Аналитический обзор

инцидентов, связанных с нарушением требований к обеспечению защиты информации при осуществлении переводов денежных средств

(второе полугодие 2012)

2013

Содержание

1. Общее описание ситуации
Вводная часть

Данный обзор подготовлен на основании отчетности по форме 0403203 «Сведения о выявлении инцидентов, связанных с нарушением требований к обеспечению защиты информации при осуществлении переводов денежных средств», предоставленной в Банк России операторами по переводу денежных средств, операторами услуг платежной инфраструктуры *(далее – отчитывающиеся операторы)* в соответствии с Указанием 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» во втором полугодии 2012 года (далее – анализируемый период).

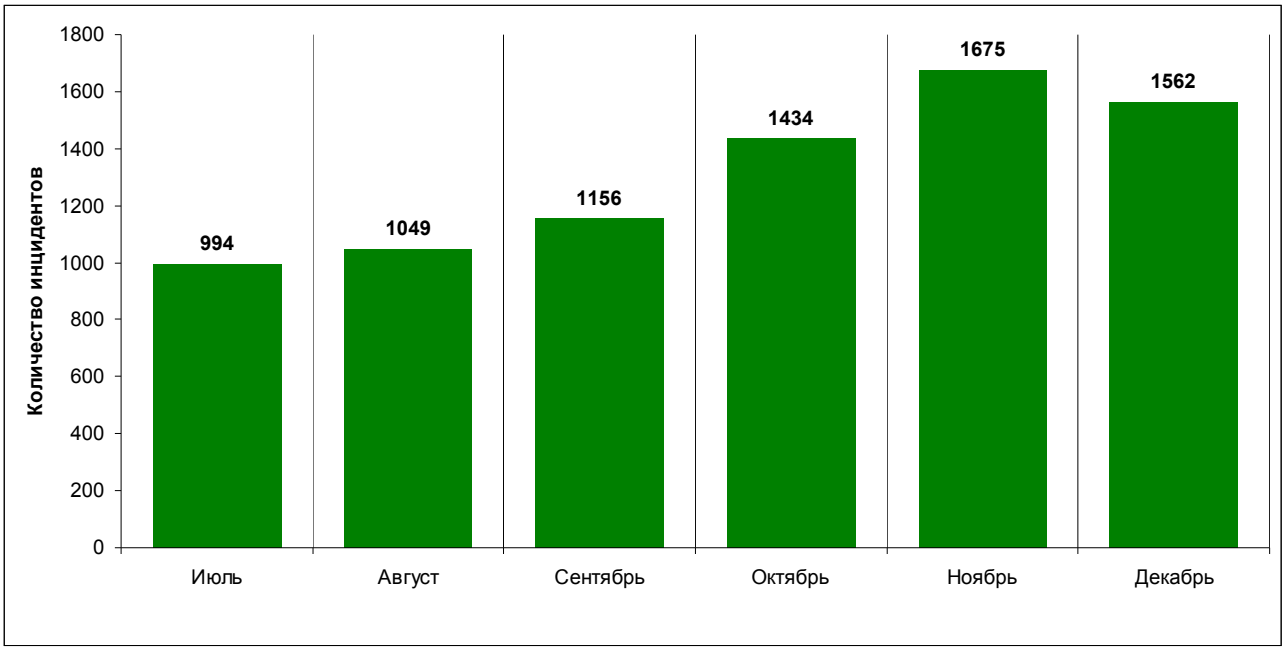
В обзор включены данные об инцидентах, связанных с нарушением требований к обеспечению защиты информации при осуществлении переводов денежных средств, под которыми понимаются события, возникшие вследствие нарушения требований к обеспечению защиты информации при осуществлении переводов денежных средств и приведшие или способные привести к невозможности предоставления услуг по осуществлению переводов денежных средств, к несвоевременности осуществления переводов денежных средств и (или) к осуществлению переводов денежных средств лицами, не обладающими правом распоряжения этими денежными средствами.

К инцидентам, связанным с нарушением требований к обеспечению защиты информации при осуществлении переводов денежных средств, не относятся противоправные действия, совершаемые нетехническими методами, например, методами социальной инженерии.

1.1. Количество выявленных инцидентов

Динамика общего количества инцидентов представлена на рисунке 1:

Рисунок 1. Количество инцидентов



В июле-ноябре 2012 года фиксировался рост числа выявленных инцидентов, в декабре – определенное снижение.

1.2. Распределение по количеству инцидентов, выявляемых одним оператором.

Динамика доли операторов, не выявивших инциденты, приведена в таблице 1. Данные свидетельствуют, что на протяжении отчетного периода основная часть отчитывающихся операторов инциденты не выявила.

Таблица 1. Динамика доли операторов, не выявивших инцидентов

	Июль	Август	Сентябрь	Октябрь	Ноябрь	Декабрь
Доля операторов, не выявивших инциденты, в общем количестве операторов	93%	92%	89%	89%	88%	90%

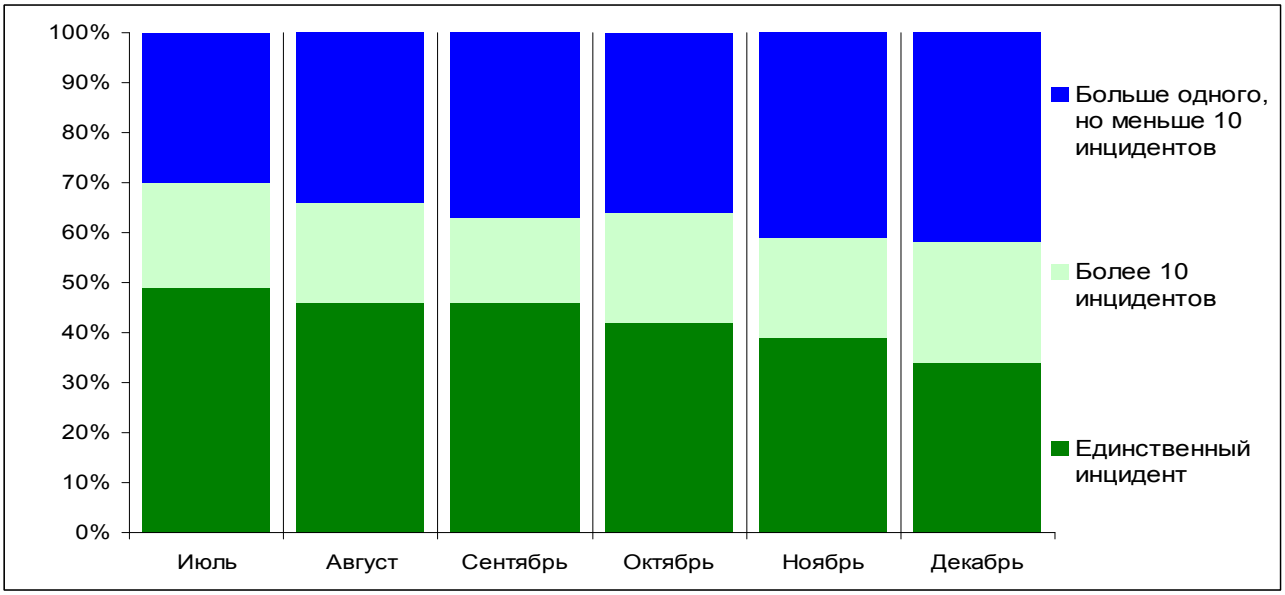
Распределение операторов, сообщивших о выявлении инцидентов, по количеству инцидентов, приходящемуся на одного оператора, представлено в таблице 2:

Таблица 2. Распределение операторов, выявивших инциденты, по количеству инцидентов, приходящемуся на одного оператора (в процентах от общего количества операторов, выявивших инциденты)

	Июль	Август	Сентябрь	Октябрь	Ноябрь	Декабрь
Единственный инцидент	49%	46%	45%	42%	39%	34%
Больше одного, но меньше 10	31%	34%	37%	35%	41%	42%
Больше 10, но меньше 20	10%	5%	4%	12%	7%	11%
Больше 20, но меньше 50	3%	11%	8%	5%	5%	7%
Больше 50, но меньше 100	4%	0%	5%	4%	4%	3%
Больше ста инцидентов	3%	4%	1%	2%	4%	3%

Таким образом, порядка 80% отчитывающихся операторов, выявивших инциденты, выявляют менее 10 инцидентов в месяц, при этом, от 34% до 49% этих операторов сообщают только об одном выявленном инциденте. Порядка 20% сталкиваются более чем с 10 инцидентами в месяц (рисунок 2).

Рисунок 2. Распределение операторов, выявивших инциденты, по количеству инцидентов, приходящемуся на одного оператора (в процентах от количества операторов, выявивших инциденты)



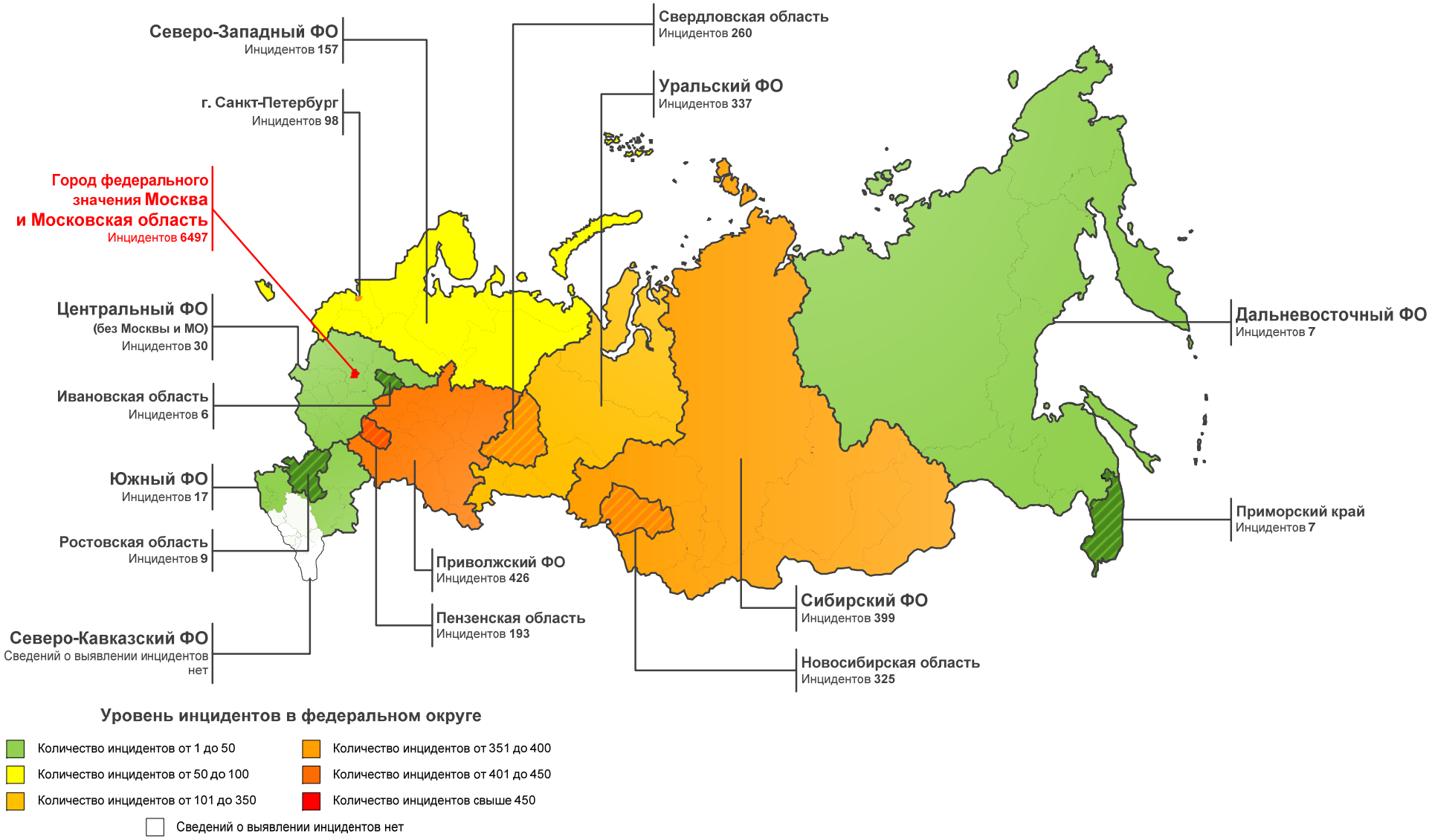
1.3. Распределение инцидентов по федеральным округам

Данные о распределении инцидентов по федеральным округам приведены в таблице 3 и на рисунке 3.

Таблица 3. Распределение инцидентов по федеральным округам

№ п/п	Федеральный округ	Количество инцидентов за полугодие	Регион в округе, в котором зафиксировано наибольшее количество инцидентов
1.	Город федерального значения Москва и Московская область	6497	Москва и Московская область
2.	Приволжский федеральный округ	426	Пензенская область
3.	Сибирский федеральный округ	399	Новосибирская область
4.	Уральский федеральный округ	337	Свердловская область
5.	Северо-Западный федеральный округ	157	гор. Санкт-Петербург
6.	Центральный федеральный округ (без г. Москвы и области)	30	Ивановская область
7.	Южный федеральный округ	17	Ростовская область
8.	Дальневосточный федеральный округ	7	Приморский край
9.	Северо-Кавказский федеральный округ	0	-

Рисунок 3. Распределение инцидентов по федеральным округам



2. Динамика распределения количества инцидентов по видам их последствий и по объектам информационной инфраструктуры, на которых они были выявлены.

2.1. Общая информация

Указанием Банка России от 09.06.2012 №2831-У установлены классификаторы инцидентов двух типов: по типам их последствий и по типам объектов информационной инфраструктуры.

2.2. Распределение инцидентов по типам их последствий

Данные по распределению инцидентов по типам их последствий за анализируемый период времени приведены в таблице 4:

Таблица 4. Распределение инцидентов по типам их последствий, в процентах от общего количества инцидентов

Код последствия	Последствие инцидента	Доля в общем количестве инцидентов
1	Воздействие вредоносного кода, приводящее к нарушению штатного функционирования средства вычислительной техники, результатом которого является нарушение предоставления услуг по переводу денежных средств или несвоевременности осуществления переводов денежных средств.	0,2%
2	Реализация воздействий с целью создания условий невозможности предоставления услуг по переводу денежных средств или несвоевременности осуществления переводов денежных средств.	6,8%
3	Нарушение конфиденциальности информации, необходимой для удостоверения клиентами операторов по переводу денежных средств права распоряжения денежными средствами.	29,7%
4	Компрометация ключевой информации средств криптографической защиты информации, используемых при осуществлении переводов денежных средств.	9,7%
5	Осуществление переводов денежных средств лицами, не обладающими правом распоряжения этими денежными средствами.	43,1%
6	Воздействие вредоносного кода, приводящее к осуществлению переводов денежных средств с использованием искаженной информации, содержащейся в распоряжениях клиентов.	6,4%

7	Невозможность предоставления услуг по переводу денежных средств в платежной системе в течении трех часов и более.	4,1%

Согласно приведенным данным:

1. Инциденты, связанные с воздействием вредоносного кода, приводящим к нарушению штатного функционирования средства вычислительной техники, результатом которого является нарушение предоставления услуг по переводу денежных средств или несвоевременности осуществления переводов денежных средств возникают крайне редко.
2. Инциденты, связанные с реализацией воздействий с целью создания условий невозможности предоставления услуг по переводу денежных средств или несвоевременности осуществления переводов денежных средств в отдельные месяцы составляют более 10% от общего числа инцидентов.
3. Инциденты, связанные с нарушением конфиденциальности информации, необходимой для удостоверения клиентами операторов по переводу денежных средств права распоряжения денежными средствами по своему количеству занимают второе место в общем числе инцидентов, поскольку к этому типу инцидентов отчитывающиеся операторы обычно относят, помимо прочего, инциденты, связанные со скиммингом.
4. Доля инцидентов, связанных с компрометацией ключевой информации средств криптографической защиты информации (СКЗИ), используемых при осуществлении переводов денежных средств в общем числе инцидентов составляет порядка 10% от общего числа инцидентов. При этом в отчетах содержится информация о том, что именно с данным типом инцидентов связан наибольший финансовый ущерб. При этом сами по себе СКЗИ являются надежным средством защиты, а риски их использования обусловлены «человеческим фактором» – низкой исполнительской дисциплиной, халатностью при хранении ключевой информации.
5. Поскольку осуществление переводов денежных средств лицами, не обладающими правом распоряжения этими денежными средствами, является

основной целью злоумышленников, инциденты данного вида закономерно составляют большую долю всех выявляемых инцидентов.

6. Доля инцидентов, связанных с воздействием вредоносного кода, приводящим к осуществлению переводов денежных средств с использованием искаженной информации, содержащейся в распоряжениях клиентов, достаточно стабильна и составляет менее 10% от общего числа инцидентов.

7. Инциденты, связанные с невозможностью предоставления услуг по переводу денежных средств в платежной системе в течении трех и более часов, происходят достаточно редко.

2.3. Распределение инцидентов по типам объектов информационной инфраструктуры

За анализируемый период доля инцидентов по типам объектов информационной инфраструктуры распределилась следующим образом (таблица 5):

Таблица 5. Распределение инцидентов по типам объектов информационной инфраструктуры, в процентах от общего количества инцидентов

Код объекта	Объект информационной инфраструктуры	Доля в общем количестве инцидентов
1	Автоматизированные системы, используемые для осуществления переводов денежных средств	24,6%
2	Программное обеспечение, используемое для осуществления переводов денежных средств	32,2%
3	Средства вычислительной техники, используемые для осуществления переводов денежных средств	38,0%
4	Телекоммуникационное оборудование, используемое для осуществления переводов денежных средств	1,2%
5	Технические средства по защите информации, используемые для осуществления переводов денежных средств.	4,0%

3. Деятельность банковского сообщества по повышению уровня защиты информации при осуществлении переводов денежных средств

Кредитные организации, сталкивающиеся с угрозами, обозначенными в настоящем обзоре, в настоящее время реализуют комплекс мероприятий (более

60) организационного и технического характера, направленных на обеспечение защиты информации.

Поскольку основное количество схем хищений направлено на реализацию различных атак на процедуры и технологии расчетов с использованием электронных средств платежа, включая системы дистанционного банковского обслуживания (ДБО), то и основные мероприятия ориентированы на защиту этих средств. К основным мероприятиям относятся:

- разработка рекомендаций и памяток для клиентов по безопасному использованию электронных средств платежа;
- регулярное информирование клиентов об актуальных угрозах;
- фиксация в договорах с клиентами требований по обязательному применению ими антивирусных средств, по использованию компьютера только для работы с системами ДБО, по порядку использования и хранения ключей СКЗИ и других подобных требований, направленных на повышение уровня ответственности клиента;
- установление разовых, суточных и иных лимитов на перевод/снятие денежных средств;
- технические меры по борьбе со скиммингом;
- видеонаблюдение в местах установки банкоматов;
- переход ряда банков на использование EMV-карт (хорошо зарекомендовавшая себя на практике в ряде европейских стран мера борьбы со скиммингом);
- использование получаемых по SMS или формируемых иным способом одноразовых паролей/кодов для подтверждения платежных поручений;
- внедрение носителей с неизвлекаемыми ключами электронной подписи;
- разработка программных и аппаратных средств формирования доверенной среды для работы клиента ДБО.

Банками проводится также ряд внутренних мероприятий, которые включают в себя регламентацию и документирование вопросов защиты информации, мероприятия по реагированию на инциденты, связанные с нарушением требований к обеспечению защиты информации при осуществлении переводов денежных средств.

Кроме того, банками создаются внутренние автоматизированные системы, осуществляющие мониторинг действий пользователей и регистрацию событий, позволяющих выявить противоправные действия.

Кредитные организации уделяют внимание взаимодействию с провайдерами услуг, разработке схем защищенной сети, обеспечивающей бесперебойное функционирование платежной системы, использованию резервных Интернет-провайдеров для защиты от DDoS-атак.

Важным является участие банков в различных добровольных межбанковских сообществах с целью обмена информацией, помогающей успешно противодействовать мошенническим действиям.