Межбанковская конференция
«Актуальные вопросы обеспечения информационной безопасности банков и защиты информации при осуществлении перевода денежных средств в национальной платежной системе Российской Федерации»

Сбор и анализ сведений о выявлении инцидентов, связанных с нарушением требований к обеспечению защиты информации при осуществлении переводов денежных средств

Толстая Светлана Александровна
главный экономист
Департамент регулирования расчетов

29 мая 2013 года

Отчетность по форме 0403203 *«Сведения о выявлении инцидентов, связанных с нарушением требований к обеспечению защиты информации при осуществлении переводов денежных средств»*

- **форма отчетности, сроки предоставления, методики составления определены в** ***Указании Банка России от 9 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»***

- **сбор осуществляется с августа 2012 года**

Сроки предоставления:

- ежемесячно не позднее десятого рабочего дня месяца, следующего за отчетным;

- по требованию Банка России - не позднее десяти рабочих дней со дня получения письменного требования Банка России.

Кто предоставляет: операторы услуг платежной инфраструктуры, операторы по переводу денежных средств

- ***подготовлен и опубликован на сайте Банка России «Аналитический обзор инцидентов, связанных с нарушением требований к обеспечению защиты информации при осуществлении переводов денежных средств (второе полугодие 2012)»***

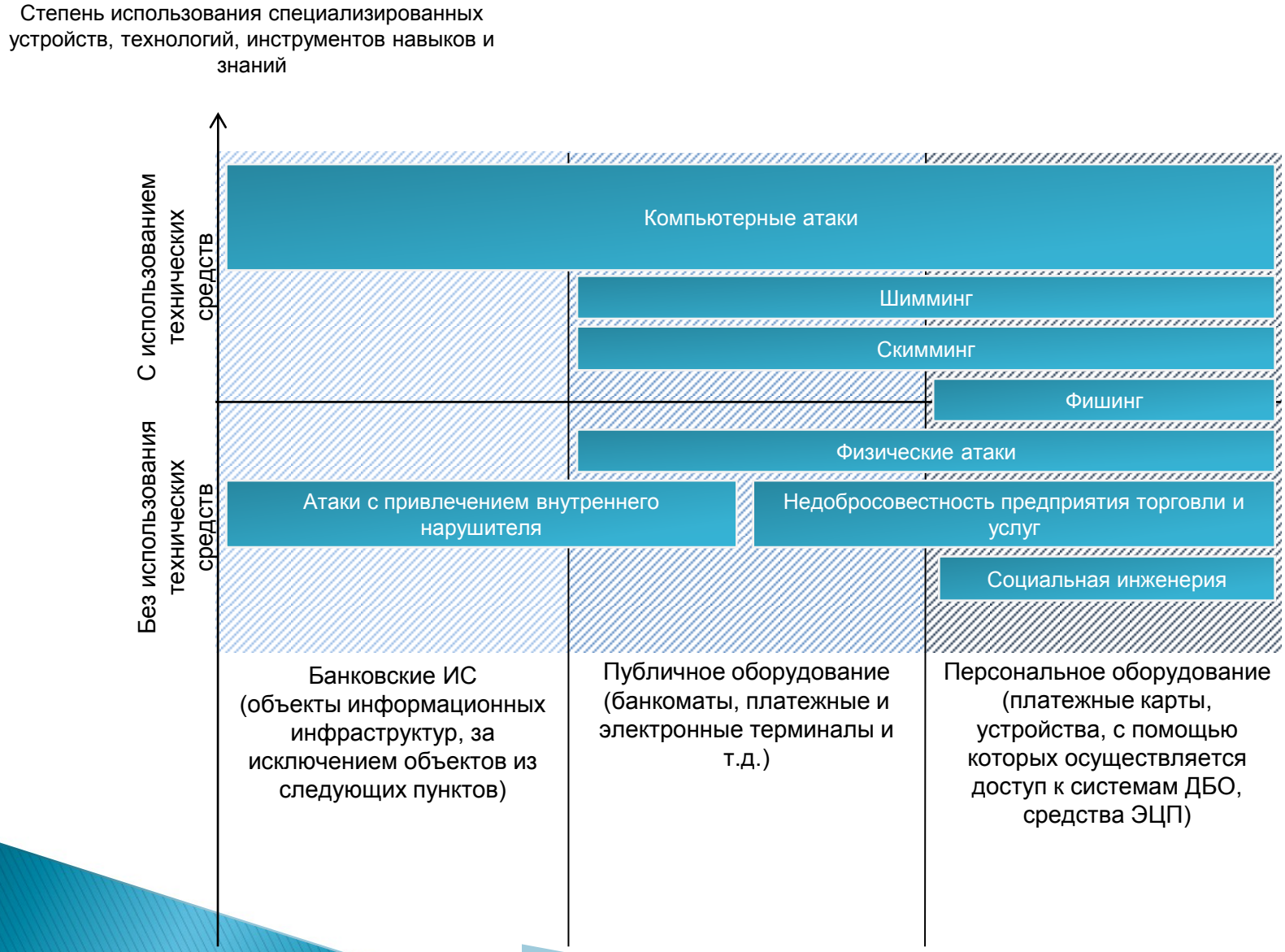
Угрозы нарушения защиты информации при осуществлении переводов денежных средств с использованием электронных средств платежа, систем ДБО

- Хищение денежных средств,
- Хищение информации с целью создания условий для хищения денежных средств в будущем (необходимой для осуществления переводов денежных средств, для удостоверения права распоряжения денежными средствами),
- Нарушение предоставления платежных услуг и услуг платежной инфраструктуры,
- Нарушение конфиденциальности защищаемой информации.

Реализация:

- скимминг;
- использование поддельных платежных карт («белый пластик»);
- несанкционированные операции с использованием реквизитов платежных карт (без использования карты);
- использование потерянных и украденных карт;
- удаленный доступ и управление, «подмена управления», «перехват управления»;
- воздействие вредоносного ПО, вирусные инфекции;
- атаки, направленные на отказ в обслуживании;
- фишинг;
- социальная инженерия;
- телефонное мошенничество;
- т.п.

Распределение актуальных методов осуществления несанкционированных операций (по технологичности и направленности)



Внесение изменений в Указание Банка России от 9 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»

- **Уточнение критериев включения в отчетность инцидентов**
- **Уточнение параметров, описывающих инциденты**
- **Введение оценок ущерба**
- **Дополнение новым разделом: «Сведения об инцидентах предыдущих отчетных периодов»**
- **Уточнение сроков представления отчетности**
- **Установление обязанности оператора платежной системы предоставлять отчетность о выявлении инцидентов зарубежным операционным центром**

Уточнение критериев включения в отчетность инцидентов (1)

К инцидентам, связанным с нарушением требований к обеспечению защиты информации при осуществлении переводов денежных средств 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 по переводу денежных средств и доведены им до клиента*

* *Требований, в соответствии с которыми оператор платежной системы, оператор услуг платежной инфраструктуры, оператор по переводу денежных средств, банковский платежный агент (субагент) обеспечивают защиту информации при осуществлении переводов денежных средств (ч.3 ст.27 ФЗ-161)*

установлены Положением Банка России от 9 июня 2012 года № 382-П.

Указание о внесении изменений в Положение Банка России от 9 июня 2012 года № 382-П

Уточнение критериев включения в отчетность инцидентов (2)

События, которые

- **привели к несвоевременности (к нарушению сроков, установленных законодательством Российской Федерации, правилами платежных систем и (или) договорами, заключаемыми клиентами, операторами по переводу денежных средств, операторами услуг платежной инфраструктуры, операторами платежных систем, банковскими платежными агентами (субагентами), участниками платежных систем) 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 платежной системы, распоряжениях клирингового центра.**

Указание о внесении изменений в Положение Банка России от 9 июня 2012 года № 382-П

Уточнение критериев включения в отчетность инцидентов (3)

Отчитывающийся оператор - оператор услуг платежной инфраструктуры:

в отчетность включаются сведения об инцидентах, самостоятельно выявленных в отчетном периоде.

Отчитывающийся оператор - оператор по переводу денежных средств:

в отчетность включаются сведения об инцидентах :

- самостоятельно выявленных в отчетном периоде инцидентах;
- ставших ему известными инцидентах, выявленных клиентами,
- ставшие ему известными инцидентах, выявленных банковскими платежными агентами, привлеченными к деятельности по оказанию услуг по переводу денежных средств оператором по переводу денежных средств, и банковскими платежными субагентами, привлеченными указанными банковскими платежными агентами.

Отчитывающийся оператор - оператор платежной системы, привлекающий для оказания операционных услуг участникам платежной системы операционный центр, находящийся за пределами Российской Федерации:

в отчетность включаются сведения о ставших ему известными инцидентах на основе информации, полученной в соответствии с подпунктом 2.13.1 пункта 2.13 и абзацем седьмым подпункта 2.16.2 пункта 2.16 Положения Банка России № 382-П.

Заполнение граф в отчетности по форме 0403203 проводится на основе сведений, имеющихся у отчитывающегося оператора на дату предоставления отчетности, в том числе которые были получены в ходе рассмотрения инцидента (разбирательства по инциденту).

Уточнение параметров, описывающих инциденты

1. **Даты – выявления, возникновения инцидента, завершения разбирательства по инциденту**
2. **Условия возникновения инцидента**
3. **Описание инцидента**
4. **Причины инцидента**
5. **Регион выявления инцидента**
6. **Отношения к платежной системе**
7. **Последствия инцидента**

Условия возникновения инцидентов, сведения о которых включаются в отчетность по форме 0403203

Причины возникновения инцидентов, сведения о которых включаются в отчетность по форме 0403203

- нарушение клиентом условий использования электронного средства платежа, о которых отчитывающийся оператор информирует клиента в соответствии с ч 3 ст. 9 ФЗ «О национальной платежной системе»
- использование электронного средства платежа без согласия клиента вследствие кражи, потери, нарушении конфиденциальности аутентификационной информации
- размещение на банкоматах и платежных терминалах специализированных средств, предназначенных для несанкционированного получения (съема) информации, необходимой для осуществления переводов денежных средств, в том числе аутентификационной информации
- внешние воздействия из сети Интернет, связанные с атаками типа «отказ в обслуживании» (атаками типа DoS/DDoS), с подменой адреса и (или) ресурса сети Интернет и др.
- распространение информации, побуждающей клиента оператора по переводу денежных средств сообщать информацию, необходимую для осуществления переводов денежных средств, в том числе аутентификационную информацию
- умышленное нарушение порядка эксплуатации объекта информационной инфраструктуры
- неумышленное нарушение порядка эксплуатации объекта информационной инфраструктуры
- физическое воздействие на объект информационной инфраструктуры, приводящее к его повреждению
- хищение объекта информационной инфраструктуры
- сбой и (или) отказ в работе объекта (-ов) информационной инфраструктуры
- воздействие вредоносного кода

Последствия инцидентов, сведения о которых включаются в отчетность по форме 0403203

Оценки ущерба:

- **Сумма переводов денежных средств, содержащаяся в распоряжениях клиентов, распоряжениях участников платежной системы или распоряжениях клирингового центра;**
- **Сумма переводов денежных средств, по которым наступила окончательность перевода денежных средств;**
- **Оценка в денежном выражении «косвенного» финансового ущерба (убытков причиненных в результате инцидента, за исключением суммы переводов денежных средств, по которым наступила окончательность перевода денежных средств).**

Оценка периода времени, в течение которого услуги по осуществлению переводов денежных средств не предоставлялись.

Изменение сведений об инцидентах, включенных в отчетность по форме 0403203

Дополнение новым разделом: «Сведения об инцидентах предыдущих отчетных периодов»

В разделе указываются сведения об инцидентах, выявленных в предыдущих отчетных периодах и разбирательство по которым на дату представления отчетности завершено.

Заполняется на основе сведений об инциденте, имеющихся у отчитывающегося оператора на дату окончания проведения разбирательства по данному инциденту, в том числе исходя из наличия новых сведений, выявленных в ходе разбирательства.

Благодарю за внимание!

Толстая Светлана Александровна
Департамент регулирования расчетов
tsa4@cbr.ru

29 мая 2013 года