работник операционного центра, работник участника, техническое средство
1.4. Фамилия, имя, отчество работника, выявившего инцидент ИБ	
1.5. Подразделение работника, выявившего инцидент ИБ	
1.6. Должность работника, выявившего инцидент ИБ	
1.7. Роль работника, выявившего инцидент ИБ	(пользователь, администратор АБС, работник службы ИБ)
1.8. Контактная информация работника, 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. Категория инцидента ИБ	несвоевременность переводов денежных средств; несанкционированный перевод денежных средств или угроза такого события; перевод денежных средств с использованием искаженной информации, содержащейся в распоряжениях участников ПС ОРС
2.2. Факт нарушения требований к обеспечению ИБ	«нет»; «реквизиты документа, пункт документа»
2.3. Данные о нарушителе требований к обеспечению ИБ	«нет»; «Фамилия И.О., должность нарушителя»
2.4. 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»
2.5. Факт реализации угрозы ИБ	«нет»; «идентификатор источника угрозы согласно действующему перечню актуальных угроз ИБ»
2.6. Факт нарушения свойств безопасности	«нет»; «Конфиденциальность»; «Целостность»; «Доступность»

2.7. Факт нестандартного (несанкционированного) поведения	«нет»; «нарушение установленного порядка и режима дня»; «отклонение от сложившегося порядка и режима использования информационных ресурсов»
2.8. Факт преднамеренности возникновения инцидента ИБ	«случайный»; «намеренный»; «ошибочный»
2.9. Тип инцидента ИБ	«свершившийся»; «попытка осуществления инцидента ИБ»
2.10. Степень сложности обнаружения инцидента ИБ	«Обычная»; «Высокая»
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»; «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)»; «общесистемные программные средства»; «прикладные программные средства»; «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»; «НКО в целом»; «операционный центр ПС ОРС» «участник ПС ОРС» «вся ПС ОРС»
Группа 4. Атрибуты, отражающие значимость инцидента ИБ	
4.1. Приоритет инцидента ИБ	«1 (Высокий)»; «2 (Средний)»; «3 (Низкий)»;
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. Функциональная группа	«нет»; «наименование функциональной группы специалистов, которой поручено реагирование на инцидент ИБ»
5.4. Время назначения функциональной группы	«нет»; «время, когда была назначена функциональная группа, ответственная за реагирование на инцидент ИБ»
5.5. Назначение специалиста — члена ГРИИБ	«нет»; «фамилия специалиста, ответственного за реагирование на инцидент ИБ»
5.6. Статус инцидента ИБ	«Зарегистрирован» «Назначен»; «В работе»; «Закрыт»
5.7. Установленный срок закрытия инцидента ИБ	«нет»; «установленный срок закрытия инцидента ИБ»
5.8. Необходимость информирования об инциденте ИБ структурных подразделений НКО.	«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 НКО 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 НКО	«нет»; «перечень подразделений»