УТВЕРЖДЕНЫ
Приказом
Президента-Председателя Правления
ПАО АКБ «Связь-Банк»
от 04 февраля 2016 г. № 50

Правила
реагирования на инциденты, связанные с нарушением требований к обеспечению защиты информации при осуществлении переводов денежных средств в Платежной системе BLIZKO

город Москва
2016
Содержание

1. Общие положения

1.1. Настоящие Правила реагирования на инциденты, связанные с нарушением требований к обеспечению защиты информации при осуществлении переводов денежных средств в Платежной системе BLIZKO (далее – Правила) определяют порядок действий по обнаружению инцидентов информационной безопасности (далее - ИБ), анализу и реагированию на инциденты ИБ, связанные с нарушением требований к обеспечению защиты информации при осуществлении переводов денежных средств в Платежной системе BLIZKO (далее – ПС BLIZKO).
1.2. Оператором Платежной системы BLIZKO (далее – Оператор ПС BLIZKO) является Межрегиональный коммерческий банк развития связи и информатики (публичное акционерное общество) (ПАО АКБ «Связь-Банк»).
1.3. Оператор ПС BLIZKO обеспечивает для Участников ПС BLIZKO и их Партнеров, операторов услуг платежной инфраструктуры, привлекаемых для оказания услуг платежной инфраструктуры в ПС BLIZKO, доступ в Личном кабинете Уполномоченного лица в Удостоверяющем центре (далее - Личный кабинет УЛ в УЦ) к следующей информации:
- о выявленных в платежной системе инцидентах, связанных с нарушениями требований к обеспечению защиты информации при осуществлении переводов денежных средств (в случае их наличия);
- о методиках анализа и реагирования на инциденты, связанные с нарушениями требований к обеспечению защиты информации при осуществлении переводов денежных средств.
1.4. Настоящие Правила разработаны на основании действующего законодательства Российской Федерации и внутренних нормативных документов Оператора ПС BLIZKO, в том числе:
- Федерального закона от 27 июня 2011 г. № 161 «О национальной платежной системе»;
- Постановления Правительства РФ от 13 июня 2012 г. № 584 «Об утверждении Положения о защите информации в платежной системе»;
- Положения Банка России от 09 июня 2012 г. № 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»;
- Указания Банка России от 09 июня 2012 г. № 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» (далее – Указание Банка России № 2831);
- действующих Правил Платежной системы BLIZKO (Далее – Правила ПС BLIZKO).
1.5. Действия настоящих Правил распространяется на операторов по переводу денежных средств, являющихся Участниками ПС BLIZKO, и операторов услуг платежной инфраструктуры, привлекаемых для оказания услуг платежной инфраструктуры в ПС BLIZKO.

2. Термины и определения

В настоящих Правилах используются следующие термины и определения:
2.1. ***Инцидент ИБ*** - инцидент, связанный с нарушениями требований к обеспечению защиты информации при осуществлении переводов денежных средств в ПС BLIZKO. К Инцидентам ИБ относятся события, которые возникли вследствие нарушения требований к обеспечению защиты информации при осуществлении переводов денежных средств и/или

условий осуществления (требований к осуществлению) перевода денежных средств, связанных с обеспечением защиты информации при осуществлении переводов денежных средств, которые установлены Оператором ПС BLIZKO и доведены им до Участника ПС BLIZKO, и которые:
- привели к несвоевременности (к нарушению сроков, установленных действующим законодательством Российской Федерации, Правилами ПС BLIZKO и/или договорами, заключаемыми участниками ПС BLIZKO) 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 клиентов, распоряжениях Участников ПС BLIZKO, распоряжениях Оператора ПС BLIZKO.

2.2. ***Обработка 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 Оператора ПС BLIZKO и (или) ее Участников ПС BLIZKO.

2.3. ***Оператор по переводу денежных средств*** – организация, которая в соответствии с законодательством Российской Федерации вправе осуществлять перевод денежных средств.

2.4. ***Оператор услуг платежной инфраструктуры*** – операционный центр, платежный клиринговый центр / центральный платежный клиринговый контрагент и расчетный центр.

2.5. ***Закрытие инцидента ИБ*** - действия работников Оператора ПС BLIZKO и/или Участника ПС BLIZKO в рамках реагирования на инцидент ИБ, результатом которых являются:
- устранение нарушений, реализованных в результате Инцидента ИБ;
- устранение причин выявленного Инцидента ИБ;
- выяснение причин нетипичного поведения работников Оператора ПС BLIZKO и/или Участника ПС BLIZKO и (или) иных лиц, нештатного функционирования информационных систем и иных объектов среды информационных активов Оператора ПС BLIZKO и/или Участника ПС BLIZKO, а также нетипичных событий в осуществлении технологических процессов.

2.6. ***Платежная система BLIZKO (ПС BLIZKO)*** – совокупность организаций, объединенных единым информационным пространством и взаимодействующих по Правилам Платежной системы BLIZKO в целях осуществления переводов денежных средств, включающая Оператора ПС BLIZKO, Операторов услуг платежной инфраструктуры и Участников ПС BLIZKO.

2.7. ***Участник Платежной системы BLIZKO (Участник ПС BLIZKO)*** – организация, присоединившаяся к Правилам ПС BLIZKO и заключившая с Оператором ПС BLIZKO договор участия в Платежной системе BLIZKO с целью оказания услуг по переводу денежных средств в рамках Платежной системы BLIZKO.

3. Цели и задачи обработки Инцидентов ИБ

3.1. Основными целями обработки Инцидентов ИБ являются:
- 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 осуществление банковских технологических процессов Оператора ПС BLIZKO и/или Участников ПС BLIZKO;

- оперативное совершенствование системы обеспечения информационной безопасности Оператора ПС BLIZKO и Участников ПС BLIZKO.

3.2. Основными задачами обработки Инцидентов ИБ являются:
- своевременное обнаружение Инцидентов ИБ;
- оперативное реагирование на Инциденты ИБ;
- координация деятельности работников структурных подразделений Оператора ПС BLIZKO и/или Участника ПС BLIZKO в рамках процессов реагирования на Инциденты ИБ, в том числе их закрытия;
- ведение базы данных зарегистрированных Инцидентов ИБ;
- накопление и повторное использование знаний по обнаружению Инцидентов ИБ и реагированию на них;
- анализ Инцидентов ИБ;
- оценка эффективности и совершенствование процессов обработки Инцидентов ИБ;
- предоставление отчетов по результатам обработки Инцидентов ИБ, в том числе информации о фактах обнаружения Инцидентов ИБ и результатах реагирования на них. Порядок предоставления данной информации/отчетов определяется внутренними документами Оператора ПС BLIZKO и/или Участника ПС BLIZKO.

4. Обнаружение Инцидентов ИБ

4.1. Обнаружение Инцидентов ИБ выполняется работниками Оператора ПС BLIZKO и/или Участника ПС BLIZKO/Оператора услуг платежной инфраструктуры, либо техническими средствами Оператора ПС BLIZKO и/или Участника ПС BLIZKO.

4.2. Регистрация информации об Инцидентах ИБ, включая сбор информации, связанной с Инцидентом ИБ, выполняется Оператором ПС BLIZKO и/или Участником ПС BLIZKO в соответствии с внутренними документами Оператора ПС BLIZKO и/или Участника ПС BLIZKO.

4.3. Основными источниками информации об Инцидентах ИБ, связанных с нарушениями требований к обеспечению защиты информации при осуществлении переводов денежных средств в ПС BLIZKO, могут быть:
- сообщения работников Оператора ПС BLIZKO и/или Участника ПС BLIZKO;
- сведения, отраженные в журналах регистрации событий информационных систем Оператора ПС BLIZKO и/или Участника ПС BLIZKO;
- результаты работы средств защиты информации Оператора ПС BLIZKO и/или Участника ПС BLIZKO;
- результаты внутренних проверок;
- другие источники информации об Инцидентах ИБ.

5. Оповещение Оператором ПС BLIZKO Участников ПС BLIZKO/Оператора услуг платежной инфраструктуры о возникновении Инцидентов ИБ

5.1. Оповещение Участников ПС BLIZKO/Операторов услуг платежной инфраструктуры о выявленных Инцидентах ИБ осуществляется путем размещения Оператором ПС BLIZKO в Личном кабинете УЛ в УЦ отчетности по форме и в срок, приведенными в Правилах ПС BLIZKO.

5.2. Предоставление Оператором ПС BLIZKO Участникам ПС BLIZKO/Операторам услуг платежной инфраструктуры отчетности по форме и в срок, приведенными в Правилах ПС BLIZKO, осуществляется в соответствии с п. 1.3 настоящих Правил.

5.3. Отсутствие предоставленной отчетности по форме и в срок, приведенными в Правилах ПС BLIZKO, означает отсутствие выявленных Инцидентов ИБ в отчетном периоде.

5.4. В случае необходимости немедленного реагирования на выявленный Инцидент ИБ Оператор ПС BLIZKO информирует Участников ПС BLIZKO/Операторов услуг платежной инфраструктуры любым доступным способом, предусмотренным Правилами ПС BLIZKO.

6. Оповещение Участниками ПС BLIZKO/Операторами услуг платежной инфраструктуры Оператора ПС BLIZKO о возникновении Инцидентов ИБ

6.1. Оповещение Оператора ПС BLIZKO о выявленных Инцидентах ИБ осуществляется путем предоставления Участником ПС BLIZKO/Оператором услуг платежной инфраструктуры по Согласованным каналам связи или посредством направления Официального письма отчетности по форме и в срок, приведенными в Правилах ПС BLIZKO.
6.2. Отсутствие предоставленной отчетности по форме и в срок, приведенными в Правилах ПС BLIZKO, означает отсутствие выявленных Инцидентов ИБ в отчетном периоде.
6.3. В случае необходимости немедленного реагирования на выявленный Инцидент ИБ Участник ПС BLIZKO/Оператор услуг платежной инфраструктуры информирует Оператора ПС BLIZKO любым доступным способом, предусмотренным Правилами ПС BLIZKO.

7. Порядок анализа и реагирования на Инциденты ИБ

7.1. Оператор ПС BLIZKO и/или Участник ПС BLIZKO/Оператора услуг платежной инфраструктуры при выявлении в ПС BLIZKO Инцидентов ИБ реализует комплекс мер, направленных на устранение последствий Инцидента ИБ, причин, вызвавших Инцидент ИБ, и на недопущение его повторного возникновения.
7.2. Анализ Инцидентов ИБ выполняется на основе:
- результатов проведения контроля выполнения 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 в затронутых Инцидентом ИБ информационных активах, автоматизированных системах,
- анализа степени тяжести последствий, наступивших в результате Инцидентов ИБ.
7.3. В процессе анализа устанавливаются причины возникновения выявленных Инцидентов ИБ.
7.4. В процессе анализа определяются наиболее проблемные с точки зрения подверженности Инцидентам ИБ сегменты и компоненты информационной инфраструктуры Оператора ПС BLIZKO и/или Участника ПС BLIZKO/Оператора услуг платежной инфраструктуры, наиболее существенные уязвимости и недостатки в обеспечении ИБ.
7.5. В процессе анализа Инцидентов ИБ оценивается достаточность принятых мер и выделенных ресурсов для реагирования на Инциденты ИБ, проводится оценка результатов реагирования на выявленные Инциденты ИБ.
7.6. В процессе анализа проверяются действия работников Оператора ПС BLIZKO и/или Участника ПС BLIZKO/Оператора услуг платежной инфраструктуры, осуществляемые при реагировании на Инциденты ИБ. Целью проведения данной проверки является формирование (инициирование) совершенствований в части:
- внесения изменений во внутренние нормативные документы Оператора ПС BLIZKO и/или Участников ПС BLIZKO/Операторов услуг платежной инфраструктуры, определяющие порядок обнаружения и реагирования на Инциденты ИБ;

- изменения состава лиц, привлекаемых к реагированию на Инциденты ИБ;
- совершенствования порядка эксплуатации технических средств защиты информации, а также технических средств, используемых при осуществлении переводов денежных средств.

7.7. По результатам анализа Инцидентов ИБ Оператор ПС BLIZKO и Участники ПС BLIZKO/Операторы услуг платежной инфраструктуры формируют отчеты по результатам обработки Инцидентов ИБ. Данные отчеты формируются по форме и методике составления, приведенными в Правилах ПС BLIZKO, на ежемесячной основе. Порядок взаимодействия структурных подразделений Оператора ПС BLIZKO и/или Участников ПС BLIZKO/Операторов услуг платежной инфраструктуры при формировании отчетов по результатам обработки Инцидентов ИБ определяется внутренними документами Оператора ПС BLIZKO и/или Участников ПС BLIZKO/Операторов услуг платежной инфраструктуры.

8. Заключительные положения

8.1. Настоящие Правила вступают в силу со дня их утверждения приказом Президента-Председателя Правлением Банка и действует до их отмены либо принятия нового документа.

8.2. Изменения и дополнения к настоящим Правилам утверждаются Президентом-Председателем Правлением Банка.

8.3. Разработчиком и структурным подразделением, отвечающим за актуализацию Правил, является Департамент безопасности.

8.4. Если при изменении действующего законодательства Российской Федерации или внесении изменений в нормативные акты Банка России, а также нормативные документы Банка отдельные пункты настоящих Правил вступят в противоречие с ними, то данные пункты утрачивают свою юридическую силу, и до момента внесения изменений в настоящие Правила работники Банка руководствуются действующим законодательством Российской Федерации, нормативными актами Банка России, а также нормативными документами Банка. Факт прекращения действия одного или нескольких пунктов не влияет на действие настоящих Правил в целом.