Положение о порядке обнаружения, анализа и реагирования на инциденты, связанные с нарушением требований к обеспечению защиты информации при осуществлении переводов денежных средств в Платёжной Системе ВТБ

1. Общие положения

1.1. Настоящее Положение определяет 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 Платёжной Системе ВТБ (далее - Системе).

1.2. Оператором Платёжной Системы ВТБ (далее – Оператор, Оператор Системы) является ОАО Банк ВТБ. Оператор определяет Правила Системы, осуществляет открытие и обслуживание банковских счетов участников Системы, контролирует соблюдение Правил Системы и выполняет другие действия в рамках своей компетенции, определенные Правилами Системы.

Оператор самостоятельно выполняет в рамках Системы функции оператора по переводу денежных средств, функции оператора услуг платёжной инфраструктуры и совмещает свою деятельность с оказанием операционных услуг, услуг платёжного клиринга и расчётных услуг.

1.3. Текст настоящего Положения публикуется на официальном сайте Системы в сети Интернет по адресу http://www.vtb.ru.

1.4. Настоящее Положение разработано на основании следующих нормативно-правовых актов Российской Федерации, нормативных актов Банка России и нормативных актов Оператора:

- Федерального закона от 27 июня 2011 года № 161 «О национальной платежной системе»;
- Постановления Правительства от 13 июня 2012 года № 584 «Об утверждении Положения о защите информации в платежной системе»;
- Положения Банка России от 9 июня 2012 года № 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 года № 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);
- Правил Платёжной Системы ВТБ, утверждённых приказом ОАО Банк ВТБ от 06.11.2014 №744 (далее – Правила Системы).

2. Термины и определения

В настоящем Положении используются следующие термины и определения:

2.1. ***Инцидент ИБ*** - инцидент, связанный с нарушениями требований к обеспечению защиты информации при осуществлении переводов денежных средств в Системе. 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 и доведены им до Участника, и которые:

- привели к несвоевременности (к нарушению сроков, установленных законодательством Российской Федерации, Правилами Системы и (или) договорами, заключаемыми участниками Системы) 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 Системы, распоряжениях Оператора.

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 Системы и (или) ее Участников.

2.3. ***Закрытие инцидента ИБ*** - действия работников Оператора и (или) Участника Системы 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 и (или) Участника Системы и (или) иных лиц, нештатного функционирования информационных систем и иных объектов среды информационных активов Оператора и (или) Участника Системы, а также нетипичных событий в осуществлении технологических процессов.

2.4. ***Платёжная Система ВТБ (Система)*** – платежная система, созданная в соответствии с законодательством Российской Федерации и осуществляющая переводы, в том числе трансграничные, денежных средств через банковские счета, открытые в ОАО Банк ВТБ.

2.5. ***Участник Системы (Участник)*** – оператор по переводу денежных средств, присоединившийся к Правилам Системы. Порядок присоединения к Правилам Системы определяется Правилами Системы.

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 и (или) Участников;
- оперативное совершенствование системы обеспечения информационной безопасности Оператора и Участников Системы.

3.2. Основными задачами обработки Инцидентов ИБ являются:

- своевременное обнаружение Инцидентов ИБ;
- оперативное реагирование на Инциденты ИБ;
- координация деятельности работников структурных подразделений Оператора и (или) Участника Системы 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 руководству информации и отчётов по результатам обработки Инцидентов ИБ, в том числе информации о фактах обнаружения Инцидентов ИБ и результатах реагирования на них. Порядок предоставления данной информации определяется внутренними документами Оператора и (или) Участника Системы.

4. Обнаружение Инцидентов ИБ

4.1. Обнаружение Инцидентов ИБ выполняется работниками Оператора и (или) Участника, либо техническими средствами Оператора и (или) Участника.

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

4.3. Основными источниками информации об Инцидентах ИБ, связанных с нарушениями требований к обеспечению защиты информации при осуществлении переводов денежных средств в Системе, могут быть:

- сообщения работников Оператора и (или) Участника;
- сведения, отражённые в журналах регистрации событий информационных систем Оператора и (или) Участника;
- результаты работы средств защиты информации Оператора и (или) Участника;
- результаты внутренних проверок;
- другие источники информации об Инцидентах ИБ.

5. Оповещение Оператором Участников Системы о возникновении Инцидентов ИБ

5.1. Оповещение Участников Системы о выявленных Инцидентах ИБ осуществляется путем предоставления Оператором отчётности по форме и методике составления, приведёнными в Приложении 2 к Указанию Банка России № 2831, на ежемесячной основе, не позднее пятого рабочего дня, следующего за отчётным периодом.

5.2. Предоставление Оператором Участнику Системы отчётности по форме и методике составления, приведёнными в Приложении 2 к Указанию Банка России № 2831, осуществляется в соответствии с Правилами Системы.

5.3. Отсутствие предоставленной отчётности по форме и методике составления, приведёнными в Приложении 2 к Указанию Банка России № 2831, означает отсутствие выявленных Инцидентов ИБ в отчётном периоде.

5.4. В случае необходимости немедленного реагирования на выявленный Инцидент ИБ Оператор информирует Участников Системы любым доступным способом, предусмотренным договорными отношениями между Оператором и Участниками Системы.

6. Оповещение Участниками Системы Оператора Системы о возникновении Инцидентов ИБ

6.1. Оповещение Оператора о выявленных Инцидентах ИБ осуществляется путем предоставления Участником Системы отчётности по форме и методике составления, приведёнными в Приложении 2 к Указанию Банка России № 2831, на ежемесячной основе, не позднее пятого рабочего дня, следующего за отчётным периодом.

6.2. Предоставление Участником Системы Оператору отчётности по форме и методике составления, приведёнными в Приложении 2 к Указанию Банка России № 2831, осуществляется в соответствии с Правилами Системы.

6.3. Отсутствие предоставленной отчётности по форме и методике составления, приведёнными в Приложении 2 к Указанию Банка России № 2831, означает отсутствие выявленных Инцидентов ИБ в отчётном периоде.

6.4. В случае необходимости немедленного реагирование на выявленный Инцидент ИБ Участник Системы информирует Оператора любым доступным способом, предусмотренным договорными отношениями, заключёнными между Участником Системы и Оператором.

7. Порядок анализа и реагирования на Инциденты ИБ

7.1. Оператор и (или) Участник Системы при выявлении в Системе 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, затронутых Инцидентом ИБ информационных активах, автоматизированных системах, степени тяжести последствий от обнаруженных 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 и (или) Участника Системы, 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 и (или) Участника Системы, осуществляемые при реагировании на Инциденты ИБ. Целью проведения данной проверки является формирование (инициирование) совершенствований в части:

- корректировки внутренних документов Оператора и (или) Участников Системы, определяющих порядок обнаружения и реагирования на Инциденты ИБ;
- изменения состава лиц, привлекаемых к реагированию на Инциденты ИБ;
- корректировки порядка эксплуатации технических средств защиты информации, а также технических средств, используемых при осуществлении переводов денежных средств.

7.7. По результатам анализа Инцидентов ИБ Оператор и Участники Системы формируют отчёты по результатам обработки Инцидентов ИБ. Данные отчёты формируются по форме и методике составления, приведёнными в Приложении 2 к Указанию Банка России № 2831, на ежемесячной основе. Порядок взаимодействия структурных подразделений Оператора и (или) Участников Системы при формировании отчётов по результатам обработки Инцидентов ИБ определяются внутренними документами Оператора и (или) Участников Системы.

7.8. Порядок взаимодействия уполномоченных лиц Оператора и (или) Участника Системы, участвующих в анализе и реагировании на Инциденты ИБ, определяются внутренними документами Оператора и (или) Участника Системы.

Президент – Председатель Правления
ОАО Банк ВТБ

А.Л.Костин