Порядок обработки инцидентов, связанных с нарушением требований к обеспечению защиты информации при осуществлении переводов денежных средств в АО КБ «ИВАНОВО»

1. ТЕРМИНЫ И ОПРЕДЕЛЕНИЯ

1.1. **Банк** – АО КБ «ИВАНОВО».
1.2. **ИБ** – информационная безопасность.
1.3. **Инцидент ИБ** - инцидент, связанный с нарушениями требований к обеспечению защиты информации при осуществлении переводов денежных средств.
К Инцидентам ИБ в рамках настоящего Порядка 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 Банком и которые:
- ✓ привели к несвоевременности (к нарушению сроков, установленных законодательством Российской Федерации, нормативными документами Банка России, внутрибанковскими документами и (или) договорами, заключаемыми с клиентами/контрагентами) 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/контрагентов.

1.4. **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.
1.5. **Закрытие инцидента ИБ** - действия работников Банка 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 Банка и (или) иных лиц, нештатного функционирования информационных систем и иных объектов информационной среды, а также нетипичных событий в осуществлении технологических процессов.

1.6 **Компрометация ключа** – констатация лицом, владеющим закрытым (секретным) ключом электронной подписи и/или шифрования, обстоятельств, при которых возможно несанкционированное использование данного ключа неуполномоченными лицами.
1.7 **ЭП**- электронная подпись.

2. ЦЕЛИ И ЗАДАЧИ ОБРАБОТКИ ИНЦИДЕНТОВ ИБ

2.1. 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;

- оперативное совершенствование системы обеспечения информационной безопасности.

2.2. Основными задачами обработки Инцидентов ИБ являются:
- своевременное обнаружение Инцидентов ИБ;
- оперативное реагирование на Инциденты ИБ;
- координация деятельности работников структурных подразделений Банка в рамках процессов реагирования на Инциденты ИБ, в том числе их закрытия;
- ведение Журнала 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 Банка информации и отчётов по результатам обработки Инцидентов ИБ, в том числе информации о фактах обнаружения Инцидентов ИБ и результатах реагирования на них.

3. ТРЕБОВАНИЯ ДЛЯ КЛИЕНТОВ ПО ОБЕСПЕЧЕНИЮ ЗАЩИТЫ ИНФОРМАЦИИ ПРИ ОСУЩЕСТВЛЕНИИ ПЕРЕВОДОВ ДЕНЕЖНЫХ СРЕДСТВ

3.1. Используйте лицензионное программное обеспечение на устройствах (персональный компьютер, ноутбук, планшет, смартфон и т.д.).

3.2. Обязательно установите себе решение для защиты от информационных угроз (антивирус, защита от шпионских программ, защита от фишинга, сетевой экран и т.д.).

3.3. Устройства, с которых осуществляются переводы денежных средств должны быть исправны, функционировать в штатном режиме, с использованием операционной среды, чистой от вирусов, программ шпионов и программ удаленного доступа.

3.4. Обмен ЭД между Банком и Клиентом осуществляется с применением средств криптозащиты информации (далее – СКЗИ) - ЭП и шифрования.

3.5. Клиентом должен быть определен порядок учёта, хранения и использования носителей ключевой информации (съемный носитель цифровой информации) с секретными ключами ЭП и шифрования, который должен полностью исключать возможность несанкционированного доступа к ним.

3.6. По окончании рабочего дня, а также вне времени составления и обмена ЭД носители секретных ключей ЭП должны быть удалены из устройства, используемого для перевода денежных средств, храниться в сейфах.

3.7. Регулярно проверяйте состояние своих банковских счетов (в том числе счетов, к которым привязаны дебетовые и кредитные карты) и просматривайте банковские выписки, чтобы убедиться в отсутствии "лишних" операций.

4. ПОРЯДОК ОБРАБОТКИ ИНЦИДЕНТОВ

При осуществлении перевода денежных средств возможно возникновение следующих групп инцидентов:

4.1. Компрометация ключа ЭП и/или идентификаторов для доступа к переводу денежных средств.

4.1.1 Необходимо немедленно заблокировать ЭП или идентификаторы для доступа к переводу денежных средств. Блокировка осуществляется одним из приведенных способом:

- Обращение по телефону +7(4932)32-78-31 в службу технической поддержки, для блокировки необходимо использовать карточку компрометации (выдается банком при получении ЭП).

- Представителю организации лично явится в службу технической поддержки с обращением о блокировке.
- Написать заявление на блокировку и отдать ее в ближайший офис банка.

4.1.2 Запросить выписку по счету и проверить ее на отсутствие несанкционированных переводов денежных средств. В случае обнаружения несанкционированных переводов денежных средств действовать согласно пункта 4.3 настоящего порядка.

4.1.3 Переформировать ЭП и/или идентификаторы для доступа к переводу денежных средств

4.1.4 Возобновить штатную работу по переводу денежных средств.

4.2. Нештатное функционирование системы переводов денежных средств.

4.2.1. Приостановить любые переводы денежных средств.

4.2.2. Обратится по телефону +7(4932)32-78-31 в службу технической поддержки.

4.2.3. Следовать указания специалистов службы технической поддержки для устранения нештатного работы системы по переводу денежных средств.

4.2.4. Запросить выписку по счету и проверить ее на отсутствие несанкционированных переводов денежных средств. В случае обнаружения несанкционированных переводов денежных средств действовать согласно пункту 4.3 настоящего порядка.

4.2.5. Возобновить штатную работу по переводу денежных средств.

4.3. Обнаружение несанкционированных переводов денежных средств.

4.3.1. Написать заявление о несанкционированном переводе денежных средств и отдать его в ближайший офис банка.