Стандарт Банка России СТО БР БФБО-1.5-2018 "Безопасность финансовых (банковских) операций. Управление инцидентами информационной безопасности. О Формах и сроках взаимодействия Банка России с участниками информационного обмена при выявлении инцидентов, связанных с нарушением требований к обеспечению защиты информации" (принят и введен в действие приказом Банка России от 14 сентября 2018 года N ОД-2403)

Дата введения: 1 ноября 2018 г.

Введение

Настоящий стандарт определяет следующие аспекты взаимодействия Банка России с кредитными организациями, некредитными финансовыми организациями, субъектами национальной платежной системы (далее при совместном упоминании - участники информационного обмена) при выявлении инцидентов, связанных с нарушением требований к обеспечению защиты информации:

форму представления данных, используемую участниками информационного обмена для регистрации в Банке России;

форму представления данных, используемую участниками информационного обмена для информирования Банка России об инцидентах, связанных с нарушением требований к обеспечению защиты информации, и сроки их представления в Банк России;

форму запроса Банка России к участнику информационного обмена, обслуживающему получателя средств;

форму представления данных, используемую участниками информационного обмена для представления ответа на запрос Банка России к участнику информационного обмена, обслуживающему получателя средств, и сроки их представления в Банк России;

форму информационного сообщения Банка России участнику информационного обмена, обслуживающему плательщика;

форму представления данных, используемую участниками информационного обмена для направления запроса в Банк России, об установлении (или снятии) на их банковские (корреспондентские) счета (субсчета) ограничения в виде запрета на списание денежных средств при выявлении инцидентов, связанных с нарушением требований к обеспечению защиты информации;

форму информационного сообщения Банка России об установлении или снятии на банковские (корреспондентские) счета (субсчета) участников информационного обмена ограничения в виде запрета на списание денежных средств при выявлении инцидентов, связанных с нарушением требований к обеспечению защиты информации;

форму распространения Банком России среди участников информационного обмена данных о выявленных инцидентах, связанных с нарушением требований к обеспечению защиты информации;

форму представления данных, используемую участниками информационного обмена для направления в Банк России информации о планируемых мероприятиях по раскрытию информации о выявленных инцидентах, связанных с нарушением требований к обеспечению защиты информации, и сроки их представления в Банк России;

условия представления Банку России участниками информационного обмена данных о выявленных инцидентах, связанных с нарушением требований к обеспечению защиты информации;

описание технологии подготовки и направления электронных сообщений при информационном обмене с Банком России.

Форма представления данных, используемая участниками информационного обмена для информирования Банка России об инцидентах, связанных с нарушением требований к обеспечению защиты информации, применяется в следующих случаях:

- при информировании Банка России операторами по переводу денежных средств, операторами услуг платежной инфраструктуры о выявленных инцидентах, связанных с нарушением требований к обеспечению защиты информации при осуществлении переводов денежных средств, в соответствии с требованиями Банка России [3];

- при информировании Банка России операторами по переводу денежных средств, операторами услуг платежной инфраструктуры обо всех случаях и (или) попытках осуществления переводов денежных средств без согласия клиента в соответствии с требованиями Банка России [4];

- при информировании Банка России кредитными организациями о выявленных инцидентах, связанных с нарушением требований к обеспечению защиты информации при осуществлении банковской деятельности, в соответствии с требованиями Банка России [5];

при информировании Банка России некредитными финансовыми организациями о выявленных инцидентах, связанных с нарушением требований к обеспечению защиты информации при осуществлении деятельности в сфере финансовых рынков, в соответствии с требованиями Банка России [6];

- при информировании Банка России операторами по переводу денежных средств о приостановлении зачисления денежных средств на банковский счет получателя средств или увеличения остатка электронных денежных средств получателя средств в соответствии с требованиями Банка России [20];

Форма запроса Банка России к участнику информационного обмена, обслуживающему получателя средств, применяется:

при запросе у оператора по переводу денежных средств, обслуживающего получателя средств, включая оператора электронных денежных средств, информации, определяющей получателя средств, в соответствии с требованиями Банка России [4];

при направлении уведомления о приостановлении зачисления денежных средств на банковский счет получателя средств или увеличения остатка электронных денежных средств получателя средств в соответствии с требованиями Банка России [20].

Форма представления данных, используемая участниками информационного обмена для представления ответа на запрос Банка России к участнику информационного обмена, обслуживающему получателя средств, применяется:

при информировании Банка России оператором по переводу денежных средств, обслуживающим получателя средств, включая оператора электронных денежных средств, о конкретном получателе средств в соответствии с требованиями Банка России [4];

при направлении уведомления об успешном приостановлении зачисления денежных средств на банковский счет получателя средств или увеличения остатка электронных денежных средств получателя средств в соответствии с требованиями Банка России [20];

при направлении уведомления о невозможности приостановления зачисления денежных средств на банковский счет получателя средств или увеличения остатка электронных денежных средств получателя средств в соответствии с требованиями Банка России [20].

Форма информационного сообщения Банка России участнику информационного обмена, обслуживающему плательщика, применяется:

при направлении уведомления об успешном приостановлении зачисления денежных средств на банковский счет получателя средств или увеличения остатка электронных денежных средств получателя средств в соответствии с требованиями Банка России [20];

при направлении уведомления о невозможности приостановления зачисления денежных средств на банковский счет получателя средств или увеличения остатка электронных денежных средств получателя средств в соответствии с требованиями Банка России [20].

Форма представления данных, используемая участниками информационного обмена для направления запроса в Банк России, об установлении (или снятии) на их банковские (корреспондентские) счета (субсчета) ограничения в виде запрета на списание денежных средств при выявленных инцидентах, связанных с нарушением требований к обеспечению защиты информации, применяется:

при информировании Банка России участниками информационного обмена, использующими сервис срочного перевода и сервис несрочного перевода для осуществления перевода денежных средств, не являющимися подразделениями Банка России, об установлении на их банковские (корреспондентские) счета (субсчета) ограничения в виде запрета на списание денежных средств при выявлении инцидентов, связанных с нарушением требований к обеспечению защиты информации при осуществлении переводов денежных средств, на объектах информационной инфраструктуры участников информационного обмена в соответствии с требованиями Банка России [21];

при информировании Банка России участниками информационного обмена, использующими сервис срочного перевода и сервис несрочного перевода для осуществления перевода денежных средств, не являющимися подразделениями Банка России, о снятии с их банковских (корреспондентских) счетов (субсчетов) ограничения в виде запрета на списание денежных средств при выявлении инцидентов, связанных с нарушением требований к обеспечению защиты информации при осуществлении переводов денежных средств, на объектах информационной инфраструктуры участников информационного обмена в соответствии с требованиями Банка России [21].

Форма информационного сообщения Банка России об установлении или снятии на банковские (корреспондентские) счета (субсчета) участников информационного обмена ограничения в виде запрета на списание денежных средств применяется:

при направлении уведомления участнику информационного обмена в случае положительного результата контроля целостности и принятия к исполнению запросов на установление или снятие ограничения в виде запрета на списание денежных средств в соответствии с требованиями Банка России [21];

при направлении уведомления участнику информационного обмена в случае отрицательного результата контроля целостности и непринятия к исполнению запросов на установление или снятие ограничения в виде запрета на списание денежных средств в соответствии с требованиями Банка России [21].

Форма распространения Банком России среди участников информационного обмена данных о выявленных инцидентах, связанных с нарушением требований к обеспечению защиты информации, применяется при направлении информации, содержащейся в базе данных о случаях и попытках осуществления переводов денежных средств без согласия клиента, в соответствии с требованиями Банка России [4].

Форма представления данных, используемая участниками информационного обмена для направления в Банк России информации о планируемых мероприятиях по раскрытию информации о выявленных инцидентах, связанных с нарушением требований к обеспечению защиты информации, применяется при информировании Банка России оператором по переводу денежных средств, оператором услуг платежной инфраструктуры о вышеуказанных мероприятиях в соответствии с требованиями Банка России [3].

Форма представления данных, используемая участниками информационного обмена для направления в Банк России информации о планируемых мероприятиях по раскрытию информации о выявленных инцидентах, связанных с нарушением требований к защите информации при осуществлении банковской деятельности, применяется при информировании Банка России кредитными организациями о вышеуказанных мероприятиях в соответствии с требованиями Банка России [5].

Форма представления данных, используемая участниками информационного обмена для направления в Банк России информации о планируемых мероприятиях по раскрытию информации о выявленных инцидентах, связанных с нарушением требований к защите информации при осуществлении деятельности в сфере финансовых рынков, применяется при информировании Банка России некредитными финансовыми организациями о вышеуказанных мероприятиях в соответствии с требованиями Банка России [6].

1. Область применения

Настоящий стандарт устанавливает форму и сроки взаимодействия Банка России с участниками информационного обмена по выявлению инцидентов, связанных с нарушением требований к обеспечению защиты информации.

Настоящий стандарт рекомендован для применения путем включения ссылок на него и (или) прямого использования устанавливаемых в нем положений во внутренних документах участников информационного обмена, а также в договорах.

Обязательность применения настоящего стандарта иными организациями может быть установлена соглашением о взаимодействии с Банком России по вопросам противодействия компьютерным атакам.

2. Нормативные ссылки

В настоящем стандарте использованы ссылки на следующие документы:

Федеральный закон от 10 июля 2002 года N 86-ФЗ "О Центральном банке Российской Федерации (Банке России)" [1];

Федеральный закон от 27 июня 2011 года N 161-ФЗ "О национальной платежной системе" [2];

Положение Банка России от 9 июня 2012 года N 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" [3];

Нормативный акт Банка России, устанавливающий формы и порядок направления операторами по переводу денежных средств, операторами платежных систем, операторами услуг платежной инфраструктуры в Банк России информации обо всех случаях и попытках осуществления переводов денежных средств без согласия клиента и получения ими от Банка России информации, содержащейся в базе данных о случаях и попытках осуществления переводов денежных средств без согласия клиента, а также порядок реализации операторами по переводу денежных средств, операторами платежных систем, операторами услуг платежной инфраструктуры мероприятий по противодействию осуществлению переводов денежных средств без согласия клиента [4];

Нормативный акт Банка России, устанавливающий обязательные для кредитных организаций требования к обеспечению защиты информации при осуществлении банковской деятельности [5];

Нормативный акт Банка России, устанавливающий обязательные для некредитных финансовых организаций требования к обеспечению защиты информации при осуществлении деятельности в сфере финансовых рынков [6];

Нормативный акт Банка России, устанавливающий формы и порядок направления операторами по переводу денежных средств уведомлений о приостановлении зачисления денежных средств на банковский счет получателя средств или увеличения остатка электронных денежных средств получателя средств, о невозможности приостановления зачисления денежных средств на банковский счет получателя средств или приостановления увеличения остатка электронных денежных средств получателя средств [20];

Нормативный акт Банка России, устанавливающий требования к обеспечению защиты информации в платежной системе Банка России [21].

3. Термины и определения

В настоящем стандарте применяются термины в соответствии со следующими документами:

Федеральный закон от 27 июня 2011 года N 161-ФЗ "О национальной платежной системе" [2];

Положение Банка России от 9 июня 2012 года N 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" [3];

Нормативный акт Банка России, устанавливающий формы и порядок направления операторами по переводу денежных средств, операторами платежных систем, операторами услуг платежной инфраструктуры в Банк России информации обо всех случаях и попытках осуществления переводов денежных средств без согласия клиента и получения ими от Банка России информации, содержащейся в базе данных о случаях и попытках осуществления переводов денежных средств без согласия клиента, а также порядок реализации операторами по переводу денежных средств, операторами платежных систем, операторами услуг платежной инфраструктуры мероприятий по противодействию осуществлению переводов денежных средств без согласия клиента [4];

Нормативный акт Банка России, устанавливающий обязательные для кредитных организаций требования к обеспечению защиты информации при осуществлении банковской деятельности [5];

Нормативный акт Банка России, устанавливающий обязательные для некредитных финансовых организаций требования к обеспечению защиты информации при осуществлении деятельности в сфере финансовых рынков [6];

Национальный стандарт Российской Федерации ГОСТ Р ИСО/МЭК 15408-3-2013 "Информационная технология. Методы и средства обеспечения безопасности. Критерии оценки безопасности информационных технологий. Часть 3. Компоненты доверия к безопасности" [19];

Нормативный акт Банка России, устанавливающий формы и порядок направления операторами по переводу денежных средств уведомлений о приостановлении зачисления денежных средств на банковский счет получателя средств или увеличения остатка электронных денежных средств получателя средств, о невозможности приостановления зачисления денежных средств на банковский счет получателя средств или приостановления увеличения остатка электронных денежных средств получателя средств [20];

Нормативный акт Банка России, устанавливающий требования к обеспечению защиты информации в платежной системе Банка России [21].

3.1. К инцидентам, связанным с нарушениями требований к обеспечению защиты информации, относятся:

инциденты, связанные с нарушением требований к обеспечению защиты информации при осуществлении переводов денежных средств;

инциденты, связанные с нарушением требований к обеспечению защиты информации при осуществлении банковской деятельности;

инциденты, связанные с нарушением требований к обеспечению защиты информации при осуществлении деятельности в сфере финансовых рынков;

инциденты, связанные с неоказанием или несвоевременным оказанием услуг по переводу денежных средств;

инциденты, связанные с неоказанием или несвоевременным оказанием финансовых (банковских) услуг.

3.2. Для целей настоящего стандарта под инцидентом, связанным с нарушением требований к обеспечению защиты информации, понимается одно или серия связанных нежелательных или неожиданных событий защиты информации, которые могут привести или привели к следующим негативным последствиям:

переводу денежных средств без согласия клиента;

проведению финансовой (банковской) операции без согласия клиента;

неоказанию или несвоевременному оказанию услуг по переводу денежных средств;

неоказанию или несвоевременному оказанию финансовых (банковских) услуг.

К событиям защиты информации относятся следующие события:

а) получение уведомлений участниками информационного обмена, в том числе:

при получении оператором по переводу денежных средств, обслуживающим плательщика, включая оператора электронных денежных средств, уведомлений в предусмотренной договором форме от клиентов - физических, юридических лиц, индивидуальных предпринимателей или лиц, занимающихся частной практикой, о случаях и (или) попытках переводов денежных средств без согласия клиента, в том числе об использовании электронных средств платежа;

при выявлении оператором по переводу денежных средств, обслуживающим плательщика, включая оператора электронных денежных средств, операций, соответствующих признакам осуществления перевода денежных средств без согласия клиента, установленным Банком России и размещаемым на официальном сайте Банка России в сети Интернет;

получение расчетным центром платежной системы от участников платежной системы уведомлений о списании денежных средств с их корреспондентских счетов без их согласия и (или) с использованием искаженной информации, содержащейся в распоряжениях платежных клиринговых центров или участников платежной системы;

получение уведомлений от клиентов - физических лиц, и (или) индивидуальных предпринимателей, и (или) лиц, занимающихся в установленном законодательством Российской Федерации порядке частной практикой, и (или) юридических лиц о проведении финансовой (банковской) операции без их согласия;

б) идентифицированное возникновение и (или) изменение состояния совокупности объектов и ресурсов доступа, средств и систем обработки информации, в том числе автоматизированных систем (далее - АС), используемых для обеспечения информатизации бизнес-процессов и (или) технологических процессов участников информационного обмена, приводящее к следующим последствиям:

выявлению оператором по переводу денежных средств, обслуживающим плательщика, включая оператора электронных денежных средств, операций по переводу денежных средств и получению наличных денежных средств, совершенных в результате несанкционированного доступа к объектам информационной инфраструктуры оператора по переводу денежных средств, в том числе при уменьшении остатка электронных денежных средств, за исключением виртуальных платежных карт;

выполнению финансовых (банковских) операций в результате несанкционированного доступа к объектам информационной инфраструктуры некредитной финансовой организации;

осуществлению несанкционированного снятия денежных средств оператора по переводу денежных средств в банкоматах;

осуществлению несанкционированного снятия денежных средств оператора электронных денежных средств в банкоматах;

неоказанию или несвоевременному оказанию оператором по переводу денежных средств услуг по переводу денежных средств;

неоказанию или несвоевременному оказанию расчетным центром значимой платежной системы расчетных услуг;

неоказанию или несвоевременному оказанию платежным клиринговым центром значимой платежной системы услуг платежного клиринга;

неоказанию или несвоевременному оказанию операционным центром значимой платежной системы операционных услуг;

неоказанию или несвоевременному оказанию финансовых (банковских) услуг;

выявлению оператором по переводу денежных средств, включая оператора электронных денежных средств, и (или) оператором услуг платежной инфраструктуры атак, последствия от реализации которых могут привести к случаям и попыткам осуществления переводов денежных средств без согласия клиента.

4. Обозначения и сокращения

DDoS (Distributed Denial of Service) - распределенная атака типа "отказ в обслуживании" с одновременным использованием большого числа атакующих компьютеров, целью которой, как правило, является частичное нарушение штатного функционирования информационной инфраструктуры организации

IPv4 (Internet Protocol version 4) - четвертая версия интернет-протокола

URL (Uniform Resource Locator) - единый указатель ресурса

АС - автоматизированная система

БИН - банковский идентификационный номер - часть номера, расположенного на платежной карте, используемая для идентификации банка-эмитента в рамках "карточной" платежной системы при авторизации, процессинге и клиринге

Ботнет - компьютерная сеть, состоящая из узлов с запущенным однотипным централизованно управляемым вредоносным программным обеспечением

ВК - вредоносный код

ВВК - воздействие вредоносного кода

КИИ - критическая информационная инфраструктура

ОГРН - основной государственный регистрационный номер

ОКОПФ - Общероссийский классификатор организационно-правовых форм

ОКТМО - Общероссийский классификатор территорий муниципальных образований

ОС - операционная система

Сеть Интернет - информационно-телекоммуникационная сеть "Интернет"

СКЗИ - средство криптографической защиты информации

СНИЛС - страховой номер индивидуального лицевого счета застрахованного лица в системе персонифицированного учета Пенсионного фонда Российской Федерации

5. Форма представления данных, используемая участниками информационного обмена для регистрации в Банке России

5.1. Условия обязательности и временные характеристики информирования

Условия обязательности информирования:

[O] - информация блока (поля) данных представляется в обязательном порядке;

[N] - информация блока (поля) данных представляется в случае наличия технической возможности.

Временные характеристики информирования (этапы информирования):

[1] - информация блока (поля) данных представляется в рамках регистрации участника информационного обмена;

[2] - информация блока (поля) данных представляется в рамках изменения регистрационных данных участника информационного обмена.

5.2. Регистрационные данные участника информационного обмена. Блок данных [HEADER]

Номер блока (поля) данных	Идентификатор блока (поля) данных	Содержание блока (поля) данных	Формат поля данных	Формат электронного сообщения	Обязательность информирования	Этапы информирования
1.1	"schemaType" (поле данных)	тип электронного сообщения	Указывается значение [PARTICIPANT] - участник информационного обмена	{"header": {"schemaType": "participant","schemaVersion": "1","version": "1","memberId": "9527dd0c-0765-4f1c-8f5f-70a02cf4046c","sourceId": "f34030ef-358a-445c-8567-25985ce6d91c","publishedAt": "2002-10-02T15:00:00.05Z","modifiedAt": "2002-10-02T15:00:00.05Z"},	[O]	[1], [2]
1.2	"schemaVersion" (поле данных)	версия схемы типа электронного сообщения	текстовое поле (textarea)		[O]	[1], [2]
1.3	"version" (поле данных)	номер версии электронного сообщения в процессе информационного обмена	числовое значение (int)		[O]	[1], [2]
1.4	"memberId" (поле данных)	идентификатор участника информационного обмена, присвоенный Банком России	128-битный идентификатор (GUID), сформированный в соответствии со спецификацией RFC 4122 [16], присвоенный Банком России		[O]	[2]
1.5	"sourceId" (поле данных)	идентификатор, присвоенный участником информационного обмена	128-битный идентификатор (GUID), сформированный в соответствии со спецификацией RFC 4122 [16], присвоенный участником информационного обмена		[O]	[1], [2]
1.6	"publishedAt" (поле данных)	дата и время регистрации участника информационного обмена	формат представления данных в соответствии со спецификацией RFC 3339 [11]		[O]	[1], [2]
1.7	"modifiedAt" (поле данных)	дата и время изменения регистрационных данных участника информационного обмена	формат представления данных в соответствии со спецификацией RFC 3339 [11]		[O]	[2]

5.3. Регистрационные данные участника информационного обмена. Блок данных [PARTICIPANT]

Номер блока (поля) данных	Идентификатор блока (поля) данных	Содержание блока (поля) данных	Формат поля данных	Формат электронного сообщения	Обязат информ
			Определяется типом участника информационного обмена: - участник информационного обмена, осуществляющий деятельность оператора по переводу денежных средств, - номер лицензии, выданной Банком России; - участник информационного обмена, осуществляющий деятельность оператора услуг платежной инфраструктуры, - регистрационный номер оператора услуг платежной		

2.1	"orgId" (поле данных)	идентификатор участника информационного обмена	инфраструктуры; - участник информационного обмена, осуществляющий деятельность оператора платежной системы, - регистрационный номер оператора платежной системы; - участник информационного обмена, осуществляющий деятельность профессионального участника рынка ценных бумаг, - номер лицензии, выданной Банком России; - участник информационного обмена, осуществляющий деятельность управляющей компании инвестиционного фонда, паевого инвестиционного фонда и негосударственного пенсионного фонда, - номер лицензии, выданной Банком России; - участник информационного обмена, осуществляющий деятельность специализированного депозитария инвестиционного фонда, паевого инвестиционного фонда и негосударственного пенсионного фонда, - номер лицензии, выданной Банком России; - участник информационного обмена, осуществляющий деятельность акционерного инвестиционного фонда, - номер лицензии, выданной Банком России; - участник информационного обмена, осуществляющий клиринговую деятельность, - номер лицензии, выданной Банком России; - участник информационного обмена, осуществляющий деятельность по выполнению функций центрального контрагента, - регистрационный номер из книги государственной регистрации кредитных организаций;	"participant": {"orgId": "идентификатор типа участника информационного обмена","orgBrand": "наименование бренда участника информационного обмена","orgShortName": "сокращенное наименование участника информационного обмена","orgFullName": "полное наименование участника информационного обмена","orgE-mails": ["qwerty1@example.ru", "qwerty2@example.ru"],"orgIncomingEmail": "requestsFromfincert@example.ru","orgBik": "123456789","orgLegalEntityForm": "12345","orgBin": ["123456", "123456"],"orgInn": "1234567890","orgKpp": "123456789","orgOgrn": "1234567890000","isp": [{"name": "наименование оператора связи","ipAddress": ["192.168.1.0", "192.168.2.0"]}],"software": [{"sourceId": "f34030ef-358a-445c-8567-25985ce6d91c","type": "тип программного/аппаратного обеспечения участника информационного обмена","name": "наименование программного/аппаратного обеспечения","version": "версия используемого программного/аппаратного обеспечения","description": "дополнительное описание программного/аппаратного обеспечения"}],"persons": [{"memberId": "9527dd0c-0765-4f1c-8f5f-70a02cf4046c","sourceId": "f34030ef-358a-445c-8567-25985ce6d91c","lastName": "фамилия","middleName": "отчество","firstName": "имя","landlineNumber": "1234567890000","mobileNumber": "1234567890000","email": "qwerty1@example.ru","position": "должность","active": "наличие доступа в личный кабинет участника информационного обмена","category": "категория структурного подразделения ответственного лица участника информационного обмена"}],

			- участник информационного обмена, осуществляющий деятельность организатора торговли, - номер лицензии, выданной Банком России (справочник участников финансового рынка); - участник информационного обмена, осуществляющий деятельность центрального депозитария, - ОГРН; - участник информационного обмена, осуществляющий репозитарную деятельность, - номер лицензии, выданной Банком России; - участник информационного обмена, осуществляющий деятельность субъекта страхового дела, - номер лицензии, выданной Банком России; - участник информационного обмена, осуществляющий деятельность негосударственного пенсионного фонда, - номер лицензии, выданной Банком России (справочник участников финансового рынка); - участник информационного обмена, осуществляющий деятельность микрофинансовой организации, - регистрационный номер записи в государственном реестре микрофинансовых организаций; - участник информационного обмена, осуществляющий деятельность кредитного потребительского кооператива, - ОГРН; - участник информационного обмена, осуществляющий деятельность жилищного накопительного кооператива, - ОГРН; - участник информационного обмена, осуществляющий деятельность бюро кредитных историй, - номер в государственном реестре бюро	"id_cii": "идентификатор объекта КИИ","orgType": "тип участника информационного обмена","legalAddress": {"oktmo": "12345678","postalCode": "почтовый индекс","country": "трехбуквенный код страны","federalDistrict": "код федерального округа","subjectOfFederation": "00","fiasId": "e6668cfd-ae08-4b02-a385-88179dfb1097","district": "район","city": "город","cityDistrict": "внутригородской район","locality": "населенный пункт","street": "улица","house": "номер дома","building": "корпус/строение","room": "комната/кабинет","additionalInformation": "дополнительная информация"},"postAddress": {"oktmo": "12345678","postalCode": "почтовый индекс","country": "трехбуквенный код страны","federalDistrict": "код федерального округа","subjectOfFederation": "00","fiasId": "8abe47a7-24dd-4951-ae16-f2781eba9d93","district": "район","city": "город","cityDistrict": "внутригородской район","locality": "населенный пункт","street": "улица","house": "номер дома","building": "корпус/строение","room": "комната/кабинет","additionalInformation": "дополнительная информация"},"physicalAddress": [{"oktmo": "12345678","postalCode": "почтовый индекс","country": "трехбуквенный код страны","federalDistrict": "код федерального округа","subjectOfFederation": "00","fiasId": "8661e93f-6c6a-4b19-b485-14e27e564169","district": "район","city": "город","cityDistrict": "внутригородской район","locality": "населенный пункт","street": "улица","house": "номер дома","building": "корпус/строение","room": "комната/кабинет","additionalInformation": "дополнительная информация"}]}}	

			кредитных историй; - участник информационного обмена, осуществляющий актуарную деятельность - регистрационный номер записи о внесении сведений в единый реестр ответственных актуариев; - участник информационного обмена, осуществляющий деятельность кредитного рейтингового агентства, - номер выданного бланка свидетельства о внесении сведений о юридическом лице в реестр кредитных рейтинговых агентств;		
			- участник информационного обмена, осуществляющий деятельность сельскохозяйственного кредитного потребительского кооператива, - номер в государственном реестре сельскохозяйственных кредитных потребительских кооперативов; - участник информационного обмена, осуществляющий деятельность ломбарда, - номер в государственном реестре ломбардов; - участник информационного обмена (государственные органы, иностранные организации, провайдеры, разработчики программного обеспечения, центры компетенции по противодействию киберугрозам) - полное наименование организации		
2.2	"orgBrand" (поле данных)	наименование бренда участника информационного обмена	текстовое поле (textarea)		
2.3	"orgShortName" (поле данных)	сокращенное наименование участника информационного обмена	текстовое поле (textarea)		
2.4	"orgFullName" (поле данных)	полное наименование участника информационного обмена	текстовое поле (textarea)		
2.5	"orgEmails" (поле данных)	адреса групповых почтовых ящиков участника информационного обмена	Адреса электронных почтовых ящиков участника информационного обмена представляются в формате в соответствии со спецификацией RFC 5322 [18]		

2.6	"orgIncomingEmail" (поле данных)	адрес почтового ящика участника информационного обмена для получения сообщений от Банка России	Адрес электронного почтового ящика для получения сообщений от Банка России представляется в формате в соответствии со спецификацией RFC 5322 [18]		
2.7	"orgBik" (поле данных)	БИК участника информационного обмена	в формате AAAAAAAAA		
2.8	"orgLegalEntityForm" (поле данных)	код ОКОПФ участника информационного обмена	в формате пяти цифр - XXXXX		
2.9	"orgBin" (поле данных)	БИН участника информационного обмена	в формате шести цифр - XXXXXX		
2.10	"orgInn" (поле данных)	ИНН участника информационного обмена	в формате XXXXXXXXXX		
2.11	"orgKpp" (поле данных)	КПП участника информационного обмена	в формате девятизначного кода - NNNNPPXXX		
2.12	"orgOgrn" (поле данных)	ОГРН участника информационного обмена	13 цифр в формате СГГККННХХХХХЧ		
2.13	"isp" (блок данных)	идентификатор оператора связи	В случае необходимости указания нескольких значений полей данных (name, ipAddress) указывается один или несколько объектов в блоке данных "isp"		
2.13.1	"name" (поле данных)	наименование оператора связи	текстовое поле (textarea)		
2.13.2	"ipAddress" (поле данных)	внешние IP-адреса участника информационного обмена	Логические адреса вида IPv4 должны соответствовать спецификации RFC 791 [12]		
2.14	"software" (блок данных)	состав используемого программного/аппаратного обеспечения	В случае необходимости указания нескольких значений полей данных (sourceId, type, name, version, description) указывается один или несколько объектов в блоке данных "software"		
2.14.1	"sourceId" (поле данных)	идентификатор, присвоенный участником информационного обмена	128-битный идентификатор (GUID), сформированный в соответствии со спецификацией RFC 4122 [16], присвоенный участником информационного обмена		
			Выбирается один код из ограниченного множества возможных значений: 1) системные уровни: - [hw] - аппаратное обеспечение, - [net] - сетевое оборудование, - [net_s] - сетевые приложения и сервисы, - [hw_s] - серверные компоненты виртуализации, программные инфраструктурные сервисы, - [os] - операционные системы, системы управления базами данных, серверы приложений;		

2.14.2	"type" (поле данных)	тип программного/аппаратного обеспечения участника информационного обмена	2) уровень АС и приложений, эксплуатируемых для предоставления услуг в рамках бизнес-процессов или технологических процессов участника информационного обмена: - [rbs] - система дистанционного банковского обслуживания, - [front-office] - система обработки транзакций, осуществляемых с использованием платежных карт, - [web] - информационные ресурсы сети Интернет, - [abs] - автоматизированная банковская система, - [back-office] - система посттранзакционного обслуживания операций, осуществляемых с использованием платежных карт, - [int-services] - внутренняя информационная инфраструктура, направленная на поддержание бизнес-процессов участника информационного обмена (почтовые серверы, файловые серверы); - [participant_w] - оконечное оборудование (АРМ), используемые работниками участника информационного обмена.		
2.14.3	"name" (поле данных)	наименование используемого программного/аппаратного обеспечения	текстовое поле (textarea)		
2.14.4	"version" (поле данных)	версия используемого программного/аппаратного обеспечения	текстовое поле (textarea)		
2.14.5	"description" (поле данных)	дополнительное описание используемого программного/аппаратного обеспечения	текстовое поле (textarea)		
2.15	"persons" (блок данных)	идентификаторы ответственного лица	В случае необходимости указания нескольких значений полей данных (memberId, sourceId, lastName, middleName, firstName, landlineNumber, mobileNumber, email, position, active) указывается один или несколько объектов в блоке данных "persons"		
2.15.1	"memberId" (поле данных)	идентификатор ответственного лица участника информационного обмена, присвоенный Банком России	128-битный идентификатор (GUID), сформированный в соответствии со спецификацией RFC 4122 [16], присвоенный Банком России		

2.15.2	"sourceId" (поле данных)	идентификатор ответственного лица в системе участника информационного обмена	128-битный идентификатор (GUID), сформированный в соответствии со спецификацией RFC 4122 [16], присвоенный участником информационного обмена		
2.15.3	"lastName" (поле данных)	фамилия	текстовое поле (textarea)		
2.15.4	"middleName" (поле данных)	отчество	текстовое поле (textarea)		
2.15.5	"firstName" (поле данных)	имя	текстовое поле (textarea)		
2.15.6	"landlineNumber" (поле данных)	городской телефон	текстовое поле (textarea)		
2.15.7	"mobileNumber" (поле данных)	мобильный телефон	текстовое поле (textarea)		
2.15.8	"email" (поле данных)	электронный адрес	текстовое поле (textarea)		
2.15.9	"position" (поле данных)	должность	текстовое поле (textarea)		
2.15.10	"active" (поле данных)	наличие доступа в личный кабинет участника информационного обмена	Выбирается один код из ограниченного множества возможных значений: - [ACT] - доступ в личный кабинет участника информационного обмена активирован; - [DIS] - доступ в личный кабинет участника информационного обмена не активирован		
2.15.11	"category" (поле данных)	категория структурного подразделения ответственного лица участника информационного обмена	Выбирается один код из ограниченного множества возможных значений: - [MANAGEMENT] - высшее руководство; - [SECURITY] - подразделения информационной безопасности; - [IT] - подразделения информатизации; - [RISKS] - подразделения по управлению рисками; - [PAYMENT] - операционные подразделения; - [OTHER] - иные структурные подразделения		
2.16	"ID_CII" (поле данных)	идентификатор объекта КИИ	текстовое поле (textarea)		

2.17	"orgType" (поле данных)	тип участника информационного обмена	Выбирается один код из ограниченного множества возможных значений: - [PSP] - участник информационного обмена, осуществляющий деятельность оператора по переводу денежных средств; - [SOPI] - участник информационного обмена, осуществляющий деятельность оператора услуг платежной инфраструктуры; - [PS] - участник информационного обмена, осуществляющий деятельность оператора платежной системы. Некредитные финансовые организации: - [PSB] - участник информационного обмена, осуществляющий деятельность профессионального участника рынка ценных бумаг; - [MOF] - участник информационного обмена, осуществляющий деятельность управляющей компании инвестиционного фонда, паевого инвестиционного фонда и негосударственного пенсионного фонда;		
			- [SDIF] - участник информационного обмена, осуществляющий деятельность специализированного депозитария инвестиционного фонда, паевого инвестиционного фонда и негосударственного пенсионного фонда; - [IncIF] - участник информационного обмена, осуществляющий деятельность акционерного инвестиционного фонда; - [CC] - участник информационного обмена, осуществляющий клиринговую деятельность; - [CCOUNT] - участник информационного обмена, осуществляющий деятельность по выполнению функций центрального контрагента;		

			- [TDO] - участник информационного обмена, осуществляющий деятельность организатора торговли; - [CD] - участник информационного обмена, осуществляющий деятельность центрального депозитария; - [RO] - участник информационного обмена, осуществляющий репозитарную деятельность; - [SIB] - участник информационного обмена, осуществляющий деятельность субъектов страхового дела; - [NGPF] - участник информационного обмена, осуществляющий деятельность негосударственного пенсионного фонда; - [MFO] - участник информационного обмена, осуществляющий деятельность микрофинансовой организации; - [CCC] - участник информационного обмена, осуществляющий деятельность кредитного потребительского кооператива; - [HCCC] - участник информационного обмена, осуществляющий деятельность жилищного накопительного кооператива; - [CHB] - участник информационного обмена, осуществляющий деятельность бюро кредитных историй; - [AA] - участник информационного обмена, осуществляющий актуарную деятельность;		
			- [CRA] - участник информационного обмена, осуществляющий деятельность кредитного рейтингового агентства; - [ACCC] - участник информационного обмена, осуществляющий деятельность сельскохозяйственного кредитного потребительского		

			кооператива; - [PWS] - участник информационного обмена, осуществляющий деятельность ломбарда. Государственные органы: - [FED] - участник информационного обмена - федеральный орган исполнительной власти; - [REG] - участник информационного обмена - орган исполнительной власти субъекта Российской Федерации; - [localGov] - участник информационного обмена - орган местного самоуправления; - [LEA] - правоохранительные органы. Операторы связи: - [MO] - участник информационного обмена - оператор сотовой связи; - [ISP] - участник информационного обмена - интернет-провайдер; Разработчики программного обеспечения: - [devBANK] - участник информационного обмена - разработчик прикладного программного обеспечения для финансовой (банковской) деятельности; - [devVIRUS] - участник информационного обмена - разработчик средств защиты от воздействия вредоносного кода (далее - средств от ВВК); - [devOTHER] - участник информационного обмена - иной разработчик программного обеспечения. Иностранные организации: - [FNB] - участник информационного обмена - иностранный центральный (национальный) банк; - [FB] - участник информационного обмена - иностранный банк; - [FOTHER] - участник информационного обмена - иная иностранная организация. Центры компетенции по противодействию киберугрозам:		

			- [CERTRUS] - участник информационного обмена - российский центр по противодействию киберугрозам; - [CERTINT] - участник информационного обмена - иностранный центр по противодействию киберугрозам; - [OTHER] - участник информационного обмена - иная организация		
2.18	"legalAddress" (блок)	юридический адрес участника информационного обмена	перечисление текстовых полей (textarea)		
2.19	"postAddress" (блок данных данных)	почтовый адрес участника информационного обмена	перечисление текстовых полей (textarea)		
2.20	"physicalAddress" (блок данных)	фактический адрес участника информационного обмена	перечисление текстовых полей (textarea)		

<1> Обязательность информирования устанавливается только для кредитных организаций.

6. Форма представления данных, используемая участниками информационного обмена для информирования Банка России об инцидентах, связанных с нарушением требований к обеспечению защиты информации, и сроки их представления в Банк России

6.1. Условия обязательности и временные характеристики информирования

Условия обязательности информирования:

[O] - информация блока (поля) данных представляется в обязательном порядке;

[N] - информация блока (поля) данных представляется в случае наличия технической возможности.

Временные характеристики информирования (этапы информирования):

[1] - информация блока (поля) данных представляется в рамках первичного уведомления (для значимых субъектов критической информационной инфраструктуры информация направляется в Банк России в течение трех часов с момента выявления инцидента, для иных участников информационного обмена - в течение 24 часов с момента выявления инцидента);

[2] - информация блока (поля) данных представляется в рамках промежуточного уведомления (для значимых субъектов критической информационной инфраструктуры информация направляется в Банк России в течение трех часов с момента выявления инцидента, для иных участников информационного обмена - в течение двух рабочих дней с момента первичного уведомления или предыдущего промежуточного уведомления);

[3] - информация блока (поля) данных представляется в рамках окончательного уведомления по результатам закрытия инцидента (в течение трех рабочих дней с момента закрытия инцидента участником информационного обмена).

[*] - информация блока (поля) данных представляется в незамедлительном порядке в случае получения от клиента участника информационного обмена - юридического лица уведомления, указанного в части 11 статьи 9 Федерального закона от 27 июня 2011 года N 161-ФЗ "О национальной платежной системе".

6.2. Идентификационные данные инцидента. Блок данных [HEADER]

Номер блока (поля) данных	Идентификатор блока (поля) данных	Содержание блока (поля) данных	Формат поля данных	Формат электронного сообщения	Обязательность информирования	Этапы информирования
1.1	"schemaType" (поле данных)	тип электронного сообщения	Указывается значение [INCIDENT] - инцидент	{"header": {"schemaType": "incident","schemaVersion": "1","version": "1","memberId": "9527dd0c-0765-4f1c-8f5f-70a02cf4046c","sourceId": "f34030ef-358a-445c-8567-25985ce6d91c","publishedAt": "2002-10-02T15:00:00.05Z","modifiedAt": "2002-10-02T15:00:00.05Z"},	[O]	[1], [2], [3], [*]
1.2	"schema Version" (поле данных)	версия схемы типа электронного сообщения	текстовое поле (textarea)		[O]	[1], [2], [3], [*]
1.3	"version" (поле данных)	номер версии электронного сообщения в процессе информационного обмена	числовое значение (int)		[O]	[1], [2], [3], [*]
1.4	"memberId" (поле данных)	идентификатор участника информационного обмена, присвоенный Банком России	128-битный идентификатор (GUID), сформированный в соответствии со спецификацией RFC 4122 [16], присвоенный Банком России		[O]	[1], [2], [3], [*]
1.5	"sourceId" (поле данных)	идентификатор инцидента, присвоенный участником информационного обмена	128-битный идентификатор (GUID), сформированный в соответствии со спецификацией RFC 4122 [16], присвоенный участником информационного обмена		[O]	[1], [2], [3], [*]
1.6	"publishedAt" (поле данных)	дата и время первичного информирования	формат представления данных в соответствии со спецификацией RFC 3339 [11]		[O]	[1], [2], [3], [*]
1.7	"modifiedAt" (поле данных)	дата и время промежуточного или окончательного уведомления	формат представления данных в соответствии со спецификацией RFC 3339 [11]		[O]	[2], [3]

6.3. Описание инцидента. Блок данных [INCIDENT]

Номер блока (поля) данных	Идентификатор блока (поля) данных	Содержание блока (поля) данных	Формат поля данных	Формат электронного сообщен

2.1	"fincertId" (поле данных)	идентификатор инцидента, присвоенный Банком России	текстовое поле (textarea)	"incident": {"fincertId": "20180324215113","fixationAt": "2 10-02T15:00:00.05Z","description" "описание инцидента","lawEnforcementRequ {"addressed": "субъект, обратившийся в правоохранител органы","request": "информация факте обращения в полицию участника информационного обмена","number": "123123","numberTicket": "1234567890","dateTimeAt": "200 02T15:00:00.05Z"},"assistance": "идентификатор необходимости оказания поддержки участнику информационного обмена со сто Банка России","vectorCode": "идентификатор вектора компьютерной атаки","serviceTyp [{"sourceId": "f34030ef-358a-445c 8567-25985av6d91c","type": "тип атакуемого объекта","name": "наименование программного/аппаратного обеспечения","version": "версия программного/аппаратного обеспечения","description": "дополнительное описание типа атакуемого объекта"}],"registrati {"department": "структурное (организационное) подразделени участника информационного обм где инцидент был зарегистриров (выявлен)","technicalDevice": "техническое средство регистра инцидента"},"typeOfAttack": "код типа компьютерной атаки","measuresAndRecomendati [{"sourceId": "f34030ef-358a-445c 8567-25985ce6d91c","dateTimeAt" "2018-03-22T08:14:38Z","action": "предпринятые действия по ликвидации инцидента","text": " принятых мер или рекомендаций","attachment": {"sourceId": "f34030ef-358a-445c- 25985ce6d91c","comment": "опис вложения","dateTimeAt": "2018-0 22T08:14:38Z","file": {"name": "им файла","size": "размер файла в байтах","base64": "вложение в формате base64"},"fileLink": "http://domain.com/archive.rar"}}]
2.2	"fixationAt" (поле данных)	дата и время регистрации инцидента участником информационного обмена	формат представления данных в соответствии со спецификацией RFC 3339 [11]	
2.3	"description" (поле данных)	описание инцидента	текстовое поле (textarea)	
2.4	"lawEnforcementRequest" (блок данных)	обращение участника информационного обмена в правоохранительные органы		
2.4.1	"addressed" (поле данных)	субъект, обратившийся в правоохранительные органы	Выбирается один код из ограниченного множества возможных значений: - [PIE] - участник информационного обмена; - [CIE] - клиент участника информационного обмена	
2.4.2	"request" (поле данных)	информация о факте обращения в правоохранительные органы участника информационного обмена	Выбирается один код из ограниченного множества возможных значений: - [POL] - направлено обращение в правоохранительные органы; - [NPL] - обращение в правоохранительные органы не направлено	
2.4.3	"number" (поле данных)	номер заявления из книги учета сообщений о преступлениях	числовое значение (int)	
2.4.4	"numberTicket" (поле данных)	номер талона-корешка о приеме и регистрации заявления	числовое значение (int)	
2.4.5	"dateTimeAt" (поле данных)	дата и время принятия заявления	формат представления данных в соответствии со спецификацией RFC 3339 [11]	
2.5	"assistance" (поле данных)	идентификатор необходимости оказания поддержки участнику информационного обмена со стороны Банка России	Выбирается один код из ограниченного множества возможных значений: - [HLP] - необходима поддержка от Банка России; - [NND] - поддержка от Банка России не требуется	
2.6	"vectorCode" (поле данных)	идентификатор вектора компьютерной атаки	Выбирается один код из ограниченного множества возможных значений: - вектор [INT] - направленный на инфраструктуру участника информационного обмена; - вектор [EXT] - направленный на клиента участника информационного обмена	
2.7	"serviceType" (блок данных)	идентификатор объекта информационной инфраструктуры	В случае необходимости указания нескольких значений полей данных (sourceId, type, name, version, description) указывается один или несколько объектов в блоке данных "serviceType"	
2.7.1	"sourceId" (поле данных)	идентификатор, присвоенный участником информационного обмена	128-битный идентификатор (GUID), сформированный в соответствии со спецификацией RFC 4122 [16], присвоенный участником информационного обмена	

2.7.2	"type" (поле данных)	тип атакуемого объекта	Выбирается один код из ограниченного множества возможных значений: 1) системные уровни: - [hw] - аппаратное обеспечение, - [net] - сетевое оборудование, - [net_s] - сетевые приложения и сервисы, - [hw_s] - серверные компоненты виртуализации, программные инфраструктурные сервисы, - [os] - операционные системы, системы управления базами данных, серверы приложений;
			2) уровень АС и приложений, эксплуатируемых для предоставления услуг в рамках бизнес-процессов или технологических процессов участника информационного обмена: - [rbs] - система дистанционного банковского обслуживания, - [front-office] - система обработки транзакций, осуществляемых с использованием платежных карт, - [web] - информационные ресурсы сети Интернет, - [abs] - автоматизированная банковская система, - [back-office] - система посттранзакционного обслуживания операций, осуществляемых с использованием платежных карт; - [int-services] - внутренняя информационная инфраструктура, направленная на поддержание бизнес-процессов участника информационного обмена (почтовые серверы, файловые серверы); - [participant_w] - оконечное оборудование (АРМ), используемые работниками участника информационного обмена;
			3) уровень АС и приложений, эксплуатируемых клиентом участника информационного обмена: - [cfs] - файловый сервер, - [crbs] - система дистанционного банковского обслуживания, - [ecs] - сервер электронной почты; - [client_w] - автоматизированные системы, используемые работниками клиента участника информационного обмена;
			4) иная система: - [oth] - иная система
2.7.3	"name" (поле данных)	наименование программного/аппаратного обеспечения	текстовое поле (textarea)
2.7.4	"version" (поле данных)	версия программного/аппаратного обеспечения	текстовое поле (textarea)
2.7.5	"description" (поле данных)	дополнительное описание типа атакуемого объекта	текстовое поле (textarea)

2.8	"registration" (блок данных)	идентификатор локализации инцидента		
2.8.1	"department" (поле данных)	атакуемое структурное (организационное) подразделение участника информационного обмена, где инцидент был зарегистрирован (выявлен)	текстовое поле (textarea)	
2.8.2	"technicalDevice" (поле данных)	техническое средство регистрации инцидента	текстовое поле (textarea)	
2.9	"typeOfAttack" (поле данных)	идентификатор типа компьютерной атаки	Выбирается один код из ограниченного множества возможных значений: - [trafficHijackAttacks] - компьютерные атаки, связанные с изменением маршрутно-адресной информации; - [malware] - компьютерные атаки, связанные с использованием вредоносного программного обеспечения применительно к объектам информационной инфраструктуры участников информационного обмена и их клиентов; - [socialEngineering] - компьютерные атаки, возникшие в результате побуждения клиентов к осуществлению операций по переводу денежных средств путем обмана или злоупотребления доверием; - [ddosAttacks] - компьютерные атаки типа "отказ в обслуживании" (DDoS-атаки) применительно к информационной инфраструктуре участников информационного обмена; - [atmAttacks] - компьютерные атаки, связанные с реализацией несанкционированного доступа к банкоматам и платежным терминалам участников информационного обмена; - [vulnerabilities] - компьютерные атаки, связанные с эксплуатацией уязвимостей информационной инфраструктуры участников информационного обмена и их клиентов; - [bruteForces] - компьютерные атаки, связанные с подбором (взломом), компрометацией аутентификационных (учетных) данных; - [spams] - компьютерные атаки, связанные с реализацией спам-рассылки, осуществляемой в отношении участников информационного обмена и их клиентов; - [controlCenters] - компьютерные атаки, связанные с выявлением взаимодействия объектов информационной инфраструктуры участников информационного обмена с командными центрами Ботнет;	

			- [sim] - компьютерные атаки, связанные с изменением (подменой) идентификатора мобильного абонента (IMSI) номера сим-карты, а также с заменой идентификатора мобильного оборудования (IMEI); - [phishingAttacks] - компьютерные атаки, связанные с информацией, вводящей участников информационного обмена и их клиентов, а также иных лиц, взаимодействующих с ними, в заблуждение относительно принадлежности информации, распространяемой посредством сети Интернет, вследствие сходства доменных имен, оформления или содержания; - [prohibitedContents] - компьютерные атаки, связанные с распространением информации, касающейся предложения и (или) предоставления на территории Российской Федерации финансовых услуг лицами, не имеющими права их оказывать в соответствии с законодательством Российской Федерации. Размещение в сети Интернет запрещенного контента; - [maliciousResources] - компьютерные атаки, связанные с размещением в сети Интернет информации, позволяющей осуществить неправомерный доступ к информационным системам участников информационного обмена и их клиентов, используемым при предоставлении (получении) финансовых услуг, в том числе путем неправомерного доступа к конфиденциальной информации клиентов. Размещение в сети Интернет вредоносного ресурса; - [changeContent] - компьютерные атаки, связанные с изменением контента; - [scanPorts] - компьютерные атаки, связанные со сканированием программных портов объектов информационной инфраструктуры участников информационного обмена лицами, не обладающими соответствующими полномочиями; - [other] - иные компьютерные атаки, направленные на объекты информационной инфраструктуры участников информационного обмена и их клиентов	
2.10	"measuresAndRecomendations" (блок данных)	предпринятые действия по ликвидации инцидента	В случае необходимости указания нескольких значений полей данных (sourceId, dateTimeAt, action, text) указывается один или несколько объектов в блоке данных "measuresAndRecomendations"	

2.10.1	"sourceId" (поле данных)	идентификатор, присвоенный участником информационного обмена	128-битный идентификатор (GUID), сформированный в соответствии со спецификацией RFC 4122 [16], присвоенный участником информационного обмена
2.10.2	"dateTimeAt" (поле данных)	дата и время выполнения действий по ликвидации инцидента	формат представления данных в соответствии со спецификацией RFC 3339 [11]
2.10.3	"action" (поле данных)	предпринятые действия по ликвидации инцидента	Выбирается один код из ограниченного множества возможных значений:- [measures] - принятые меры;- [recommendations] - рекомендации
2.10.4	"text" (поле данных)	принятые меры или рекомендации	текстовое поле (textarea)
2.10.5	"attachment" (блок данных)	дополнительные данные о принятых мерах по ликвидации инцидента	
2.10.5.1	"sourceId" (поле данных)	идентификатор, присвоенный участником информационного обмена	128-битный идентификатор (GUID), сформированный в соответствии со спецификацией RFC 4122 [16], присвоенный участником информационного обмена
2.10.5.2	"comment" (поле данных)	описание вложения	текстовое поле (textarea)
2.10.5.3	"dateTimeAt" (поле данных)	дата и время добавления файла	формат представления данных в соответствии со спецификацией RFC 3339 [11]
2.10.5.4	"file" (блок данных)	файл данных	Указывается наименование, размер файла (не более 5 Мб), выполняется кодировка в формате Base64
2.10.5.5	"fileLink" (поле данных)	ссылка для получения (скачивания) файла данных	Указывается URL-адрес для скачивания файла, в случае если его размер превышает 5 Мб, в соответствии со спецификацией RFC 3986 [15]

6.4. Классификация инцидента. Блок данных [INCIDENT]

Номер блока (поля) данных	Идентификатор блока (поля) данных	Содержание блока (поля) данных	Формат поля данных	Формат электронного сообщения	Обязательность информирования	Эт информ

3.1	"location" (блок данных)	идентификатор географического местоположения реализации инцидента		"location": {"subjectOfFederation": "00","locality": "наименование населенного пункта"},"classification": {"typeOfIncident": "тип инцидента","ext": [{"events": "события защиты информации","method": "способ формирования и передачи распоряжений на осуществление транзакций, позволяющий совершить финансовую операцию"}],"int": [{"events": "события защиты информации","typeOfIntruder": "тип нарушителя"}],"damage": {"operating": "оценка операционных расходов участника информационного обмена в момент представления сведений о реализации инцидента (вектор INT)","relative": "относительная (качественная) оценка масштаба (тяжести последствий) от реализации инцидента (вектор INT)"},"schemaConclusion": "описание схемы вывода денежных средств","attachments": [{"sourceId": "f34030ef-358a-445c-8567-25985ce6d91c","comment": "описание вложения","dateTimeAt": "2018-03-22T08:14:38Z","file": {"name": "имя файла","size": "размер файла в байтах","base64": "вложение в формате base64"},"fileLink": "http://domain.com/archive.rar"}]},	[O]	[1], [2]
3.1.1	"subjectOf Federation" (поле данных)	код ОКТМО верхнего уровня	текстовое поле (textarea)		[O]	[1], [2]
3.1.2	"locality" (поле данных)	наименование населенного пункта	текстовое поле (textarea)		[O]	[1], [2]
3.2	"classification" (блок данных)	классификация инцидента			[O]	[1], [2]
3.2.1	"typeOfIncident" (поле данных)	тип инцидента	Выбирается один код из ограниченного множества возможных значений: - [MTR] - инцидент, связанный с нарушением требований к обеспечению защиты информации при осуществлении переводов денежных средств; - [BAC] - инцидент, связанный с нарушением требований к обеспечению защиты информации при осуществлении банковской деятельности; - [FMA] - инцидент, связанный с нарушением требований к обеспечению защиты информации при осуществлении деятельности в сфере финансовых рынков; - [DT_MTR] - инцидент, связанный с неоказанием или несвоевременным оказанием услуг по переводу денежных средств; - [DT_FS] - инцидент, связанный с неоказанием или несвоевременным оказанием финансовых услуг		[O]	[1], [2]
3.2.2.	"ext" (подблок данных)	реализация инцидента у клиента участника информационного обмена	В случае необходимости указания нескольких значений полей данных (events, method) указывается один или несколько объектов в подблоке данных "ext"		[O]	[1], [2]
			Выбирается один код из ограниченного множества возможных значений: - [MTR_WC] - получение оператором по переводу денежных средств, обслуживающим плательщика, включая оператора электронных денежных средств, уведомлений в предусмотренной договором форме от клиентов - физических, юридических лиц,			

3.2.2.1	"events" (поле данных)	события защиты информации	индивидуальных предпринимателей или лиц, занимающихся частной практикой, о случаях и (или) попытках переводов денежных средств без согласия клиента, в том числе об использовании электронных средств платежа; - [A_SC] - получение расчетным центром платежной системы уведомлений от участников платежной системы о списании денежных средств с их корреспондентских счетов без их согласия и (или) с использованием искаженной информации, содержащейся в распоряжениях платежных клиринговых центров или участников платежной системы; - [UO_WC] - выявление оператором по переводу денежных средств, обслуживающим плательщика, включая оператора электронных денежных средств, операций, соответствующих признакам осуществления перевода денежных средств без согласия клиента, установленным Банком России и размещаемым на официальном сайте Банка России в сети Интернет; - [FMA_WC] - получение уведомлений от клиентов - физических лиц, и (или) индивидуальных предпринимателей, и (или) физических лиц, занимающихся в установленном законодательством Российской Федерации порядке частной практикой, и (или) юридических лиц о проведении финансовой (банковской) операции без их согласия; - [OTH] - иные события, последствия или выявление которых могут привести к инцидентам, указанным в кодах [MTR], [BAC], [FMA], [DT_MTR], [DT_FS]		[O]	[1], [2]
			Выбирается один код из ограниченного множества возможных значений: - [SMS] - технология			

3.2.2.2	"method" (поле данных)	способ формирования и передачи распоряжений на осуществление транзакций, позволяющий совершить финансовую операцию	дистанционного обслуживания, при которой обмен информацией между клиентом и участником информационного обмена осуществляется с применением коротких текстовых сообщений с определенного в договоре банковского счета номера телефона; - [MBB] - технология дистанционного обслуживания, при которой обмен информацией между клиентом и участником информационного обмена осуществляется с применением программного обеспечения, разрабатываемого для использования в операционных системах мобильных устройств (например, iOS, Android); - [BRW] - технология дистанционного обслуживания, при которой обмен информацией между клиентом и участником информационного обмена осуществляется с применением интернет-браузера без установки дополнительного программного обеспечения; - [PCW] - технология дистанционного обслуживания, при которой обмен информацией между клиентом и участником информационного обмена осуществляется с персонального компьютера с применением дополнительного программного обеспечения, предоставляемого участником информационного обмена; - [ATM] - банкомат; - [CIN] - банкомат с возможностью приема наличных денежных средств; - [REC] - банкомат с функцией ресайклинга (recycling); - [POS] - POS-терминал; - [SST] - платежный терминал; - [CNP] - осуществление переводов с использованием платежных карт без		[O]	[1], [2]

			непосредственного использования платежных карт (CNP-транзакции); - [OTH] - иной способ формирования и передачи распоряжений на осуществление транзакций, позволяющий совершить финансовую операцию			
3.2.3	"int" (подблок данных)	реализация инцидента в информационной инфраструктуре участника информационного обмена	В случае необходимости указания нескольких значений полей данных (events, typeOfIntruder) указывается один или несколько объектов в подблоке данных "int"		[O]	[1], [2]

3.2.3.1	"events" (поле данных)	события защиты информации	Выбирается один код из ограниченного множества возможных значений: - [MTR_UA] - выявление оператором по переводу денежных средств, обслуживающим плательщика, включая оператора электронных денежных средств, операций по переводу денежных средств и получения наличных денежных средств, совершенных в результате несанкционированного доступа к объектам информационной инфраструктуры оператора по переводу денежных средств, в том числе при уменьшении остатка электронных денежных средств, за исключением виртуальных платежных карт; - [FMS_UA] - выполнение финансовых (банковских) операций в результате несанкционированного доступа к объектам информационной инфраструктуры некредитной финансовой организации; - [UPT_PSP] - осуществление несанкционированного снятия денежных средств оператора по переводу денежных средств в банкоматах; - [UPT_EMP] - осуществление несанкционированного снятия денежных средств оператора электронных денежных средств в банкоматах; - [DT_ALL] - неоказание услуг оператора по переводу денежных средств на период более двух часов в целом по всем субъектам Российской Федерации, в которых оператор по переводу денежных средств осуществляет перевод денежных средств с использованием платежных карт, их реквизитов и (или) систем (средств) дистанционного банковского обслуживания;		[O]	[1], [2]
			- [DT_SELECTED] - неоказание услуг оператора по переводу денежных средств на период более двух часов в целом по			

			отдельным субъектам Российской Федерации, в которых оператор по переводу денежных средств осуществляет перевод денежных средств с использованием платежных карт, их реквизитов и (или) систем (средств) дистанционного банковского обслуживания; - [DT_SC] - неоказание расчетным центром расчетных услуг на период более одного операционного дня; - [DTPT_SC] - невыполнение расчетным центром в течение операционного дня расчетов для принятых к исполнению распоряжений платежного клирингового центра или участников платежной системы; - [DT_CC] - прерывание клиринговым центром предоставления услуг платежного клиринга на период более одного операционного дня; - [DTPT_CC] - невыполнение клиринговым центром в течение операционного дня платежного клиринга для принятых к исполнению распоряжений участников платежной системы; - [DT_OC] - прерывание операционным центром предоставления операционных услуг на период более двух часов; - [DT_FS_ALL] - неоказание услуг некредитной финансовой организацией на период более двух часов в целом по всем субъектам Российской Федерации, в которых некредитная финансовая организация предоставляет финансовые (банковские) услуги; - [DT_FS_SEL] - неоказание услуг некредитной финансовой организацией на период более двух часов в целом по отдельным субъектам Российской Федерации, в которых некредитная финансовая организация предоставляет			

			финансовые (банковские) услуги;			
			- [PSP_CMTR] - выявление оператором по переводу денежных средств, включая оператора электронных денежных средств, и (или) оператором услуг платежной инфраструктуры атак, последствия от реализации которых, могут привести к случаям и попыткам осуществления переводов денежных средств без согласия клиента; - [CO_CFS] - выявление кредитной организацией компьютерных атак, последствия от реализации которых могут привести к случаям и попыткам осуществления финансовой (банковской) операции без согласия клиента; - [NCFI_CFS] - выявление некредитной финансовой организацией компьютерных атак, последствия от реализации которых могут привести к случаям и попыткам осуществления операции на финансовом рынке без согласия клиента; - [OTH] - иные события, последствия или выявление которых могут привести к инцидентам, указанным в кодах [MTR], [BAC], [FMA], [DT_MTR], [DT_FS]			

3.2.3.2	"typeOfIntruder" (поле данных)	тип нарушителя	Выбирается один код из ограниченного множества возможных значений: - [INT_ORG] - реализация несанкционированного доступа работников участника информационного обмена или иных лиц, обладающих полномочиями доступа к объектам информационной инфраструктуры участника информационного обмена (действия внутреннего нарушителя); - [EXT_ORG] - реализация компьютерных атак или несанкционированного доступа лиц, не обладающих полномочиями доступа к объектам информационной инфраструктуры участника информационного обмена (действия внешнего нарушителя)		[O]	[1], [2]
3.3	"damage" (блок данных)	выявление ущерба от несанкционированных операций			[O]	[2]
3.3.1	"operating" (поле данных)	оценка операционных расходов участника информационного обмена в момент представления сведений о реализации инцидента (вектор INT)	текстовое поле (textarea)		[N]	[2]
3.3.2	"relative" (поле данных)	относительная (качественная) оценка масштаба (тяжести последствий) от реализации инцидента (вектор INT)	Выбирается один код (в соответствии с разделом 14 настоящего документа) из ограниченного множества возможных значений: - [MOD] - умеренное влияние; - [ESS] - существенное влияние; - [CRIT] - критическое влияние		[O]	[2]
3.4	"schema Conclusion" (поле данных)	описание схемы вывода денежных средств	текстовое поле (textarea)		[O]	[2]
3.5	"attachments" (блок данных)	дополнительные данные для идентификации инцидента	В случае необходимости указания нескольких значений полей данных (sourceId, comment, dateTimeAt, file, fileLink) указывается один или несколько объектов в блоке данных "attachments"		[N]	[1], [

3.5.1	"sourceId" (поле данных)	идентификатор, присвоенный участником информационного обмена	128-битный идентификатор (GUID), сформированный в соответствии со спецификацией RFC 4122 [16], присвоенный участником информационного обмена		[N]	[1], [
3.5.2	"comment" (поле данных)	описание вложения	текстовое поле (textarea)		[N]	[1], [
3.5.3	"dateTimeAt" (поле данных)	дата и время добавления файла	формат представления данных в соответствии со спецификацией RFC 3339 [11]		[N]	[1], [
3.5.4	"file" (блок данных)	файл данных	Указывается наименование, размер файла (не более 5 Мб), выполняется кодировка в формате Base64		[N]	[1], [
3.5.5	"fileLink" (поле данных)	ссылка для получения (скачивания) файла данных	Указывается URL-адрес для скачивания файла, в случае если его размер превышает 5 Мб, в соответствии со спецификацией RFC 3986 [15]		[N]	[1], [

<1> Обязательность информирования устанавливается только для некредитных финансовых организаций.

6.5. Блок данных "антифрод" [ANTIFRAUD]

Блок данных "антифрод" используется участниками информационного обмена в случаях:

информирования Банка России операторами по переводу денежных средств, операторами платежных систем, операторами услуг платежной инфраструктуры обо всех случаях и попытках осуществления переводов денежных средств без согласия клиента [4];

информирования Банка России операторами по переводу денежных средств о приостановлении зачисления денежных средств на банковский счет получателя средств или увеличения остатка электронных денежных средств получателя средств [20].

Номер блока (поля) данных	Идентификатор блока (поля) данных	Содержание блока (поля) данных	Формат поля данных	Формат элем
4.1	"antifraud" (блок данных)		В случае необходимости указания нескольких значений блоков данных (payerIdentifier, payer, payee, additionalStatus) указывается один или несколько объектов в блоке данных "antifraud"	
4.1.1	"sourceId" (поле данных)	идентификатор, присвоенный участником информационного обмена, являющимся плательщиком	128-битный идентификатор (GUID), сформированный в соответствии со спецификацией RFC 4122 [16], присвоенный участником информационного обмена	
4.1.2	"victim" (поле данных)	информация о субъектном статусе плательщика	Выбирается один код из ограниченного множества возможных значений: - [person] - физическое лицо; - [entity] - юридическое лицо	
4.2	"payerIdentifier" (блок данных)	идентификационные данные, определяющие конкретного плательщика		"antifraud": [{"sourceId": "f34030ef-358a-4 субъектном статусе плательщика","paye "E25059612A71BAB224C7CB534FD7A0D3C "C49337884A71BAB224C7CB438FD7A0D3C {"bik": "123456789","inn": "123456789000 являющейся плательщиком","payerTrans перевода денежных средств","paymentC "сумма операции по осуществлению пер платежных карт","currency": "валюта опе средств","dateTimeAt": "2018-01-13T09:14 по переводу денежных средств при выпо

4.2.1	"hash" (поле данных)	результат вычисления функции хэширования номера документа, удостоверяющего личность в целях идентификации лица - плательщика, направившего уведомление о случаях и (или) попытках переводов денежных средств без согласия клиента, в том числе об использовании электронных средств платежа	Последовательность символов, полученных в результате вычисления хэш-функции SHA-256 от серии и номера документа, удостоверяющего личность. Серия и номер документа, удостоверяющего личность, представляется для вычисления хэш-функции: без пробелов (_), знака номера (N), букв (при их наличии) в верхнем регистре (ABC). Для российского паспорта это XXXXYYYYYY, где: XXXX - четырехзначная серия паспорта; YYYYYY - шестизначный номер паспорта. Кодировка исходного текста (до хэширования) - Windows-1251; Кодировка текста хэша - Windows-1251.	"12345123451234512345","sum": "сумма с средств","currency": "валюта операции по "2018-01-13T09:14:38Z",},"phoneNumber" операции","currency": "валюта операции" 13T09:14:38Z"},"idNumber": {"number": "1 "сумма операции","currency": "валюта опе
4.2.2	"hashSnils" (поле данных)	результат вычисления функции хэширования страхового номера индивидуального лицевого счета застрахованного лица в системе персонифицированного учета Пенсионного фонда Российской Федерации (далее - СНИЛС) плательщика, направившего уведомление о случаях и (или) попытках переводов денежных средств без согласия клиента, в том числе об использовании электронных средств платежа при его наличии	Последовательность символов, полученных в результате вычисления хэш-функции SHA-256 от СНИЛС плательщика. СНИЛС представляется для вычисления хэш-функции: без пробелов (_) и знаков разделения (-). СНИЛС вида: XXXXXXXXXXX Кодировка исходного текста (до хэширования) - Windows-1251; Кодировка текста хэша - Windows-1251.	"dateTimeAt": "2018-01-13T09:14:38Z"}}," идентификатор мобильного абонента (ин "международный идентификатор мобиль identification code (32 поле ISO 8583)","cat ISO 8583)","caic": "Card acceptor identificat "123456789","inn": "123456789000","paye являющейся получателем средств","paye реализации перевода денежных средств "123412341234123412"},"settlement": {"n "12345123451234512345"},"phoneNumber
4.3	"payer" (блок данных)	информация, определяющая плательщика		
4.3.1	"bik" (поле данных)	БИК оператора по переводу денежных средств, включая оператора электронных денежных средств, обслуживающего плательщика	в формате AAAAAAAAA	
4.3.2	"inn" (поле данных)	ИНН плательщика - юридического лица, и (или) индивидуального предпринимателя, и (или) лица, занимающегося частной практикой	в формате XXXXXXXXXX - для юридических лиц, в формате XXXXXXXXXX или XXXXXXXXXXX - для индивидуальных предпринимателей и (или) физических лиц, занимающихся в установленном законодательством Российской Федерации порядке частной практикой	
4.3.3	"payerName" (поле данных)	наименование организации, являющейся плательщиком	текстовое поле (textarea)	

4.3.4	"payerTransferId" (подблок данных)	идентификационные данные в зависимости от способа реализации перевода денежных средств		
4.3.4.1	"transferType" (поле данных)	тип способа реализации перевода денежных средств	Выбирается один код из ограниченного множества возможных значений: - [paymentCard] - при осуществлении операций по переводу денежных средств с использованием платежных карт; - [settelment] - при осуществлении переводов денежных средств по банковским счетам; - [phoneNumber] - при осуществлении переводов денежных средств по абонентскому номеру телефона; - [idNumber] - при изменении остатка электронных денежных средств	"number": "1KoX6AA5VTdbBTkw27YEqKFaT "идентификатор трансграничности","add дополнительного подтверждения операц
4.3.4.2	"paymentCard" (подблок данных)	при осуществлении операций по переводу денежных средств с использованием платежных карт		
4.3.4.2.1	"number" (поле данных)	номер платежной карты плательщика, выданной ему и (или) лицу, уполномоченному плательщиком, оператором по переводу денежных средств - эмитентом	в формате XXXXXXXXXXXXXXXXXX номер платежной карты представляется без пробелов (_) и знаков разделения (-).	
4.3.4.2.2	"sum" (поле данных)	сумма операции по осуществлению перевода денежных средств с использованием платежных карт	сумма операции - поле "F004" стандарта финансовых сообщений ISO 8583 [7], [8], [9]	
4.3.4.2.3	"currency" (поле данных)	валюта операции по осуществлению перевода денежных средств	валюта операции - поле "F049" стандарта финансовых сообщений ISO 8583 [7], [8], [9]	
4.3.4.2.4	"dateTimeAt" (поле данных)	дата и время операции	формат представления данных в соответствии со спецификацией RFC 3339 [11]	
4.3.4.2.5	"rrn" (поле данных)	номер, генерируемый для операции по переводу денежных средств при выполнении ее авторизации	номер, генерируемый для операции по переводу денежных средств при выполнении ее авторизации - поле "F037" стандарта финансовых сообщений ISO 8583 [7], [8], [9] Значение поля "F037" (Retrieval Reference Number) должно формироваться хостом банка-эквайрера по следующему правилу: YJJJXXNNNNNN, где: Y - последняя цифра года; JJJ - юлианская дата; XX - идентификатор, присвоенный хосту банка-эквайрера оператором; NNNNNN - последовательный номер транзакции в течение дня	

4.3.4.3	"settlement" (подблок данных)	при осуществлении переводов денежных средств по банковским счетам посредством списания денежных средств с банковских счетов плательщиков		
4.3.4.3.1	"number" (поле данных)	номер банковского счета плательщика, открытого у оператора по переводу денежных средств, обслуживающего плательщика	в формате XXXXXXXXXXXXXXXXXXXX номер банковского счета представляется без пробелов (_) и знаков разделения (-).	
4.3.4.3.2	"sum" (поле данных)	сумма операции по переводу денежных средств	текстовое поле (textarea)	
4.3.4.3.3	"currency" (поле данных)	валюта операции по переводу денежных средств	текстовое поле (textarea)	
4.3.4.3.4	"dateTimeAt" (поле данных)	дата и время операции	формат представления данных в соответствии со спецификацией RFC 3339 [11]	
4.3.4.4	"phoneNumber" (подблок данных)	при осуществлении переводов денежных средств по абонентскому номеру телефона		
4.3.4.4.1	"number" (поле данных)	номер телефона плательщика, указанный в договоре банковского счета и (или) договоре об использовании электронного средства платежа, заключенном с плательщиком	в формате KKKXXXNNNNNNN, где: KKK - от одного до трех символов кода страны; XXX - код оператора; NNNNNNN - 7 знаков номера. Номер телефона представляется без знака плюс (+), пробелов (_) и знаков разделения (-).	
4.3.4.4.2	"sum" (поле данных)	сумма операции	текстовое поле (textarea)	
4.3.4.4.3	"currency" (поле данных)	валюта операции	текстовое поле (textarea)	
4.3.4.4.4	"dateTimeAt" (поле данных)	дата и время операции	формат представления данных в соответствии со спецификацией RFC 3339 [11]	
4.3.4.5	"idNumber" (подблок данных)	при изменении остатка электронных денежных средств		
4.3.4.5.1	"number" (поле данных)	идентификационный номер плательщика, в частности номер электронного кошелька плательщика, используемого им на основании договора банковского счета и (или) договора об использовании электронного средства платежа, заключенного с оператором по переводу денежных средств	текстовое поле (textarea)	
4.3.4.5.2	"sum" (поле данных)	сумма операции	текстовое поле (textarea)	
4.3.4.5.3	"currency" (поле данных)	валюта операции	текстовое поле (textarea)	
4.3.4.5.4	"dateTimeAt" (поле данных)	дата и время операции	формат представления данных в соответствии со спецификацией RFC 3339 [11]	

4.3.5	"device" (подблок данных)	параметры устройства, с использованием которого осуществлен доступ к автоматизированной системе, программному обеспечению с целью осуществления перевода денежных средств без согласия клиента	
4.3.5.1	"ip" (поле данных)	сетевой адрес компьютера и (или) коммуникационного устройства (маршрутизатора) (IP)	Сетевой адрес IPv4 должен соответствовать спецификации RFC 791 [12]
4.3.5.2	"imsi" (поле данных)	International Mobile Subscriber Identity (IMSI) - международный идентификатор мобильного абонента (индивидуальный номер абонента (клиента - физического лица), по которому система распознает пользователя мобильной связи, использующего стандарты GSM и UMTS	число (15-разрядное в десятичном представлении) AA-BBBBBB-CCCCCC-EE
4.3.5.3	"imei" (поле данных)	International Mobile Equipment Identity (IMEI) - международный идентификатор мобильного оборудования (мобильного устройства клиента - физического лица)	число (15-разрядное в десятичном представлении) AA-BBBBBB-CCCCCC-EE
4.3.5.4	"aiic" (поле данных)	идентификатор участника, являющегося банком-эквайрером при осуществлении операций по переводу денежных средств с использованием платежных карт	идентификатор участника, являющегося банком-эквайрером при осуществлении операций по переводу денежных средств с использованием платежных карт (Acquiring institution identification code) - поле "F032" стандарта финансовых сообщений ISO 8583 [7], [8], [9]
4.3.5.5	"cati" (поле данных)	идентификатор банкомата и (или) электронного терминала, на котором осуществляется операция по переводу и (или) снятию денежных средств	идентификатор банкомата и (или) электронного терминала, на котором осуществляется операция по переводу и (или) снятию денежных средств (Card acceptor terminal identification), - поле "F041" стандарта финансовых сообщений ISO 8583 [7], [8], [9] Значение идентификатора терминала должно быть выровнено влево и дополнено пробелами справа до 8 символов

4.3.5.6	"caic" (поле данных)	идентификатор банкомата и (или) электронного терминала, на котором осуществляется операция по переводу и (или) снятию денежных средств, по его географическому местоположению	идентификатор банкомата и (или) электронного терминала, на котором осуществляется операция по переводу и (или) снятию денежных средств, по его географическому местоположению (Card acceptor identification code) - поле "F042" стандарта финансовых сообщений ISO 8583 [7], [8], [9] Значение идентификатора пункта обслуживания должно быть выровнено влево и дополнено пробелами справа до 15 символов
4.4	"payee" (блок данных)	информация, определяющая получателя средств	
4.4.1	"bik" (поле данных)	БИК оператора по переводу денежных средств, обслуживающего получателя средств	в формате AAAAAAAAA
4.4.2	"inn" (поле данных)	ИНН получателя средств - юридического лица, и (или) индивидуального предпринимателя, и (или) лица, занимающегося частной практикой	в формате XXXXXXXXXX - для юридических лиц, в формате XXXXXXXXXX или XXXXXXXXXXXX - для индивидуальных предпринимателей и (или) физических лиц, занимающихся в установленном законодательством Российской Федерации порядке частной практикой
4.4.3	"payeeName" (поле данных)	наименование организации, являющейся получателем средств	текстовое поле (textarea)
4.4.4	"payeeTransferId" (подблок данных)	идентификационные данные в зависимости от способа реализации перевода денежных средств	
4.4.4.1	"transferType" (поле данных)	тип способа реализации перевода денежных средств	Выбирается один код из ограниченного множества возможных значений: - [paymentCard] - при осуществлении операций по переводу денежных средств с использованием платежных карт; - [settelment] - при осуществлении переводов денежных средств по банковским счетам; - [phoneNumber] - при осуществлении переводов денежных средств по абонентскому номеру телефона; - [idNumber] - при изменении остатка электронных денежных средств
4.4.4.2	"paymentCard" (подблок данных)	при осуществлении операций по переводу денежных средств с использованием платежных карт	

4.4.4.2.1	"number" (поле данных)	номер платежной карты получателя средств, выданной ему и (или) лицу, уполномоченному получателем средств, оператором по переводу денежных средств - эмитентом	в формате XXXXXXXXXXXXXXXXXX номер платежной карты представляется без пробелов (_) и знаков разделения (-).	
4.4.4.3	"settlement" (подблок данных)	при осуществлении переводов денежных средств по банковским счетам посредством списания денежных средств с банковских счетов плательщиков		
4.4.4.3.1	"number" (поле данных)	номер расчетного счета получателя средств, открытого у оператора по переводу денежных средств, обслуживающего получателя средств	в формате XXXXXXXXXXXXXXXXXXXX номер банковского счета представляется без пробелов (_) и знаков разделения (-).	
4.4.4.4	"phoneNumber" (подблок данных)	при осуществлении переводов денежных средств по абонентскому номеру телефона		
4.4.4.4.1	"number" (поле данных)	номер телефона получателя средств	в формате KKKXXXNNNNNNNN, где: KKK - от одного до трех символов кода страны; XXX - код оператора; NNNNNNN - 7 знаков номера. Номер телефона представляется без знака плюс (+), пробелов (_) и знаков разделения (-).	
4.4.4.5	"idNumber" (подблок данных)	при изменении остатка электронных денежных средств		
4.4.4.5.1	"number" (поле данных)	идентификационный номер получателя средств, в частности номер электронного кошелька получателя средств, используемого им на основании договора банковского счета и (или) договора об использовании электронного средства платежа, заключенного с оператором по переводу денежных средств	текстовое поле (textarea)	
4.5	"additionalStatus" (блок данных)	дополнительные статусы реализации несанкционированной операции		
4.5.1	"crossBorder" (поле данных)	идентификатор трансграничности	Выбирается один код из ограниченного множества возможных значений: - [CRB] - трансграничный перевод; - [DOM] - перевод внутри страны	

4.5.2	"additionalTransactionApprove" (поле данных)	идентификатор дополнительного подтверждения операции	Выбирается один или несколько кодов из ограниченного множества возможных значений: - [3DS] - операция подтверждена с использованием 3D Secure; - [DCS] - реализация технологических мер по использованию раздельных технологий [3]; - [NAA] - операция без подтверждения; - [SMS] - подтверждение операции выполнено с применением коротких текстовых сообщений (СМС-сообщений); - [LTR] - операция выполнена в соответствии со списком доверенных получателей средств; - [TEL] - операция подтверждена по телефону; - [OAA] - иной способ подтверждения	

6.6. Информация о технических данных, описывающих компьютерные атаки, направленные на объекты информационной инфраструктуры участников информационного обмена и их клиентов, а также соответствующие формы электронных сообщений. Блок данных [IMPACTS]

6.6.1. Компьютерные атаки, связанные с изменением маршрутно-адресной информации [trafficHijackAttacks] (для вектора [INT], [EXT])

Номер блока (поля) данных	Идентификатор блока (поля) данных	Содержание блока (поля) данных	Формат поля данных	Формат электронного сообщения	Обязательность информирования	Этапы информирования
1.1	"sourceId" (поле данных)	идентификатор, присвоенный участником информационного обмена	128-битный идентификатор (GUID), сформированный в соответствии со спецификацией RFC 4122 [16], присвоенный участником информационного обмена	"impacts": {"trafficHijackAttacks": [{"sourceId": "f34030ef-358a-445c-8567-25985ce6d91c","legalAsPath": "штатный AS-Path","wrongAsPath": "подставной AS-Path","lookingGlass": "ссылка на используемый Looking Glass для проверки AS-Path","legalPrefix": "штатный prefix","wrongPrefix": "подставной prefix"}],	[N]	[2], [3]
1.2	"legalAsPath" (поле данных)	штатный AS-Path	текстовое поле (textarea)		[N]	[2], [3]
1.3	"wrongAsPath" (поле данных)	подставной AS-Path	текстовое поле (textarea)		[N]	[2], [3]
1.4	"lookingGlass" (поле данных)	ссылка на используемый Looking Glass для проверки AS-Path	текстовое поле (textarea)		[N]	[2], [3]
1.5	"legalPrefix" (поле данных)	штатный prefix	текстовое поле (textarea)		[N]	[2], [3]
1.6	"wrongPrefix" (поле данных)	подставной prefix	текстовое поле (textarea)		[N]	[2], [3]

6.6.2. Компьютерные атаки, связанные с использованием вредоносного программного обеспечения применительно к объектам информационной инфраструктуры участников информационного обмена и их клиентов [malware] (для вектора [INT], [EXT])

Номер блока (поля) данных	Идентификатор блока (поля) данных	Содержание блока (поля) данных	Формат поля данных	Формат электр

2	"sourceId" (поле данных)	идентификатор, присвоенный участником информационного обмена	128-битный идентификатор (GUID), сформированный в соответствии со спецификацией RFC 4122 [16], присвоенный участником информационного обмена	
2.1	"target" (блок данных)	идентификатор объекта атаки		
2.1.1	"ip" (поле данных)	IP-адрес	Логический адрес IPv4 должен соответствовать спецификации RFC 791 [12]	
2.2	"sources" (блок данных)	идентификаторы источников вредоносных ресурсов в сети Интернет, с которыми взаимодействует атакуемый объект	В случае необходимости указания нескольких значений полей данных (ip, domain, url) указывается один или несколько объектов в блоке данных "sources"	"malware": [{"sourceId": "f34030ef-358a-445c-8 "127.0.0.1"},"sources": [{"ip": "127.0.0.1","dom "http://example.com"}],"classifications": [{"ven BBK","vendorVerdict": "классификация ВК"}]," "4BA5139A444538479D9D750E2E2779BF","sha "D2B063763378A8CB38B192B2F71E78BC1378 "E25059612A71BAB224C7CB438FD7A0D3C1C7 {"sourceId": "f34030ef-358a-445c-8567-25985c вложения","dateTimeAt": "2018-03-22T08:14:3 файла в байтах","base64": "вложение в форм "http://domain.com/archive.rar"}}],"malwareMe "qwerty@example.ru","server": "127.0.0.1"}],"r "f34030ef-358a-445c-8567-25985ce6d91c","cor "2018-03-22T08:14:38Z","file": {"name": "имя с "вложение в формате base64"},"fileLink": "http://domain.com/archive.rar"},"harmfulResou "example.com","url": "http://example.com"}],"ic компрометирующего идентификатора",
2.2.1	"ip" (поле данных)	IP-адрес	Логический адрес IPv4 должен соответствовать спецификации RFC 791 [12]	
2.2.2	"domain" (поле данных)	доменное имя	Доменное имя согласно спецификации RFC 1034 [14], а также международной иерархии доменных зон в соответствии со спецификацией RFC 5890 [13]	
2.2.3	"url" (поле данных)	URL-адрес	URL в соответствии со спецификацией RFC 3986 [15]	
2.3	"classifications" (блок данных)	классификация ВК	В случае необходимости указания нескольких значений полей данных (vendorName, vendorVerdict) указывается один или несколько объектов в блоке данных "classifications"	
2.3.1	"vendorName" (поле данных)	наименование используемого участником информационного обмена средства от ВВК	текстовое поле (textarea)	
2.3.2	"vendorVerdict" (поле данных)	класс ВК в соответствии со средством от ВВК участника информационного обмена	текстовое поле (textarea)	
2.4	"malwareSamples" (блок данных)	указываются образцы ВК, которые могут характеризоваться хэш-функцией или прикрепленным вложением	В случае необходимости указания нескольких значений подблоков данных (hash, attachment) указывается один или несколько объектов в блоке данных "malwareSamples"	"comment": "дополнительное описание"}],"fil компрометирующего идентификатора","com [{"impact": "тип выявленного компрометирук "дополнительное описание"}],"prc": [{"impac идентификатора","comment": "дополнительн выявленного компрометирующего идентифи
2.4.1	"hash" (подблок данных)	образец ВК в виде хэш-функций (для каждого образца ВК вычисляется хэш-функция MD5, SHA-1, SHA-256)		
2.4.1.1	"md5" (поле данных)	образец ВК в виде хэш-функции MD5	последовательность символов, полученных в результате вычисления хэш-функции MD5	
2.4.1.2	"sha1" (поле данных)	образец ВК в виде хэш-функции SHA-1	последовательность символов, полученных в результате вычисления хэш-функции SHA-1	

2.4.1.3	"sha256" (поле данных)	образец ВК в виде хэш-функции SHA-256	последовательность символов, полученных в результате вычисления хэш-функции SHA-256	описание"}]}],"infectionMethods": [{"type": "т заражения","comment": "дополнительное оп
2.4.2	"attachment" (подблок данных)	образец ВК в виде файла		
2.4.2.1	"sourceId" (поле данных)	идентификатор, присвоенный участником информационного обмена	128-битный идентификатор (GUID), сформированный в соответствии со спецификацией RFC 4122 [16], присвоенный участником информационного обмена	
2.4.2.2	"comment" (поле данных)	описание вложения	текстовое поле (textarea)	
2.4.2.3	"dateTimeAt" (поле данных)	дата и время добавления файла	формат представления данных в соответствии со спецификацией RFC 3339 [11]	
2.4.2.4.1	"file" (подблок данных)	дополнительные материалы, содержащие образцы ВК	Указывается наименование, размер файла (не более 5 Мб), выполняется кодировка в формате Base64	
2.4.2.5	"fileLink" (поле данных)	дополнительные материалы, содержащие образцы ВК	Указывается URL-адрес для скачивания файла, в случае если его размер превышает 5 Мб, в соответствии со спецификацией RFC 3986 [15]	
2.5	"malwareMessage Senders" (блок данных)	идентификаторы электронных почтовых ящиков, с которых поступило письмо с вложенным ВК	В случае необходимости указания нескольких значений полей данных (email, server) указывается один или несколько объектов в блоке данных "malwareMessage"	
2.5.1	"email" (поле данных)	адрес электронного почтового ящика отправителя	Адрес электронного почтового ящика отправителя представляется в формате в соответствии со спецификацией RFC 5322 [18]	
2.5.2	"server" (поле данных)	IP-адрес последнего почтового сервера	Логический адрес IPv4 должен соответствовать спецификации RFC 791 [12]	
2.6	"malwareMessageAttachment" (подблок данных)	файл с исходным кодом электронного письма (в случае, если ВК был прислан на электронный почтовый ящик)		
2.6.1	"sourceId" (поле данных)	идентификатор, присвоенный участником информационного обмена	128-битный идентификатор (GUID), сформированный в соответствии со спецификацией RFC 4122 [16], присвоенный участником информационного обмена	
2.6.2	"comment" (поле данных)	описание вложения	текстовое поле (textarea)	
2.6.3	"dateTimeAt" (поле данных)	дата и время добавления файла	формат представления данных в соответствии со спецификацией RFC 3339 [11]	
2.6.4.1	"file" (блок данных)	файл данных, содержащий образец ВК	Указывается наименование, размер файла (не более 5 Мб), выполняется кодировка в формате Base64	

2.6.4	"fileLink" (поле данных)	ссылка для получения (скачивания) файла данных, содержащего образцы ВК	Указывается URL-адрес для скачивания файла, в случае если его размер превышает 5 Мб, в соответствии со спецификацией RFC 3986 [15]
2.7	"harmfulResourceAddress" (блок данных)	идентификаторы вредоносных ресурсов, с которых был загружен ВК	В случае необходимости указания нескольких значений полей данных (ip, domain, url) указывается один или несколько объектов в блоке данных "harmfulResourceAddress"
2.7.1	"ip" (поле данных)	IP-адрес	Логический адрес IPv4 должен соответствовать спецификации RFC 791 [12]
2.7.2	"domain" (поле данных)	доменное имя	Доменное имя согласно спецификации RFC 1034 [14], а также международной иерархии доменных зон в соответствии со спецификацией RFC 5890 [13]
2.7.3	"url" (поле данных)	URL-адрес	URL в соответствии со спецификацией RFC 3986 [15].
2.8	"iocs" (блок данных)	выявленные индикаторы компрометации	В случае необходимости указания нескольких значений полей данных (net, fil, reg, prc, oth) указывается один или несколько объектов в блоке данных "iocs"
2.8.1	"net" (подблок данных)	сетевые индикаторы	В случае необходимости указания нескольких значений полей данных (impact, comment) указывается один или несколько объектов в блоке данных "net"
2.8.1.1	"impact" (поле данных)	тип выявленного компрометирующего идентификатора	Выбирается один код из ограниченного множества возможных значений: - [CRT] - создание технических данных; - [UPD] - изменение технических данных; - [DLT] - удаление технических данных
2.8.1.2	"comment" (поле данных)	дополнительное описание	текстовое поле (textarea)
2.8.2	"fil" (подблок данных)	файловые индикаторы	В случае необходимости указания нескольких значений полей данных (impact, comment) указывается один или несколько объектов в блоке данных "fil"
2.8.2.1	"impact" (поле данных)	тип выявленного компрометирующего идентификатора	Выбирается один код из ограниченного множества возможных значений: - [CRT] - создание технических данных; - [UPD] - изменение технических данных; - [DLT] - удаление технических данных
2.8.2.2	"comment" (поле данных)	дополнительное описание	текстовое поле (textarea)
2.8.3	"reg" (подблок данных)	индикаторы реестра ОС	В случае необходимости указания нескольких значений полей данных (impact, comment) указывается один или несколько объектов в блоке данных "reg"

2.8.3.1	"impact" (поле данных)	тип выявленного компрометирующего идентификатора	Выбирается один код из ограниченного множества возможных значений: - [CRT] - создание технических данных; - [UPD] - изменение технических данных; - [DLT] - удаление технических данных	
2.8.3.2	"comment" (поле данных)	дополнительное описание	текстовое поле (textarea)	
2.8.4	"prc" (подблок данных)	индикаторы процессов ОС	В случае необходимости указания нескольких значений полей данных (impact, comment) указывается один или несколько объектов в блоке данных "prc"	
2.8.4.1	"impact" (поле данных)	тип выявленного компрометирующего идентификатора	Выбирается один код из ограниченного множества возможных значений: - [CRT] - создание технических данных; - [UPD] - изменение технических данных; - [DLT] - удаление технических данных	
2.8.4.2	"comment" (поле данных)	дополнительное описание	текстовое поле (textarea)	
2.8.5	"oth" (подблок данных)	индикаторы, не учтенные в (2.8.1 - 2.8.4.2)	В случае необходимости указания нескольких значений полей данных (impact, comment) указывается один или несколько объектов в блоке данных "oth"	
2.8.5.1	"impact" (поле данных)	тип выявленного компрометирующего идентификатора	Выбирается один код из ограниченного множества возможных значений: - [CRT] - создание технических данных; - [UPD] - изменение технических данных; - [DLT] - удаление технических данных	
2.8.5.2	"comment" (поле данных)	дополнительное описание	текстовое поле (textarea)	
2.9	"infectionMethods" (блок данных)	идентификаторы предполагаемых способов "заражения"	В случае необходимости указания нескольких значений полей данных (type, comment) указывается один или несколько объектов в блоке данных "infectionMethods"	
2.9.1	"type" (поле данных)	тип предполагаемого способа заражения	Выбирается один код из ограниченного множества возможных значений: - [EML] - по каналам электронной почты; - [DSD] - с носителя информации; - [LCL] - распространение по локальной сети; - [OTH] - иной способ	
2.9.2	"comment" (поле данных)	примечание к выбранному типу	текстовое поле (textarea)	

6.6.3. Компьютерные атаки, возникшие в результате побуждения клиентов к осуществлению операций по переводу денежных средств путем обмана или злоупотребления доверием [socialEngineering] (для вектора [EXT])

Номер блока (поля) данных	Идентификатор блока (поля) данных	Содержание блока (поля) данных	Формат поля данных	Формат электронного сообщения	Обязательность информирования	инфо

3	"sourceId" (поле данных)	идентификатор, присвоенный участником информационного обмена	128-битный идентификатор (GUID), сформированный в соответствии со спецификацией RFC 4122 [16], присвоенный участником информационного обмена	"socialEngineering": {"sourceId": "f34030ef-358a-445c-8567-25985ce6d91c","soiTypes": ["идентификаторы методов социальной инженерии"],"soiSenders": [{"phoneNumber": "1212312345678","email": "qwerty@example.ru","server": "127.0.0.1"}],"messageAttachment": {"sourceId": "f34030ef-358a-445c-8567-25985ce6d91c","comment": "примечание к вложению","dateTimeAt": "2018-03-22T08:14:38Z","file": {"name": "имя файла","size": "размер файла в байтах","base64": "вложение в форматебase64"},"fileLink": "http://domain.com/archive.rar"},"description": "дополнительное описание"},	[N]	
3.1	"soiTypes" (поле данных)	идентификаторы методов социальной инженерии	Выбирается один или несколько кодов из ограниченного множества возможных значений: - [MOB] - звонок с мобильного телефонного номера; - [TPH] - звонок с телефонного номера 8-800; - [SMS] - СМС-сообщение; - [SNW] - социальная инженерия с использованием социальных сетей; - [MSG] - социальная инженерия с использованием средств мгновенных сообщений; - [OTH] - иной способ реализации методов социальной инженерии		[N]	
3.2	"soiSenders" (блок данных)	идентификаторы реализации методов социальной инженерии	В случае необходимости указания нескольких значений полей данных (phoneNumber, email, server) указывается один или несколько объектов в блоке данных "soiSenders"		[N]	
3.2.1	"phoneNumber" (поле данных)	телефонный номер	в формате KKKXXXNNNNNNN, где: KKK - от одного до трех символов кода страны; XXX - код оператора; NNNNNNN - 7 знаков номера.		[N]	
			Номер телефона представляется без знака плюс (+), пробелов (_) и знаков разделения (-).			
3.2.2	"email" (поле данных)	электронный почтовый адрес	Адрес электронного почтового ящика отправителя представляется в формате в соответствии со спецификацией RFC 5322 [18]		[N]	

3.2.3	"server" (поле данных)	IP-адрес последнего почтового сервера	Логический адрес IPv4 должен соответствовать спецификации RFC 791 [12]		[N]	
3.3	"message Attachment" (блок данных)	файлы данных, описывающие метод социальной инженерии			[N]	
3.3.1	"sourceId" (поле данных)	идентификатор, присвоенный участником информационного обмена	128-битный идентификатор (GUID), сформированный в соответствии со спецификацией RFC 4122 [16], присвоенный участником информационного обмена		[N]	
3.3.2	"comment" (поле данных)	описание вложения	текстовое поле (textarea)		[N]	
3.3.3	"dateTimeAt" (поле данных)	дата и время добавления файла	формат представления данных в соответствии со спецификацией RFC 3339 [11]		[N]	
3.3.4.1	"file" (подблок данных)	файлы данных, описывающие метод социальной инженерии	Указывается наименование, размер файла (не более 5 Мб), выполняется кодировка в формате Base64		[N]	
3.3.5	"fileLink" (поле данных)	файлы данных, описывающие метод социальной инженерии	Указывается URL-адрес для скачивания файла, в случае если его размер превышает 5 Мб, в соответствии со спецификацией RFC 3986 [15]		[N]	
3.4	"description" (поле данных)	дополнительное описание	текстовое поле (textarea)		[N]	

6.6.4. Компьютерные атаки типа "отказ в обслуживании" (DDoS-атаки) применительно к информационной инфраструктуре участников информационного обмена [ddosAttacks] (для вектора [INT])

Номер блока (поля) данных	Идентификатор блока (поля) данных	Содержание блока (поля) данных	Формат поля данных	Формат электронного сообщения	Обязательность информирования	Этапы информировани
4	"sourceId" (поле данных)	идентификатор, присвоенный участником информационного обмена	128-битный идентификатор (GUID), сформированный в соответствии со спецификацией RFC 4122 [16], присвоенный участником информационного обмена		[N]	[2], [3]
4.1	"target" (блок данных)	идентификаторы объекта атаки			[N]	[2], [3]
4.1.1	"ip" (поле данных)	IP-адрес	Логический адрес IPv4 должен соответствовать спецификации RFC 791 [12]		[N]	[2], [3]

4.1.2	"domain" (поле данных)	доменное имя	Доменное имя согласно спецификации RFC 1034 [14], а также международной иерархии доменных зон в соответствии со спецификацией RFC 5890 [13]	"ddosAttacks": [{"sourceId": "f34030ef-358a-445c-8567-25985ce6d91c","target": {"ip": "127.0.0.1","domain": "example.com","url": "http://example.com","assignment": "назначение атакуемого объекта","serviceType": "тип информационного сервиса","network": "адрес сети"},"attackType": {"type": "тип атаки (по уровням OSI)","comment": "дополнительное описание"},"sources": [{"ip": "127.0.0.1"}],"power": {"pps": "количество пакетов в секунду","mps": "количество мегабит в секунду","rps": "количество запросов в секунду"},"startTimeAt": "2018-03-22T08:14:38Z","endTimeAt": "2018-03-22T09:15:44Z","negativeImpact": {"type": "тип негативного влияния","comment": "примечание к выбранному типу"}}],	[N]	[2], [3]
4.1.3	"url" (поле данных)	URL-адрес	URL в соответствии со спецификацией RFC 3986 [15]		[N]	[2], [3]
4.1.4	"assignment" (поле данных)	назначение атакуемого объекта	назначение объекта атаки в информационной инфраструктуре участника информационного обмена (сервер, система хранения данных, телеком, персональный компьютер, межсетевой экран и т.д.)		[N]	[2], [3]
4.1.5	"serviceType" (поле данных)	тип информационного сервиса	текстовое поле (textarea)		[N]	[2], [3]
4.1.6	"network" (поле данных)	адрес сети	Логический адрес IPv4 в соответствии со спецификацией RFC 791 [12] с указанием маски сети (Subnet Mask) согласно спецификации RFC 997 [17]		[N]	[2], [3]
4.2	"attackType" (блок данных)	тип атаки			[N]	[2], [3]

4.2.1	"type" (поле данных)	тип атаки (по уровням OSI)	Выбирается один код из ограниченного множества возможных значений: [1] - "L2/3: ICMP-flood",[2] - "L2/3: NTP-amplification",[3] - "L2/3: TFTP-amplification",[4] - "L2/3: SENTINEL-amplification",[5] - "L2/3: DNS-amplification",[6] - "L2/3: SNMP-amplification",[7] - "L2/3: SSDP-amplification",[8] - "L2/3: CHARGEN-amplification",[9] - "L2/3: RIPv1-amplification",[10] - "L2/3: BitTorrent-amplification",[11] - "L2/3: QTPD-amplification",[12] - "L2/3: Quake-amplification",[13] - "L2/3: LDAP-amplification",[14] - "L2/3: 49ad34-amplification",[15] - "L2/3: Portmap-amplification",[16] - "L2/3: Kad-amplification",[17] - "L2/3: NetBIOS-amplification",[18] - "L2/3: Steam-amplification",[19] - "L3: DPI-attack",[20] - "L4: LAND-attack",[21] - "L4: TCP-SYN-attack",[22] - "L4: TCP-ACK-attack",[23] - "L4: Smurf-attack",[24] - "L4: ICMP/UDP-frag",[25] - "L4: TCP-frag",[26] - "L6: SSL-attack",[27] - "L7: DNS Water Torture Attack",[28] - "L7: Wordpress Pingback DDoS",[29] - "L7: DNS-flood",[30] - "L7: HTTP/S-flood",[31] - "L7: FTP-flood",[32] - "L7: SMTP-flood",[33] - "L7: VoIP/SIP-attack",[34] - "L7: POP3-flood",[35] - "L7: SlowRate-attack,"[36] - "other"		[N]	[2], [3]
4.2.2	"comment" (поле данных)	дополнительное описание	текстовое поле (textarea)		[N]	[2], [3]
4.3	"sources" (блок данных)	идентификаторы источников реализации атаки	В случае необходимости указания нескольких значений поля данных (ip) указывается один или несколько объектов в блоке данных "sources"		[N]	[2], [3]

4.3.1	"ip" (поле данных)	IP-адрес источника реализации атаки (в случае большого количества источников компьютерной атаки в блоке "sources" указывается топ 100 IP-адресов атакующих, при этом полный перечень прикладывается в текстовом файле)	Логический адрес IPv4 должен соответствовать спецификации RFC 791 [12]		[N]	[2], [3]
4.4	"power" (блок данных)	мощность реализации атаки			[N]	[2], [3]
4.4.1	"pps" (поле данных)	количество пакетов в секунду	пакет в секунду (Packet per second)		[N]	[2], [3]
4.4.2	"mps" (поле данных)	количество мегабит в секунду	мегабит в секунду (Megabit per second)		[N]	[2], [3]
4.4.3	"rps" (поле данных)	количество запросов в секунду	запросов в секунду (Request per second)		[N]	[2], [3]
4.5	"startTimeAt" (поле данных)	время начала атаки	формат представления данных в соответствии со спецификацией RFC 3339 [11]		[N]	[2], [3]
4.6	"endTimeAt" (поле данных)	время окончания атаки	формат представления данных в соответствии со спецификацией RFC 3339 [11]		[N]	[2], [3]
4.7	"negativeImpact" (блок данных)	негативный эффект от реализации атаки			[N]	[2], [3]
4.7.1.	"type" (поле данных)	тип негативного влияния	Выбирается один код из ограниченного множества возможных значений: - [NAW] - прерывание доступности сервиса; - [OTH] - деградация сервиса; - [NCQ] - негативного влияния на сервис не оказано		[N]	[2], [3]
4.7.2.	"comment" (поле данных)	дополнительное описание	текстовое поле (textarea)		[N]	[2], [3]

6.6.5. Компьютерные атаки, связанные с реализацией несанкционированного доступа к банкоматам и платежным терминалам участников информационного обмена [atmAttacks] (для вектора [INT])

Номер блока (поля) данных	Идентификатор блока (поля) данных	Содержание блока (поля) данных	Формат поля данных	Формат электронного сообщения	Обязательность информирования	Этапы информирования

5	"sourceId" (поле данных)	идентификатор, присвоенный участником информационного обмена	128-битный идентификатор (GUID), сформированный в соответствии со спецификацией RFC 4122 [16], присвоенный участником информационного обмена	"atmAttacks": {"sourceId": "f34030ef-358a-445c-8567-25985ce6d91c","target": {"type": "тип объекта атаки","description": "дополнительное описание"},"attackType": [{"type": "тип атаки в зависимости от объекта атаки","description": "дополнительное описание"}],"attackImage": {"sourceId": "f34030ef-358a-445c-8567-25985ce6d91c","comment": "примечание к вложению","dateTimeAt": "2018-03-22T08:14:38Z","file": {"name": "имя файла","size": "размер файла в байтах","base64": "вложение в формате base64"},"fileLink": "http://domain.com/archive.rar"}},	[N]	[2], [3]
5.1	"target" (блок данных)	идентификатор объекта атаки			[N]	[2], [3]
5.1.1	"type" (поле данных)	тип объекта атаки	Выбирается один код из ограниченного множества возможных значений: - [ATM] - банкомат; - [CIN] - банкомат с возможностью приема денежных средств; - [REC] - банкомат с функцией ресайклинга (recycling); - [POS] - POS-терминал; - [SST] - платежный терминал; - [OTH] - иной объект		[N]	[2], [3]
5.1.2	"description" (поле данных)	дополнительное описание	текстовое поле (textarea)		[N]	[2], [3]
5.2	"attackType" (блок данных)	тип атаки	В случае необходимости указания нескольких значений полей данных (type, description) указывается один или несколько объектов в блоке данных "sources"		[N]	[2], [3]
5.2.1	"type" (поле данных)	тип атаки в зависимости от объекта атаки	Выбирается один код из ограниченного множества возможных значений: - [BBX] - атаки "блэкбокс"; - [DSP] - атаки "прямой диспенс" и их разновидности; - [SKM] - скимминг; - [OTH] - иной способ		[N]	[2], [3]
5.2.2	"description" (поле данных)	дополнительное описание	текстовое поле (textarea)		[N]	[2], [3]
5.3	"attackImage" (блок данных)	дополнительные материалы реализации атаки			[N]	[2], [3]
5.3.1	"sourceId" (поле данных)	идентификатор, присвоенный участником информационного обмена	128-битный идентификатор (GUID), сформированный в соответствии со спецификацией RFC 4122 [16], присвоенный участником информационного обмена		[N]	[2], [3]
5.3.2	"comment" (поле данных)	описание вложения	текстовое поле (textarea)		[N]	[2], [3]

5.3.3	"dateTimeAt" (поле данных)	дата и время добавления файла	формат представления данных в соответствии со спецификацией RFC 3339 [11]		[N]	[2], [3]
5.3.4.1	"file" (подблок данных)	файл данных, содержащий дополнительные материалы	Указывается наименование, размер файла (не более 5 Мб), выполняется кодировка в формате Base64		[N]	[2], [3]
5.3.5	"fileLink" (поле данных)	ссылка для получения (скачивания) файла данных, содержащего дополнительные материалы	Указывается URL-адрес для скачивания файла, в случае если его размер превышает 5 Мб, в соответствии со спецификацией RFC 3986 [15]		[N]	[2], [3]

6.6.6. Компьютерные атаки, связанные с эксплуатацией уязвимостей информационной инфраструктуры участников информационного обмена и их клиентов [vulnerabilities] (для вектора [INT], [EXT])

Номер блока (поля) данных	Идентификатор блока (поля) данных	Содержание блока (поля) данных	Формат поля данных	Формат электронного сообщения	Обязате информ
6	"sourceId" (поле данных)	идентификатор, присвоенный участником информационного обмена	128-битный идентификатор (GUID), сформированный в соответствии со спецификацией RFC 4122 [16], присвоенный участником информационного обмена	"vulnerabilities": [{"sourceId": "f34030ef-358a-445c-8567-25985ce6d91c","target": {"ip": "127.0.0.1","domain": "example.com","url": "http://example.com","serviceType": "тип информационного сервиса"},"sources": [{"ip": "127.0.0.1","url": "http://example.com"}],"identifier": "идентификатор уязвимости","cvss": "Метрика CVSS","idCustom": {"description": "описание уязвимости","swName": "наименование программного обеспечения","swVer": "версия программного обеспечения","cweType": "тип ошибки CWE","class": "класс уязвимости","osName": "операционная система, под управлением которой функционирует программное обеспечение с обнаруженной уязвимостью","detectedAt": "дата и время выявления уязвимости","baseCVSS": "базовый вектор уязвимости","danger": "уровень опасности выявленной уязвимости","measures": "возможные меры по устранению уязвимости","status": "статус уязвимости","exploit": "наличие эксплойта","recommendation": "информация об устранении уязвимости","link": "ссылки на источники информации об устранении уязвимости","manufacturer": "компания (организация) - производитель (разработчик) программного обеспечения, в котором обнаружена уязвимость"}}],	[
6.1	"target" (блок данных)	идентификаторы объекта атаки			[
6.1.1	"ip" (поле данных)	IP-адрес	Логический адрес IPv4 должен соответствовать спецификации RFC 791 [12]		[
6.1.2	"domain" (поле данных)	доменное имя	Доменное имя согласно спецификации RFC 1034 [14], а также международной иерархии доменных зон в соответствии со спецификацией RFC 5890 [13]		[
6.1.3	"url" (поле данных)	URL-адрес	URL в соответствии со спецификацией RFC 3986 [15]		[
6.1.4	"serviceType" (поле данных)	тип информационного сервиса	текстовое поле (textarea)		[
6.2	"sources" (блок данных)	идентификаторы источников, с которых была выявлена эксплуатация уязвимости	В случае необходимости указания нескольких значений полей данных (ip, url) указывается один или несколько объектов в блоке данных "sources"		[
6.2.1	"ip" (поле данных)	IP-адрес	Логический адрес IPv4 должен соответствовать спецификации RFC 791 [12]		[
6.2.2	"url" (поле данных)	URL-адрес	URL в соответствии со спецификацией RFC 3986 [15]		[
6.3	"identifier" (поле данных)	идентификатор уязвимости	Если выявлена уязвимость, должен быть указан ее тип в соответствии с классификацией ФСТЭК России, CVE: - ФСТЭК России - https://bdu.fstec.ru/vul; - Common Vulnerabilities and Exposures (CVE), https://cve.mitre.org/data/downloads/allitems.html		[
6.4	"cvss" (поле данных)	метрика CVSS	Указывается метрика CVSS v 3.0 (The Common Vulnerability Scoring System (CVSS), если определена . Указывается максимально возможное количество метрик из перечисленных: базовая метрика, временная метрика, контекстная метрика, метрика окружения. (В случае если метрика не определена, необходимо использовать калькулятор ФСТЭК России - https://bdu.fstec.ru/cvss3)		[
6.5	"idCustom" (блок данных)	формирование идентификатора уязвимости			[

6.5.1	"description" (поле данных)	описание уязвимости	текстовое поле (textarea)		[
6.5.2	"swName" (поле данных)	наименование программного обеспечения	текстовое поле (textarea)		[
6.5.3	"swVer" (поле данных)	версия программного обеспечения	текстовое поле (textarea)		[
6.5.4	"cweType" (поле данных)	тип ошибки, установленный в соответствии с общим перечнем ошибок CWE	в соответствии с Common Weakness Enumeration (CWE) (https://cwe.mitre.org/)		[
6.5.5	"class" (поле данных)	класс уязвимости	Выбирается один код из ограниченного множества возможных значений: - [COD] - уязвимость кода - уязвимость, появившаяся в результате разработки программного обеспечения без учета требований по безопасности информации; - [ARH] - уязвимость архитектуры - уязвимость, появившаяся в результате выбора, компоновки компонентов программного обеспечения, содержащих уязвимости; - [MULT] - уязвимость многофакторная (обусловленная наличием в программном обеспечении уязвимостей различных классов)		[
6.5.6	"osName" (поле данных)	операционная система, под управлением которой функционирует программное обеспечение с обнаруженной уязвимостью	текстовое поле (textarea)		[
6.5.7	"dateTimeAt" (поле данных)	дата и время выявления уязвимости	формат представления данных в соответствии со спецификацией RFC 3339 [11]		[
6.5.8	"baseCVSS" (поле данных)	базовый вектор уязвимости	в соответствии с CVSS 3.0 (https://bdu.fstec.ru/cvss3)		[
6.5.9	"danger" (поле данных)	уровень опасности выявленной уязвимости	Выбирается один код из ограниченного множества возможных значений в соответствии с результатами базового вектора уязвимости: - [LL] - низкий уровень, если 0,0 - [ML] - средний уровень, если 4,0 - [HL] - высокий уровень, если 7,0 - [CL] - критический уровень, если V = 10,0		[
6.5.10	"measures" (поле данных)	возможные меры по устранению уязвимости	текстовое поле (textarea)		[
6.5.11	"status" (поле данных)	статус уязвимости	Выбирается один код из ограниченного множества возможных значений: - [APR_M] - "подтверждена производителем" - если наличие уязвимости было подтверждено производителем (разработчиком) программного обеспечения, в котором содержится уязвимость; - [APR_R] - "подтверждена в ходе исследований" - если наличие уязвимости было подтверждено исследователем (организацией), не являющимся производителем (разработчиком) программного обеспечения; - [Potential] - "потенциальная уязвимость" - во всех остальных случаях		[
6.5.12	"exploit" (поле данных)	наличие эксплойта	текстовое поле (textarea)		[
6.5.13	"recommendation" (поле данных)	информация об устранении уязвимости	текстовое поле (textarea)		[
6.5.14	"link" (поле данных)	ссылки на источники информации об устранении уязвимости	текстовое поле (textarea)		[

6.5.15	"manufacturer" (поле данных)	компания (организация) - производитель (разработчик) программного обеспечения, в котором обнаружена уязвимость	текстовое поле (textarea)		[

6.6.7. Компьютерные атаки, связанные с подбором (взломом), компрометацией аутентификационных (учетных) данных [bruteForces] (для вектора [INT])

Номер блока (поля) данных	Идентификатор блока (поля) данных	Содержание блока (поля) данных	Формат поля данных	Формат электронного сообщения	Обязательность информирования	Этапы информирое
7	"sourceId" (поле данных)	идентификатор, присвоенный участником информационного обмена	128-битный идентификатор (GUID), сформированный в соответствии со спецификацией RFC 4122 [16], присвоенный участником информационного обмена	"bruteForces": [{"sourceId": "f34030ef-358a-445c-8567-25985ce6d91c","target": {"ip": "127.0.0.1","url": "http://example.com","serviceType": "тип сервиса"},"sources": [{"ip": "127.0.0.1"}],"accountOs": {"name": "имя учетной записи","privileges": "уровень (привилегии) учетной записи"}}],	[N]	[2], [3]
7.1	"target" (блок данных)	идентификаторы объекта атаки			[N]	[2], [3]
7.1.1	"ip" (поле данных)	IP-адрес	Логический адрес IPv4 должен соответствовать спецификации RFC 791 [12]		[N]	[2], [3]
7.1.2	"domain" (поле данных)	доменное имя	Доменное имя согласно спецификации RFC 1034 [14], а также международной иерархии доменных зон в соответствии со спецификацией RFC 5890 [13]		[N]	[2], [3]
7.1.3	"url" (поле данных)	URL-адрес	URL в соответствии со спецификацией RFC 3986 [15]		[N]	[2], [3]
7.1.4	"serviceType" (поле данных)	тип информационного сервиса	текстовое поле (textarea)		[N]	[2], [3]
7.2	"sources" (блок данных)	идентификаторы источников реализации атаки	В случае необходимости указания нескольких значений поля данных (ip) указывается один или несколько объектов в блоке данных "sources"		[N]	[2], [3]
7.2.1	"ip" (поле данных)	IP-адрес источника реализации атаки (в случае большого количества источников компьютерной атаки в блоке данных "sources" указывается топ-100 IP-адресов атакующих, при этом полный перечень прикладывается в текстовом файле)	Логический адрес IPv4 должен соответствовать спецификации RFC 791 [12]		[N]	[2], [3]
7.3	"accountOs" (блок данных)	идентификаторы скомпрометированной учетной записи			[N]	[2], [3]
7.3.1	"name" (поле данных)	имя учетной записи	текстовое поле (textarea)		[N]	[2], [3]
7.3.2	"privileges" (поле данных)	уровень (привилегии) учетной записи	текстовое поле (textarea)		[N]	[2], [3]

6.6.8. Компьютерные атаки, связанные с реализацией спам-рассылки, осуществляемой в отношении участников информационного обмена и их клиентов [spams] (для вектора [INT], [EXT])

Номер блока (поля) данных	Идентификатор блока (поля) данных	Содержание блока (поля) данных	Формат поля данных	Формат электронного сообщения	Обязательность информирования	Этапы информирова
8	"sourceId" (поле данных)	идентификатор, присвоенный участником информационного обмена	128-битный идентификатор (GUID), сформированный в соответствии со спецификацией RFC 4122 [16], присвоенный участником информационного обмена	"spams": [{"sourceId": "f34030ef-358a-445c-8567-25985ce6d91c","receivedAt": "2018-03-22T08:14:38Z","targets": [{"email": "qwerty@example.ru"}],"sources": [{"ip": "127.0.0.1","domain": "example.com","email": "qwerty@example.ru"}],"spamImages": {"sourceId": "f34030ef-358a-445c-8567-25985ce6d91c","comment": "описание вложения","dateTimeAt": "2018-03-22T08:14:38Z","file": {"name": "имя файла","size": "размер файла в байтах","base64": "вложение в формате base64"},"fileLink": "http://domain.com/archive.rar"}}],	[N]	[2], [3]
8.1	"receivedAt" (поле данных)	дата и время получения спам-сообщения	формат представления данных в соответствии со спецификацией RFC 3339 [11]		[N]	[2], [3]
8.2	"targets" (блок данных)	идентификаторы объектов атаки (получатели спам-сообщения)	В случае необходимости указания нескольких значений поля данных (email) указывается один или несколько объектов в блоке данных "targets"		[N]	[2], [3]
8.2.1	"email" (поле данных)	электронный почтовый адрес получателя спам-сообщения	Адрес электронного почтового ящика отправителя представляется в формате в соответствии со спецификацией RFC 5322 [18]		[N]	[2], [3]
8.3	"sources" (блок данных)	идентификаторы источников реализации атаки (отправители спам-сообщения)	В случае необходимости указания нескольких значений полей данных (ip, domain, email) указывается один или несколько объектов в блоке данных "sources"		[N]	[2], [3]
8.3.1	"ip" (поле данных)	IP-адрес	Логический адрес IPv4 должен соответствовать спецификации RFC 791 [12]		[N]	[2], [3]
8.3.2	"domain" (поле данных)	доменное имя	Доменное имя согласно спецификации RFC 1034 [14], а также международной иерархии доменных зон в соответствии со спецификацией RFC 5890 [13]		[N]	[2], [3]
8.3.3	"email" (поле данных)	электронный почтовый адрес отправителя спам-сообщения	Адрес электронного почтового ящика отправителя представляется в формате в соответствии со спецификацией RFC 5322 [18]		[N]	[2], [3]
8.4	"spamImage" (блок данных)	образец спам-сообщения			[N]	[2], [3]

8.4.1	"sourceId" (поле данных)	идентификатор, присвоенный участником информационного обмена	128-битный идентификатор (GUID), сформированный в соответствии со спецификацией RFC 4122 [16], присвоенный участником информационного обмена		[N]	[2], [3]
8.4.2	"comment" (поле данных)	описание вложения	текстовое поле (textarea)		[N]	[2], [3]
8.4.3	"dateTimeAt" (поле данных)	дата и время добавления файла	формат представления данных в соответствии со спецификацией RFC 3339 [11]		[N]	[2], [3]
8.4.4.1	"file" (блок данных)	файл данных, содержащий дополнительные материалы	Указывается наименование, размер файла (не более 5 Мб), выполняется кодировка в формате Base64		[N]	[2], [3]
8.4.5	"fileLink" (поле данных)	ссылка для получения (скачивания) файла данных, содержащего дополнительные материалы	Указывается URL-адрес для скачивания файла, в случае если его размер превышает 5 Мб, в соответствии со спецификацией RFC 3986 [15]		[N]	[2], [3]

6.6.9. Компьютерные атаки, связанные с выявлением взаимодействия объектов информационной инфраструктуры участников информационного обмена с командными центрами Ботнет [controlCenters] (для вектора [INT])

Номер блока (поля) данных	Идентификатор блока (поля) данных	Содержание блока (поля) данных	Формат поля данных	Формат электронного сообщения	Обязательность информирования	Э инфор
9	"sourceId" (поле данных)	идентификатор, присвоенный участником информационного обмена	128-битный идентификатор (GUID), сформированный в соответствии со спецификацией RFC 4122 [16], присвоенный участником информационного обмена	"controlCenters": [{"sourceId": "f34030ef-358a-445c-8567-25985ce6d91c","target": {"ip": "127.0.0.1","url": "http://example.com"},"hostUrl": "http://example.com","intruderIp": "1.1.1.1","intruderActions": "что предшествовало инциденту","description": "известные сведения о командном центре Ботнет","nodes": [{"ip": "127.0.0.1","lastRequestRateTimeAt": "2018-03-22T08:08:49Z"}]}],	[N]	[
9.1	"target" (блок данных)	идентификаторы объекта атаки			[N]	[
9.1.1	"ip" (поле данных)	IP-адрес	Логический адрес IPv4 должен соответствовать спецификации RFC 791 [12]		[N]	[
9.1.2	"url" (поле данных)	URL-адрес	URL в соответствии со спецификацией RFC 3986 [15]		[N]	[
9.2	"hostUrl" (поле данных)	URL, на котором размещен командный центр Ботнет	URL в соответствии со спецификацией RFC 3986 [15]		[N]	[
9.3	"intruderIp" (поле данных)	IP-адрес злоумышленника, разместившего командный центр Ботнет	Логический адрес IPv4 должен соответствовать спецификации RFC 791 [12]		[N]	[
9.4	"intruderActions" (поле данных)	описание несанкционированной активности в информационной инфраструктуре участника информационного обмена	текстовое поле (textarea)		[N]	[
9.5	"description" (поле данных)	дополнительное описание командного центра Ботнет	текстовое поле (textarea)		[N]	[
9.6	"nodes" (блок данных)	идентификаторы обращения к командному центру Ботнет	В случае необходимости указания нескольких значений полей данных (ip, lastRequestRateTimeAt) указывается один или несколько объектов в блоке данных		[N]	[
9.6.1	"ip" (поле данных)	внешний IP-адрес (участника информационного обмена)	Логический адрес IPv4 должен соответствовать спецификации RFC 791 [12]		[N]	[
9.6.2	"lastRequest RatetimeAt" (поле данных)	дата и время последнего взаимодействия с командным центром Ботнет	формат представления данных в соответствии со спецификацией RFC 3339 [11]		[N]	[

6.6.10. Компьютерные атаки, связанные с изменением (подменой) идентификатора мобильного абонента (IMSI) номера сим-карты, а также с заменой идентификатора мобильного оборудования (IMEI) [sim] (для вектора [EXT])

Номер блока (поля) данных	Идентификатор блока (поля) данных	Содержание блока (поля) данных	Формат поля данных	Формат электронного сообщения	Обязательность информирования	Этапы информиров
10	"sourceId" (поле данных)	идентификатор, присвоенный участником информационного обмена	128-битный идентификатор (GUID), сформированный в соответствии со спецификацией RFC 4122 [16], присвоенный участником информационного обмена	"sim": {"sourceId": "f34030ef-358a-445c-8567-25985ce6d91c","mobileOperator": "название оператора связи","phoneNumber": "1212312345678","imsi": "123456789000000","imsiChangedAt": "2018-03-22T08:08:49Z"},	[N]	[2], [3]
10.1	"mobileOperator" (поле данных)	наименование мобильного оператора связи	текстовое поле (textarea)		[N]	[2], [3]
10.2	"phoneNumber" (поле данных)	номер мобильного телефона	в формате KKKXXXNNNNNNNN, где: KKK - от одного до трех символов кода страны; XXX - код оператора; NNNNNNN - 7 знаков номера. Номер телефона представляется без знака плюс (+), пробелов (_) и знаков разделения (-).		[N]	[2], [3]
10.3	"imsi" (поле данных)	уникальный номер сим-карты (номер IMSI)	в формате: XXXXXXXXXXXXXXX		[N]	[2], [3]
10.4	"imsiChangedAt" (поле данных)	дата и время фиксации смены IMSI	формат представления данных в соответствии со спецификацией RFC 3339 [11]		[N]	[2], [3]

6.6.11. Компьютерные атаки, связанные с информацией, вводящей участников информационного обмена и их клиентов, а также иных лиц, взаимодействующих с ними, в заблуждение относительно принадлежности информации, распространяемой посредством сети Интернет, вследствие сходства доменных имен, оформления или содержания. Фишинг [phishingAttacks] (для вектора [EXT], [INT])

Номер блока (поля) данных	Идентификатор блока (поля) данных	Содержание блока (поля) данных	Формат поля данных	Формат электронного сообщения	Обязательность информирования	Этапы информирования
11	"sourceId" (поле данных)	идентификатор, присвоенный участником информационного обмена	128-битный идентификатор (GUID), сформированный в соответствии со спецификацией RFC 4122 [16], присвоенный участником информационного обмена		[N]	[2], [3]
11.1	"target" (блок данных)	идентификаторы объекта атаки (легитимный ресурс)			[N]	[2], [3]
11.1.1	"ip" (поле данных)	IP-адрес	Логический адрес IPv4 должен соответствовать спецификации RFC 791 [12]		[N]	[2], [3]
11.1.2	"domain" (поле данных)	доменное имя	Доменное имя согласно спецификации RFC 1034 [14], а также международной иерархии доменных зон в соответствии со спецификацией RFC 5890 [13]	"phishingAttacks": [{"sourceId":	[N]	[2], [3]

11.2	"harmful" (блок данных)	идентификаторы источников фишинговых ресурсов	В случае необходимости указания нескольких значений полей данных (ip, url) указывается один или несколько объектов в блоке данных "harmful"	"f34030ef-358a-445c-8567-25985ce6d91c","target": {"ip": "127.0.0.1","domain": "example.com"},"harmful": [{"ip": "127.0.0.1","url": "http://example.com"}],"fixationAt": "2018-03-22T08:08:49Z ","messageAttachment": {"sourceId": "f34030ef-358a-445c-8567-25985ce6d91c","comment": "описание вложения","dateTimeAt": "2018-03-22T08:08:49Z","file": {"name": "имя файла","size": "размер файла в байтах","base64": "вложение в формате base64"},"fileLink": "http://domain.com/archive.rar"}}],	[N]	[2], [3]
11.2.1	"ip" (поле данных)	IP-адрес	Логический адрес IPv4 должен соответствовать спецификации RFC 791 [12]		[N]	[2], [3]
11.2.2	"url" (поле данных)	URL-адрес	URL в соответствии со спецификацией RFC 3986 [15]		[N]	[2], [3]
11.3	"fixationAt" (поле данных)	дата и время фиксирования фишингового сообщения	формат представления данных в соответствии со спецификацией RFC 3339 [11]		[N]	[2], [3]
11.4	"message Attachment" (блок данных)	образец фишингового обращения			[N]	[2], [3]
11.4.1	"sourceId" (поле данных)	идентификатор, присвоенный участником информационного обмена	128-битный идентификатор (GUID), сформированный в соответствии со спецификацией RFC 4122 [16], присвоенный участником информационного обмена		[N]	[2], [3]
11.4.2	"comment" (поле данных)	описание вложения	текстовое поле (textarea)		[N]	[2], [3]
11.4.3	"dateTimeAt" (поле данных)	дата и время добавления файла	формат представления данных в соответствии со спецификацией RFC 3339 [11]		[N]	[2], [3]
11.4.4.1	"file" (блок данных)	файл данных, содержащий дополнительные материалы	Указывается наименование, размер файла (не более 5 Мб), выполняется кодировка в формате Base64		[N]	[2], [3]
11.4.5	"fileLink" (поле данных)	ссылка для получения (скачивания) файла данных, содержащего дополнительные материалы	Указывается URL-адрес для скачивания файла в случае если его размер превышает 5 Мб, в соответствии со спецификацией RFC 3986 [15]		[N]	[2], [3]

6.6.12. Компьютерные атаки, связанные с распространением информации, касающейся предложений и (или) предоставления на территории Российской Федерации финансовых услуг лицами, не имеющими права их оказывать в соответствии с законодательством Российской Федерации. Размещение в сети Интернет запрещенного контента [prohibitedContents] (для вектора [EXT], [INT])

Номер блока (поля) данных	Идентификатор блока (поля) данных	Содержание блока (поля) данных	Формат поля данных	Формат электронного сообщения	Обязательность информирования	Этапы информирования
12	"sourceId" (поле данных)	идентификатор, присвоенный участником информационного обмена	128-битный идентификатор (GUID), сформированный в соответствии со спецификацией RFC 4122 [16], присвоенный участником информационного обмена	"prohibitedContents": [{"sourceId": "f34030ef-358a-445c-8567-25985ce6d91c","sources": [{"ip": "127.0.0.1","url": "http://example.com"}],"type": "тип запрещенного контента"}],	[N]	[2], [3]
12.1	"sources" (блок данных)	идентификаторы источников запрещенного контента	В случае необходимости указания нескольких значений полей данных (ip, url) указывается один или несколько объектов в блоке данных "target"		[N]	[2], [3]
12.1.1	"ip" (поле данных)	IP-адрес	Логический адрес IPv4 должен соответствовать спецификации RFC 791 [12]		[N]	[2], [3]
12.1.2	"url" (поле данных)	URL-адрес	URL в соответствии со спецификацией RFC 3986 [15]		[N]	[2], [3]
12.2	"type" (поле данных)	тип запрещенного контента	текстовое поле (textarea)		[N]	[2], [3]

6.6.13. Компьютерные атаки, связанные с размещением в сети Интернет информации, позволяющей осуществить неправомерный доступ к информационным системам участников информационного обмена и их клиентов, используемым при предоставлении (получении) финансовых услуг, в том числе путем неправомерного доступа к конфиденциальной информации клиентов. Размещение в сети Интернет вредоносного ресурса [maliciousResources] (для вектора [EXT], [INT])

Номер блока (поля) данных	Идентификатор блока (поля) данных	Содержание блока (поля) данных	Формат поля данных	Формат электронного сообщения	Обязательность информирования	Этапы информирован
13	"sourceId" (поле данных)	идентификатор, присвоенный участником информационного обмена	128-битный идентификатор (GUID), сформированный в соответствии со спецификацией RFC 4122 [16], присвоенный участником информационного обмена	"maliciousResources": [{"sourceId": "f34030ef-358a-445c-8567-25985ce6d91c","sources": [{"ip": "127.0.0.1","url": "http://example.com"}],"activityType": "описание вредоносной активности"}],	[N]	[2], [3]
13.1	"sources" (блок данных)	идентификаторы источников вредоносного ресурса	В случае необходимости указания нескольких значений полей данных (ip, url) указывается один или несколько объектов в блоке данных "target"		[N]	[2], [3]
13.1.1	"ip" (поле данных)	IP-адрес	Логический адрес IPv4 должен соответствовать спецификации RFC 791 [12]		[N]	[2], [3]
13.1.2	"url" (поле данных)	URL-адрес	URL в соответствии со спецификацией RFC 3986 [15]		[N]	[2], [3]
13.2	"activityType" (поле данных)	тип вредоносной активности	текстовое поле (textarea)		[N]	[2], [3]

6.6.14. Компьютерные атаки, связанные с изменением контента [changeContent] (для вектора [INT])

Номер блока (поля) данных	Идентификатор блока (поля) данных	Содержание блока (поля) данных	Формат поля данных	Формат электронного сообщения	Обязательность информирования	Этапы информирования
14	"sourceId" (поле данных)	идентификатор, присвоенный участником информационного обмена	128-битный идентификатор (GUID), сформированный в соответствии со спецификацией RFC 4122 [16], присвоенный участником информационного обмена	"changeContent": [{"sourceId": "f34030ef-358a-445c-8567-25985ce6d91c","targets": [{"ip": "127.0.0.1","url": "http://example.com"}],"type": "тип контента"}],	[N]	[2], [3]
14.1	"targets" (блок данных)	идентификаторы объектов атаки, на которых произведено изменение контента	В случае необходимости указания нескольких значений полей данных (ip, url) указывается один или несколько объектов в блоке данных "target"		[N]	[2], [3]
14.1.1	"ip" (поле данных)	IP-адрес	Логический адрес IPv4 должен соответствовать спецификации RFC 791 [12]		[N]	[2], [3]
14.1.2	"url" (поле данных)	URL-адрес	URL в соответствии со спецификацией RFC 3986 [15]		[N]	[2], [3]
14.2	"type" (поле данных)	тип измененного контента	текстовое поле (textarea)		[N]	[2], [3]

6.6.15. Компьютерные атаки, связанные со сканированием программных портов объектов информационной инфраструктуры участников информационного обмена лицами, не обладающими соответствующими полномочиями [scanPorts] (для вектора [INT])

Номер блока (поля) данных	Идентификатор блока (поля) данных	Содержание блока (поля) данных	Формат поля данных	Формат электронного сообщения	Обязательность информирования	Этапы информирования
15	"sourceId" (поле данных)	идентификатор, присвоенный участником информационного обмена	128-битный идентификатор (GUID), сформированный в соответствии со спецификацией RFC 4122 [16], присвоенный участником информационного обмена	"scanPorts": [{"sourceId": "f34030ef-358a-445c-8567-25985ce6d91c","sources": [{"ip": "IP-адрес"}],"ports": ["21"],"method": "информация о методах сканирования или используемом для этого программном обеспечении","startTimeAt": "2018-03-22T08:08:49Z","endTimeAt": "2018-03-22T08:09:49Z"}],	[N]	[2], [3]
15.2	"sources" (блок данных)	идентификаторы источников вредоносной активности	В случае необходимости указания нескольких значений поля данных (ip) указывается один или несколько объектов в блоке данных "sources"		[N]	[2], [3]
15.2.1	"ip" (поле данных)	IP-адрес	Логический адрес IPv4 должен соответствовать спецификации RFC 791 [12]		[N]	[2], [3]
15.3	"ports" (поле данных)	номера портов, которые подверглись сканированию	текстовое поле (textarea)		[N]	[2], [3]
15.4	"method" (поле данных)	информация о методах сканирования или используемом для этого программном обеспечении	текстовое поле (textarea)		[N]	[2], [3]
15.5	"startTimeAt" (поле данных)	время начала сканирования	формат представления данных в соответствии со спецификацией RFC 3339 [11]		[N]	[2], [3]
15.6	"endTimeAt" (поле данных)	время окончания сканирования	формат представления данных в соответствии со спецификацией RFC 3339 [11]		[N]	[2], [3]

6.6.16. Иные компьютерные атаки, направленные на объекты информационной инфраструктуры участников информационного обмена и их клиентов [other] (для вектора [INT], [EXT])

Номер блока (поля) данных	Идентификатор блока (поля) данных	Содержание блока (поля) данных	Формат поля данных	Формат электронного сообщения	Обязательность информирования	Этапы информирования
16	"sourceId" (поле данных)	идентификатор, присвоенный участником информационного обмена	128-битный идентификатор (GUID), сформированный в соответствии со спецификацией RFC 4122 [16], присвоенный участником информационного обмена	"other": {"sourceId": "f34030ef-358a-445c-8567-25985ce6d91c","description": "описание компьютерной атаки","source": {"ip": "127.0.0.1","url": "http://example.com"},"type": "иной тип запрещенного, вредоносного, измененного контента","attachment": {"sourceId": "f34030ef-358a-445c-8567-25985ce6d91c","comment": "описание вложения","dateTimeAt": "2018-03-22T08:08:49Z","file": {"name": "имя файла","size": "размер файла в байтах","base64": "вложение в формате base64"},"fileLink": "http://domain.com/archive.rar"}}},	[N]	[2], [3]
16.1	"description" (поле данных)	описание компьютерной атаки	текстовое поле (textarea)		[N]	[2], [3]
16.2	"source" (блок данных)	идентификаторы иного источника вредоносного, запрещенного контента/ресурса			[N]	[2], [3]
16.2.1	"ip" (поле данных)	IP-адрес	Логический адрес IPv4 должен соответствовать спецификации RFC 791 [12]		[N]	[2], [3]
16.2.2	"url" (поле данных)	URL-адрес	URL в соответствии со спецификацией RFC 3986 [15]		[N]	[2], [3]
16.2.3	"type" (поле данных)	иной тип запрещенного, вредоносного, измененного контента	текстовое поле (textarea)		[N]	[2], [3]
16.3	"attachment" (блок данных)	дополнительные данные для идентификации компьютерной атаки			[N]	[2], [3]
16.3.1	"sourceId" (поле данных)	идентификатор, присвоенный участником информационного обмена	128-битный идентификатор (GUID), сформированный в соответствии со спецификацией RFC 4122 [16], присвоенный участником информационного обмена		[N]	[2], [3]
15.3.2	"comment" (поле данных)	описание вложения	текстовое поле (textarea)		[N]	[2], [3]
15.3.3	"dateTimeAt" (поле данных)	дата и время добавления файла	формат представления данных в соответствии со спецификацией RFC 3339 [11]		[N]	[2], [3]
16.3.4	"file" (блок данных)	файл данных, содержащий дополнительные материалы	Указывается наименование, размер файла (не более 5 Мб), выполняется кодировка в формате Base64		[N]	[2], [3]
16.3.5	"fileLink" (поле данных)	ссылка для получения (скачивания) файла данных, содержащего дополнительные материалы	Указывается URL-адрес для скачивания файла, в случае если его размер превышает 5 мб, в соответствии со спецификацией RFC 3986 [15]		[N]	[2], [3]

6.7. Информация по результатам завершения реализации инцидента и соответствующие формы электронных сообщений

6.7.1. Организационная информация [finalReport]

Номер блока (поля) данных	Идентификатор блока (поля) данных	Содержание блока (поля) данных	Формат поля данных	Формат электронного сообщения	Обязательность информирования	Этапы информирования
1.1	"closeDateAt" (поле данных)	дата и время закрытия инцидента	формат представления данных в соответствии со спецификацией RFC 3339 [11]	"finalReport": {"closeDateAt": "дата и время закрытия инцидента","recovery": "идентификатор восстановления после реализации инцидента","description": "дополнительное описание в случае невозможности восстановления","rootCause": "ключевые причины возникновения инцидента","mainActions": "предпринятые действия для предотвращения возникновения инцидента в будущем",	[O]	[3]
1.2	"recovery" (поле данных)	идентификатор восстановления после реализации инцидента	Выбирается один код из ограниченного множества возможных значений: - [Full] - предоставление финансовых (банковских) услуг восстановлено полностью; - [Not_Full] - предоставление финансовых (банковских) услуг восстановлено частично		[O]	[3]
1.3	"description" (поле данных)	дополнительное описание в случае невозможности восстановления	текстовое поле (textarea)		[O]	[3]
1.4	"rootCause" (поле данных)	ключевые причины возникновения инцидента	текстовое поле (textarea)		[O]	[3]
1.5	"mainActions" (поле данных)	предпринятые действия для предотвращения возникновения инцидента в будущем	текстовое поле (textarea)		[O]	[3]

6.7.2. Техническая информация, описывающая сигнатуру компьютерных атак [signatures]

Номер блока (поля) данных	Идентификатор блока (поля) данных	Содержание блока (поля) данных	Формат поля данных	Формат электронного сообщения	Обязательность информирования	Этапы информирова
2.1	"signatures" (блок данных)	сигнатура	В случае необходимости указания нескольких значений полей данных (identifier, name, source, eventsAmount) указывается один или несколько объектов в блоке данных "signatures"	"signatures": [{"identifier": "идентификатор сигнатуры","name": "средство обнаружения","source": "источник получения сигнатуры","eventsAmount": "количество срабатываний сигнатуры"}],"snort": ["rule1","rule2"],"attachment":	[N]	[3]
2.2	"identifier" (поле данных)	уникальный идентификатор сигнатуры	последовательность символов, полученных в результате вычисления хэш-функции MD5		[N]	[3]
2.3	"name" (поле данных)	средство обнаружения	текстовое поле (textarea)		[N]	[3]
2.4	"source" (поле данных)	источник получения сигнатуры	текстовое поле (textarea)		[N]	[3]
2.5	"eventsAmount" (поле данных)	количество срабатываний сигнатуры	текстовое поле (textarea)		[N]	[3]

2.6	"snort" (поле данных)	Snort-правила	формат представления в виде: (ключ_1: значение_1; ключ_2: значение_2; ... ключ_N: значение_N;)	["rule1", "rule2"], "attachment": {"sourceId": "f34030ef-358a-445c-8567-25985ce6d91c","comment": "описание вложения","dateTimeAt": "2018-03-22T08:14:38Z","file": {"name": "имя файла","size": "размер файла в байтах","base64": "вложение в формате base64"},"fileLink": "http://domain.com/archive.rar"}}}}	[N]	[3]
2.7	"attachment" (блок данных)	дополнительные данные по результатам завершения реализации инцидента			[N]	[3]
2.7.1	"sourceId" (поле данных)	идентификатор, присвоенный участником информационного обмена	128-битный идентификатор (GUID), сформированный в соответствии со спецификацией RFC 4122 [16], присвоенный участником информационного обмена		[N]	[3]
2.7.2	"comment" (поле данных)	описание вложения	текстовое поле (textarea)		[N]	[3]
2.7.3	"dateTimeAt" (поле данных)	дата и время добавления файла	формат представления данных в соответствии со спецификацией RFC 3339 [11]		[N]	[3]
2.7.4	"file" (блок данных)	файл данных, содержащий дополнительные материалы	Указывается наименование, размер файла (не более 5 Мб), выполняется кодировка в формате Base64		[N]	[3]
2.7.5	"fileLink" (поле данных)	ссылка для получения (скачивания) файла данных, содержащего дополнительные материалы	Указывается URL-адрес для скачивания файла, в случае, если его размер превышает 5 Мб, в соответствии со спецификацией RFC 3986 [15]		[N]	[3]

7. Форма запроса Банка России к участнику информационного обмена, обслуживающему получателя средств

Банк России при получении информации в соответствии с главой 6 раздела 6.5 настоящего стандарта от участника информационного обмена, обслуживающего плательщика, в целях проверки конкретного получателя средств, направляет запрос участнику информационного обмена, обслуживающему получателя средств, а также уведомление о приостановлении зачисления денежных средств на банковский счет получателя средств или увеличении остатка электронных денежных средств получателя средств.

7.1. Идентификационные данные запроса Банка России. Блок данных [HEADER]

Номер блока (поля) данных	Идентификатор блока (поля) данных	Содержание блока (поля) данных	Формат поля данных	Формат электронного сообщения
1.1	"schemaType" (поле данных)	тип электронного сообщения	Указывается значение [antifraudRequest] - дополнительный запрос участнику информационного обмена - "получателю средств" несанкционированной операции	{"header": {"schemaType": "antifraudRequest","schemaVersion": "1","version": "1","memberId": "9527dd0c-0765-4f1c-8f5f-70a02cf4046c","publishedAt": "2002-10-02T15:00:00.05Z"},
1.2	"schemaVersion" (поле данных)	версия схемы типа электронного сообщения	текстовое поле (textarea)	
1.3	"version" (поле данных)	номер версии электронного сообщения в процессе информационного обмена	числовое значение (int)	
1.4	"memberId" (поле данных)	идентификатор участника информационного обмена, присвоенный Банком России	128-битный идентификатор (GUID), сформированный в соответствии со спецификацией RFC 4122 [16], присвоенный Банком России	
1.5	"publishedAt" (поле данных)	дата и время первичного информирования	формат представления данных в соответствии со спецификацией RFC 3339 [11]	

7.2. Описание формы запроса Банка России. Блок данных [antifraudRequest]

Форма запроса Банка России к участнику информационного обмена, обслуживающему получателя средств, применяется:

при запросе у оператора по переводу денежных средств, обслуживающего получателя средств, включая оператора электронных денежных средств, информации, определяющей получателя средств [4];

при направлении уведомления о приостановлении зачисления денежных средств на банковский счет получателя средств или увеличении остатка электронных денежных средств получателя средств [20].

Номер блока (поля) данных	Идентификатор блока (поля) данных	Содержание блока (поля) данных	Формат поля данных	Формат электронного сообщения
1	"antifraudRequest" (блок данных)		В случае необходимости указания нескольких значений блоков данных (payer, payee) указывается один или несколько объектов в блоке данных "antifraudRequest"	"antifraudRequest": [{"sourceId": "f34030ef-358a-445c-8567-25985ce6d91c","victim": "информация о субъектном статусе плательщика","payer": {"bik": "123456789","inn": "123456789000","namePayer": "наименование организации, являющейся плательщиком","payerTransferId": {"transferType": "тип способа реализации перевода денежных средств","paymentCard": {"number": "1234123412341234123412","sum": "сумма операции по осуществлению перевода денежных средств с использованием платежных карт","currency": "валюта операции по осуществлению перевода денежных средств","dateTimeAt": "2018-01-13T09:14:38Z","rrn": "номер, генерируемый для операции по переводу денежных средств при выполнении ее авторизации"},"settlement": {"number": "12345123451234512345","sum": "сумма операции по переводу денежных средств","currency": "валюта операции по переводу денежных средств","dateTimeAt": "2018-01-13T09:14:38Z"},"phoneNumber": {"number": "1212312345678","sum": "сумма операции","currency": "валюта операции","dateTimeAt": "2018-01-13T09:14:38Z"},"idNumber": {"number": "1KoX6AA5VTdbBTkw27YEqKFaTtEQq97AAT","sum": "сумма операции","currency": "валюта
1.1	"sourceId" (поле данных)	идентификатор, присвоенный участником информационного обмена, являющимся плательщиком	128-битный идентификатор (GUID), сформированный в соответствии со спецификацией RFC 4122 [16], присвоенный участником информационного обмена	
1.2	"victim" (поле данных)	информация о субъектном статусе плательщика	Выбирается один код из ограниченного множества возможных значений: - [person] - физическое лицо; - [entity] - юридическое лицо	
1.2	"payer" (блок данных)	информация, определяющая плательщика		
1.2.1	"bik" (поле данных)	БИК оператора по переводу денежных средств, обслуживающего плательщика	в формате AAAAAAAAA	

1.2.2	"inn" (поле данных)	ИНН плательщика - юридического лица, и (или) индивидуального предпринимателя, и (или) лица, занимающегося частной практикой	в формате XXXXXXXXXX - для юридических лиц, в формате XXXXXXXXXX или XXXXXXXXXXXX - для индивидуальных предпринимателей и (или) физических лиц, занимающихся в установленном законодательством Российской Федерации порядке частной практикой	операции","dateTimeAt": "2018-01-13T09:14:38Z"}},"device": {"ip": "127.0.0.1","imsi": "международный идентификатор мобильного абонента (индивидуальный номер абонента)","imei": "международный идентификатор мобильного оборудования","aiic": "Acquiring institution identification code (32 поле ISO 8583)",
1.2.3	"payerName" (поле данных)	наименование организации, являющейся плательщиком	текстовое поле (textarea)	
1.2.4	"payerTransferId" (подблок данных)	идентификационные данные в зависимости от способа реализации перевода денежных средств		
	"transferType" (поле данных)	тип способа реализации перевода денежных средств	Выбирается один код из ограниченного множества возможных значений: - [paymentCard] - при осуществлении операций по переводу денежных средств с использованием платежных карт; - [settlement] - при осуществлении переводов денежных средств по банковским счетам; - [phoneNumber] - при осуществлении переводов денежных средств по абонентскому номеру телефона; - [idNumber] - при изменении остатка электронных денежных средств	"cati": "Card acceptor terminal identification (41 поле ISO 8583)","caic": "Card acceptor identification code (42 поле ISO 8583)"}},"payee": {"bik": "123456789","inn": "123456789000","payeeName": "наименование организации, являющейся получателем средств","payeeTransferId": {"transferType": "тип способа реализации перевода денежных средств","paymentCard": {"number": "1234123412341234123412"},"settlement": {"number": "12345123451234512345"},"phoneNumber": {"number": "1212312345678"},"idNumber": {"number": "1KoX6AA5VTdbBTkw27YEqKFaTtEQq97AAT"}}}}]}
1.2.4.1	"paymentCard" (подблок данных)	при осуществлении операций по переводу денежных средств с использованием платежных карт		
1.2.4.1.1	"number" (поле данных)	номер платежной карты плательщика, выданной ему и (или) лицу, уполномоченному плательщиком, оператором по переводу денежных средств - эмитентом	в формате XXXXXXXXXXXXXXXXXX номер платежной карты представляется без пробелов (_) и знаков разделения (-).	
1.2.4.1.2	"sum" (поле данных)	сумма операции по осуществлению перевода денежных средств с использованием платежных карт	сумма операции - поле "F004" стандарта финансовых сообщений ISO 8583 [7], [8], [9]	
1.2.4.1.3	"currency" (поле данных)	валюта операции по осуществлению перевода денежных средств	валюта операции - поле "F049" стандарта финансовых сообщений ISO 8583 [7], [8], [9]	
1.2.4.1.4	"dateTimeAt" (поле данных)	дата и время операции	формат представления данных в соответствии со спецификацией RFC 3339 [11]	

1.2.4.1.5	"rrn" (поле данных)	номер, генерируемый для операции по переводу денежных средств при выполнении ее авторизации	номер, генерируемый для операции по переводу денежных средств при выполнении ее авторизации - поле " F 0 3 7 " стандарта финансовых сообщений ISO 8583 [7], [8], [9] Значение поля "F037" (Retrieval Reference Number) должно формироваться хостом банка-эквайрера по следующему правилу: YJJJXXNNNNNN, где: Y - последняя цифра года; JJJ - юлианская дата; XX - идентификатор, присвоенный хосту банка-эквайрера оператором; NNNNNN - последовательный номер транзакции в течение дня	
1.2.4.2	"settlement" (подблок данных)	при осуществлении переводов денежных средств по банковским счетам посредством списания денежных средств с банковских счетов плательщиков		
1.2.4.2.1	"number" (поле данных)	номер банковского счета плательщика, открытого у оператора по переводу денежных средств, обслуживающего плательщика	в формате XXXXXXXXXXXXXXXXXXXX номер банковского счета представляется без пробелов (_) и знаков разделения (-).	
1.2.4.2.2	"sum" (поле данных)	сумма операции по переводу денежных средств	текстовое поле (textarea)	
1.2.4.2.3	"currency" (поле данных)	валюта операции по переводу денежных средств	текстовое поле (textarea)	
1.2.4.2.4	"dateTimeAt" (поле данных)	дата и время операции	формат представления данных в соответствии со спецификацией RFC 3339 [11]	
1.2.4.3	"phoneNumber" (подблок данных)	при осуществлении переводов денежных средств по абонентскому номеру телефона		
1.2.4.3.1	"number" (поле данных)	номер телефона плательщика, указанный в договоре банковского счета и (или) договоре об использовании электронного средства платежа, заключенном с плательщиком	в формате KKKXXXNNNNNNNN, где: KKK - от одного до трех символов кода страны; XXX - код оператора; NNNNNNN - 7 знаков номера. Номер телефона представляется без знака плюс (+), пробелов (_) и знаков разделения (-).	
1.2.4.3.2	"sum" (поле данных)	сумма операции	текстовое поле (textarea)	
1.2.4.3.3	"currency" (поле данных)	валюта операции	текстовое поле (textarea)	
1.2.4.3.4	"dateTimeAt" (поле данных)	дата и время операции	формат представления данных в соответствии со спецификацией RFC 3339 [11]	
1.2.4.4	"idNumber" (подблок данных)	при изменении остатка электронных денежных средств		

1.2.4.4.1	"number" (поле данных)	идентификационный номер плательщика, в частности номер электронного кошелька плательщика, используемого им на основании договора банковского счета и (или) договора об использовании электронного средства платежа, заключенного с оператором по переводу денежных средств	текстовое поле (textarea)	
1.2.4.4.2	"sum" (поле данных)	сумма операции	текстовое поле (textarea)	
1.2.4.4.3	"currency" (поле данных)	валюта операции	текстовое поле (textarea)	
1.2.4.4.4	"dateTimeAt" (поле данных)	дата и время операции	формат представления данных в соответствии со спецификацией RFC 3339 [11]	
1.2.5	"device" (подблок данных)	параметры устройства, с использованием которого осуществлен доступ к автоматизированной системе, программному обеспечению с целью осуществления перевода денежных средств без согласия клиента		
1.2.5.1	"ip" (поле данных)	сетевой адрес компьютера и (или) коммуникационного устройства (маршрутизатора) (IP)	Сетевой адрес IPv4 должен соответствовать спецификации RFC 791 [12]	
1.2.5.2	"imsi" (поле данных)	International Mobile Subscriber Identity (IMSI) - международный идентификатор мобильного абонента (индивидуальный номер абонента (клиента - физического лица), по которому система распознает пользователя мобильной связи, использующего стандарты GSM и UMTS	число (15-разрядное в десятичном представлении) AA-BBBBBB-CCCCCC-EE	
1.2.5.3	"imei" (поле данных)	International Mobile Equipment Identity (IMEI) - международный идентификатор мобильного оборудования (мобильного устройства клиента - физического лица)	число (15-разрядное в десятичном представлении) AA-BBBBBB-CCCCCC-EE	

1.2.5.4	"aiic" (поле данных)	идентификатор участника, являющегося банком-эквайрером при осуществлении операций по переводу денежных средств с использованием платежных карт	идентификатор участника, являющегося банком-эквайрером при осуществлении операций по переводу денежных средств с использованием платежных карт (Acquiring institution identification code) - поле "F032" стандарта финансовых сообщений ISO 8583 [7], [8], [9]	
1.2.5.5	"cati" (поле данных)	идентификатор банкомата и (или) электронного терминала, на котором осуществляется операция по переводу и (или) снятию денежных средств	идентификатор банкомата и (или) электронного терминала, на котором осуществляется операция по переводу и (или) снятию денежных средств (Card acceptor terminal identification), - поле "F041" стандарта финансовых сообщений ISO 8583 [7], [8], [9]	
			Значение идентификатора терминала должно быть выровнено влево и дополнено пробелами справа до 8 символов	
1.2.5.6	"caic" (поле данных)	идентификатор банкомата и (или) электронного терминала, на котором осуществляется операция по переводу и (или) снятию денежных средств, по его географическому местоположению	идентификатор банкомата и (или) электронного терминала, на котором осуществляется операция по переводу и (или) снятию денежных средств, по его географическому местоположению (Card acceptor identification code) - поле "F042" стандарта финансовых сообщений ISO 8583 [7], [8], [9]	
			Значение идентификатора пункта обслуживания должно быть выровнено влево и дополнено пробелами справа до 15 символов	
1.3	"payee" (блок данных)	информация, определяющая получателя средств		
1.3.1	"bik" (поле данных)	БИК оператора по переводу денежных средств, обслуживающего получателя средств	в формате AAAAAAAAA	
1.3.2	"inn" (поле данных)	ИНН получателя средств - юридического лица, и (или) индивидуального предпринимателя, и (или) лица, занимающегося частной практикой	в формате XXXXXXXXXX - для юридических лиц, в формате XXXXXXXXXX или XXXXXXXXXXXX - для индивидуальных предпринимателей и (или) физических лиц, занимающихся в установленном законодательством Российской Федерации порядке частной практикой	
1.3.3	"namePayee" (поле данных)	наименование организации, являющейся получателем средств	текстовое поле (textarea)	
1.3.4	"payeeTransferId" (подблок данных)	идентификационные данные в зависимости от способа реализации перевода денежных средств		

	"transferType" (поле данных)	тип способа реализации перевода денежных средств	Выбирается один код из ограниченного множества возможных значений: - [paymentCard] - при осуществлении операций по переводу денежных средств с использованием платежных карт; - [settlement] - при осуществлении переводов денежных средств по банковским счетам; - [phoneNumber] - при осуществлении переводов денежных средств по абонентскому номеру телефона; - [idNumber] - при изменении остатка электронных денежных средств	
1.3.4.1	"paymentCard" (подблок данных)	при осуществлении операций по переводу денежных средств с использованием платежных карт		
1.3.4.1.1	"number" (поле данных)	номер платежной карты получателя средств, выданной ему и (или) лицу, уполномоченному получателем средств, оператором по переводу денежных средств - эмитентом	в формате XXXXXXXXXXXXXXXXX номер платежной карты представляется без пробелов (_) и знаков разделения (-).	
1.3.4.2	"settlement" (подблок данных)	при осуществлении переводов денежных средств по банковским счетам посредством списания денежных средств с банковских счетов плательщиков		
1.3.4.2.1	"number" (поле данных)	номер расчетного счета получателя средств, открытого у оператора по переводу денежных средств, обслуживающего получателя средств	в формате XXXXXXXXXXXXXXXXXXXX номер банковского счета представляется без пробелов (_) и знаков разделения (-).	
1.3.4.3	"phoneNumber" (подблок данных)	при осуществлении переводов денежных средств по абонентскому номеру телефона		
1.3.4.3.1	"number" (поле данных)	номер телефона получателя средств	в формате KKKXXXNNNNNNN, где: KKK - от одного до трех символов кода страны; XXX - код оператора; NNNNNNN - 7 знаков номера. Номер телефона представляется без знака плюс (+), пробелов (_) и знаков разделения (-).	
1.3.4.4	"idNumber" (подблок данных)	при изменении остатка электронных денежных средств		

1.3.4.4.1	"number" (поле данных)	идентификационный номер получателя средств, в частности номер электронного кошелька получателя средств, используемого им на основании договора банковского счета и (или) договора об использовании электронного средства платежа, заключенного с оператором по переводу денежных средств	текстовое поле (textarea)	

8. Форма представления данных, используемая участниками информационного обмена для представления ответа на запрос Банка России к участнику информационного обмена, обслуживающему получателя средств, и сроки их представления в Банк России

Информация в ответ на запрос Банка России в части проверки конкретного получателя средств, указанный в главе 7 настоящего стандарта, направляется в Банк России в максимально короткий срок, но не позднее дня, следующего за днем получения участником информационного обмена, обслуживающим получателя средств, соответствующего запроса Банка России.

Информация в ответ на запрос Банка России в части приостановления (невозможности приостановления) зачисления денежных средств на банковский счет получателя средств или увеличения остатка электронных денежных средств получателя средств, указанный в главе 7 настоящего стандарта, направляется незамедлительно после получения соответствующего запроса Банка России.

8.1. Идентификационные данные ответа на запрос Банка России. Блок данных [HEADER]

Номер блока (поля) данных	Идентификатор блока (поля) данных	Содержание блока (поля) данных	Формат поля данных	Формат электронного сообщения	Обязательность информирования
1.1	"schemaType" (поле данных)	тип электронного сообщения	Указывается значение [anifraudResponse] - ответ "получателя средств" несанкционированной операции Банку России	{"header": {"schemaType": "anifraudResponse","schemaVersion": "1","version": "1","memberId": "9527dd0c-0765-4f1c-8f5f-70a02cf4046c","sourceId": "f34030ef-358a-445c-8567-25985ce6d91c","publishedAt": "2002-10-02T15:00:00.05Z"},	[O]
1.2	"schemaVersion" (поле данных)	версия схемы типа электронного сообщения	текстовое поле (textarea)		[O]
1.3	"version" (поле данных)	номер версии электронного сообщения в процессе информационного обмена	числовое значение (int)		[O]
1.4	"memberId" (поле данных)	идентификатор участника информационного обмена, присвоенный Банком России	128-битный идентификатор (GUID), сформированный в соответствии со спецификацией RFC 4122 [16], присвоенный Банком России		[O]
1.5	"sourceId" (поле данных)	идентификатор, присвоенный участником информационного обмена	128-битный идентификатор (GUID), сформированный в соответствии со спецификацией RFC 4122 [16], присвоенный участником информационного обмена		[N]
1.6	"publishedAt" (поле данных)	дата и время представления ответа на запрос Банка России	формат представления данных в соответствии со спецификацией RFC 3339 [11]		[O]

8.2. Описание формы ответа на запрос Банка России. Блок данных [anifraudResponse]

Форма представления данных, используемая участниками информационного обмена для представления ответа на запрос Банка России к участнику информационного обмена, обслуживающему получателя средств, применяется:

при информировании Банка России оператором по переводу денежных средств, обслуживающим получателя средств, включая оператора электронных денежных средств, о конкретном получателе средств [4];

при направлении уведомления об успешном приостановлении зачисления денежных средств на банковский счет получателя средств или увеличении остатка электронных денежных средств получателя средств [20];

при направлении уведомления о невозможности приостановления зачисления денежных средств на банковский счет получателя средств или увеличения остатка электронных денежных средств получателя средств [20].

Номер блока (поля) данных	Идентификатор блока (поля) данных	Содержание блока (поля) данных	Формат поля данных	Формат электронного со
1	"anifraudResponse" (блок данных)		В случае необходимости указания нескольких значений блоков данных (payer, payee, additionalStatus) указывается один или несколько объектов в блоке данных "antifraud"	"anifraudResponse": [{"sourceId": "f34030ef-358a-445c- "информация о субъектном статусе плательщика","re статусе получателя средств","payeeIdentifier": {"hash "P79969612A71BAB224C7CB534FD7A0D3C1C78AD406 "B49087832A71BAB224C7CB534FD7A0D3C1C78AD406 {"bik": "123456789","inn": "123456789000","payerNam являющейся плательщиком","payerTransferId": {"trans перевода денежных средств","paymentCard": {"numb "сумма операции по осуществлению перевода денеж платежных карт","currency": "валюта операции по ос средств","dateTimeAt": "2018-01-13T09:14:38Z","rrn": по переводу денежных средств при выполнении ее а "12345123451234512345","sum": "сумма операции по средств","currency": "валюта операции по переводу д "2018-01-13T09:14:38Z"},"phoneNumber": {"number": операции","currency": "валюта операции","dateTimeAt 13T09:14:38Z"},"idNumber": {"number": "1KoX6AA5VTc "сумма операции","currency": "валюта операции",
1.2	"sourceId" (поле данных)	идентификатор, присвоенный участником информационного обмена, являющимся плательщиком	128-битный идентификатор (GUID), сформированный в соответствии со спецификацией RFC 4122 [16], присвоенный участником информационного обмена	
1.3	"victim" (поле данных)	информация о субъектном статусе плательщика	Выбирается один код из ограниченного множества возможных значений: - [person] - физическое лицо; - [entity] - юридическое лицо	
1.4	"recipient" (поле данных)	информация о субъектном статусе получателя средств	Выбирается один код из ограниченного множества возможных значений: - [person] - физическое лицо; - [entity] - юридическое лицо	
1.5	"payeeIdentifier" (блок данных)	идентификационные данные, определяющие конкретного получателя средств		
1.5.1	"hash" (поле данных)	информация о результате вычисления функции хэширования номера документа, удостоверяющего личность, в целях идентификации обратившегося (обратившихся) лица (лиц), уполномоченного (уполномоченных) распоряжаться денежными средствами получателя (получателей) средств	Последовательность символов, полученных в результате вычисления хэш-функции SHA-256 от серии и номера документа удостоверяющего личность. Серия и номер документа удостоверяющего личность представляется для вычисления хэш-функции: без пробелов (_), знака номера (N), букв (при их наличии) в верхнем регистре (ABC). Для российского паспорта это XXXXYYYYYY, где: XXXX - четырехзначная серия паспорта; YYYYYY - шестизначный номер паспорта. Кодировка исходного текста (до хэширования) - Windows-1251; Кодировка текста хэша - Windows-1251.	

1.5.2	"hashSnils" (поле данных)	информация о результате вычисления функции хэширования СНИЛС получателя (получателей) средств - лица (лиц), уполномоченного (уполномоченных) распоряжаться денежными средствами получателя (получателей) средств	Последовательность символов, полученных в результате вычисления хэш-функции SHA-256 от СНИЛС плательщика. СНИЛС представляется для вычисления хэш-функции: без пробелов (_) и знаков разделения (-). СНИЛС вида: XXXXXXXXXXX Кодировка исходного текста (до хэширования) - Windows-1251; Кодировка текста хэша - Windows-1251.	"dateTimeAt": "2018-01-13T09:14:38Z"}},"device": {"ip идентификатор мобильного абонента (индивидуальн "международный идентификатор мобильного оборуд identification code (32 поле ISO 8583)","cati": "Card acc ISO 8583)","caic": "Card acceptor identification code (42 "123456789","inn": "123456789000","payeeName": "на являющейся получателем средств","payeeTransferId" реализации перевода денежных средств","paymentC "123412341234123412","sum": "сумма операции по о средств с использованием платежных карт","currenc осуществлению перевода денежных средств с испол {"enrollment": "идентификатор приостановления опе 02T15:00:00.05Z"}},"settlement": {"number": "1234512 операции по осуществлению перевода денежных сре по осуществлению перевода денежных средств","sta приостановления операции","dateTimeAt": "2002-10-0 {"number": "1212312345678","sum": "сумма операции операции","status1": {"enrollment": "идентификатор п операции","dateTimeAt": "2002-10-02T15:00:00.05Z"}
1.6	"payer" (блок данных)	информация, определяющая плательщика		
1.6.1	"bik" (поле данных)	БИК оператора по переводу денежных средств, обслуживающего плательщика	в формате AAAAAAAAA	
1.6.2	"inn" (поле данных)	ИНН плательщика - юридического лица, и (или) индивидуального предпринимателя, и (или) лица, занимающегося частной практикой	в формате XXXXXXXXXX - для юридических лиц, в формате XXXXXXXXXX или XXXXXXXXXXXX - для индивидуальных предпринимателей и (или) физических лиц, занимающихся в установленном законодательством Российской Федерации порядке частной практикой.	
1.6.3	"payerName" (поле данных)	наименование организации, являющейся плательщиком	текстовое поле (textarea)	
1.6.4	"payerTransferId" (подблок данных)	идентификационные данные в зависимости от способа реализации перевода денежных средств		
1.6.4.1	"transferType" (поле данных)	тип способа реализации перевода денежных средств	Выбирается один код из ограниченного множества возможных значений: - [paymentCard] - при осуществлении операций по переводу денежных средств с использованием платежных карт; - [settlement] - при осуществлении переводов денежных средств по банковским счетам; - [phoneNumber] - при осуществлении переводов денежных средств по абонентскому номеру телефона; - [idNumber] - при изменении остатка электронных денежных средств	
1.6.4.2	"paymentCard" (подблок данных)	при осуществлении операций по переводу денежных средств с использованием платежных карт		

1.6.4.2.1	"number" (поле данных)	номер платежной карты плательщика, выданной ему и (или) лицу, уполномоченному плательщиком, оператором по переводу денежных средств - эмитентом	в формате XXXXXXXXXXXXXXXXXX номер платежной карты представляется без пробелов (_) и знаков разделения (-).	
1.6.4.2.2	"sum" (поле данных)	сумма операции по осуществлению перевода денежных средств с использованием платежных карт	сумма операции - поле "F004" стандарта финансовых сообщений ISO 8583 [7], [8], [9]	
1.6.4.2.3	"currency" (поле данных)	валюта операции по осуществлению перевода денежных средств	валюта операции - поле "F049" стандарта финансовых сообщений ISO 8583 [7], [8], [9]	
1.6.4.2.4	"dateTimeAt" (поле данных)	дата и время операции	формат представления данных в соответствии со спецификацией RFC 3339 [11]	},"idNumber": {"number": "1KoX6AA5VTdbBTkw27YEqK операции по изменению остатка денежных средств", изменению остатка денежных средств","status1": {"e приостановления операции","dateTimeAt": "2002-10-0
1.6.4.2.5	"rrn" (поле данных)	номер, генерируемый для операции по переводу денежных средств при выполнении ее авторизации	номер, генерируемый для операции по переводу денежных средств при выполнении ее авторизации - поле "F037" стандарта финансовых сообщений ISO 8583 [7], [8], [9] Значение поля "F037" (Retrieval Reference Number) должно формироваться хостом банка-эквайрера по следующему правилу: YJJJXXNNNNNN, где: Y - последняя цифра года; JJJ - юлианская дата; XX - идентификатор, присвоенный хосту банка-эквайрера оператором; NNNNNN - последовательный номер транзакции в течение дня	
1.6.4.3	"settlement" (подблок данных)	при осуществлении переводов денежных средств по банковским счетам посредством списания денежных средств с банковских счетов плательщиков		
1.6.4.3.1	"number" (поле данных)	номер банковского счета плательщика, открытого у оператора по переводу денежных средств, обслуживающего плательщика	в формате XXXXXXXXXXXX XXXXXXXX номер банковского счета представляется без пробелов (_) и знаков разделения (-).	
1.6.4.3.2	"sum" (поле данных)	сумма операции по переводу денежных средств	текстовое поле (textarea)	
1.6.4.3.3	"currency" (поле данных)	валюта операции по переводу денежных средств	текстовое поле (textarea)	
1.6.4.3.4	"dateTimeAt" (поле данных)	дата и время операции	формат представления данных в соответствии со спецификацией RFC 3339 [11]	
1.6.4.4	"phoneNumber" (подблок данных)	при осуществлении переводов денежных средств по абонентскому номеру телефона		

1.6.4.4.1	"number" (поле данных)	номер телефона плательщика, указанный в договоре банковского счета и (или) договоре об использовании электронного средства платежа, заключенном с плательщиком	в формате KKKXXXNNNNNNNN, где: KKK - от одного до трех символов кода страны; XXX - код оператора; NNNNNNN - 7 знаков номера. Номер телефона представляется без знака плюс (+), пробелов (_) и знаков разделения (-).
1.6.4.4.2	"sum" (поле данных)	сумма операции	текстовое поле (textarea)
1.6.4.4.3	"currency" (поле данных)	валюта операции	текстовое поле (textarea)
1.6.4.4.4	"dateTimeAt" (поле данных)	дата и время операции	формат представления данных в соответствии со спецификацией RFC 3339 [11]
1.6.4.5	"idNumber" (подблок данных)	при изменении остатка электронных денежных средств	
1.6.4.5.1	"number" (поле данных)	идентификационный номер плательщика, в частности номер электронного кошелька плательщика, используемого им на основании договора банковского счета и (или) договора об использовании электронного средства платежа, заключенного с оператором по переводу денежных средств	текстовое поле (textarea)
1.6.4.5.2	"sum" (поле данных)	сумма операции	текстовое поле (textarea)
1.6.4.5.3	"currency" (поле данных)	валюта операции	текстовое поле (textarea)
1.6.4.5.4	"dateTimeAt" (поле данных)	дата и время операции	формат представления данных в соответствии со спецификацией RFC 3339 [11]
1.6.5	"device" (подблок данных)	параметры устройства, с использованием которого осуществлен доступ к автоматизированной системе, программному обеспечению с целью осуществления перевода денежных средств без согласия клиента	
1.6.5.1	"ip" (поле данных)	сетевой адрес компьютера и (или) коммуникационного устройства (маршрутизатора) (IP)	Сетевой адрес IPv4 должен соответствовать спецификации RFC 791 [12]

1.6.5.2	"imsi" (поле данных)	International Mobile Subscriber Identity (IMSI) - международный идентификатор мобильного абонента (индивидуальный номер абонента (клиента - физического лица), по которому система распознает пользователя мобильной связи, использующего стандарты GSM и UMTS	число (15-разрядное в десятичном представлении) AA-BBBBBB-CCCCCC-EE	
1.6.5.3	"imei" (поле данных)	International Mobile Equipment Identity (IMEI) - международный идентификатор мобильного оборудования (мобильного устройства клиента - физического лица)	число (15-разрядное в десятичном представлении) AA-BBBBBB-CCCCCC-EE	
1.6.5.4	"aiic" (поле данных)	идентификатор участника, являющегося банком-эквайрером при осуществлении операций по переводу денежных средств с использованием платежных карт	идентификатор участника, являющегося банком-эквайрером при осуществлении операций по переводу денежных средств с использованием платежных карт (Acquiring institution identification code), - поле "F032" стандарта финансовых сообщений ISO 8583 [7], [8], [9]	
1.6.5.5	"cati" (поле данных)	идентификатор банкомата и (или) электронного терминала, на котором осуществляется операция по переводу и (или) снятию денежных средств	идентификатор банкомата и (или) электронного терминала, на котором осуществляется операция по переводу и (или) снятию денежных средств (Card acceptor terminal identification), - поле "F041" стандарта финансовых сообщений ISO 8583 [7], [8], [9] Значение идентификатора терминала должно быть выровнено влево и дополнено пробелами справа до 8 символов	
1.6.5.6	"caic" (поле данных)	идентификатор банкомата и (или) электронного терминала, на котором осуществляется операция по переводу и (или) снятию денежных средств, по его географическому местоположению	идентификатор банкомата и (или) электронного терминала, на котором осуществляется операция по переводу и (или) снятию денежных средств, по его географическому местоположению (Card acceptor identification code) - поле "F042" стандарта финансовых сообщений ISO 8583 [7], [8], [9] Значение идентификатора пункта обслуживания должно быть выровнено влево и дополнено пробелами справа до 15 символов	
1.7	"payee" (блок данных)	информация, определяющая получателя средств		

1.7.1	"bik" (поле данных)	БИК оператора по переводу денежных средств, обслуживающего получателя средств	в формате AAAAAAAAA
1.7.2	"inn" (поле данных)	ИНН получателя средств - юридического лица, и (или) индивидуального предпринимателя, и (или) лица, занимающегося частной практикой	в формате XXXXXXXXXX - для юридических лиц, в формате XXXXXXXXXX или XXXXXXXXXXXX - для индивидуальных предпринимателей и (или) физических лиц, занимающихся в установленном законодательством Российской Федерации порядке частной практикой
1.7.3	"payeeName" (поле данных)	наименование организации, являющейся получателем средств	текстовое поле (textarea)
1.7.4	"payeeTransferId" (подблок данных)	идентификационные данные в зависимости от способа реализации перевода денежных средств	
1.7.4.1	"transferType" (поле данных)	тип способа реализации перевода денежных средств	Выбирается один код из ограниченного множества возможных значений: - [paymentCard] - при осуществлении операций по переводу денежных средств с использованием платежных карт; - [settlement] - при осуществлении переводов денежных средств по банковским счетам; - [phoneNumber] - при осуществлении переводов денежных средств по абонентскому номеру телефона; - [idNumber] - при изменении остатка электронных денежных средств
1.7.4.2	"paymentCard" (подблок данных)	при осуществлении операций по переводу денежных средств с использованием платежных карт	
1.7.4.2.1	"number" (поле данных)	номер платежной карты получателя средств, выданной ему и (или) лицу, уполномоченному получателем средств, оператором по переводу денежных средств - эмитентом	в формате XXXXXXXXXXXXXXXXXX номер платежной карты представляется без пробелов (_) и знаков разделения (-).
1.7.4.2.2	"sum" (поле данных)	сумма операции по осуществлению перевода денежных средств с использованием платежных карт	сумма операции - поле "F004" стандарта финансовых сообщений ISO 8583 [7], [8], [9]
1.7.4.2.3	"currency" (поле данных)	валюта операции по осуществлению перевода денежных средств	валюта операции - поле "F049" стандарта финансовых сообщений ISO 8583 [7], [8], [9]
1.7.4.2.4	"status1" (подблок данных)	статус приостановления операции	

1.7.4.2.4.1	"enrollment" (поле данных)	идентификатор приостановления операции	Выбирается один код из ограниченного множества возможных значений: - [successful] - успешное приостановление зачисления денежных средств на банковский счет получателя средств или увеличения остатка электронных денежных средств получателя средств; - [unsuccessful] - невозможность приостановления зачисления денежных средств на банковский счет получателя средств или приостановления увеличения остатка электронных денежных средств получателя средств
1.7.4.2.4.2	"dateTimeAt" (поле данных)	дата и время приостановления (невозможности приостановления) зачисления денежных средств на банковский счет получателя средств или приостановления (невозможности приостановления) увеличения остатка электронных денежных средств получателя средств	формат представления данных в соответствии со спецификацией RFC 3339 [11]
1.7.4.3	"settlement" (подблок данных)	при осуществлении переводов денежных средств по банковским счетам посредством списания денежных средств с банковских счетов плательщиков	
1.7.4.3.1	"number" (поле данных)	номер расчетного счета получателя средств, открытого у оператора по переводу денежных средств, обслуживающего получателя средств	в формате XXXXXXXXXXXXXXXXXXXX номер банковского счета представляется без пробелов (_) и знаков разделения (-).
1.7.4.3.2	"sum" (поле данных)	сумма операции по переводу денежных средств	текстовое поле (textarea)
1.7.4.3.3	"currency" (поле данных)	валюта операции по переводу денежных средств	текстовое поле (textarea)
1.7.4.3.4	"status1" (подблок данных)	статус приостановления операции	

1.7.4.3.4.1	"enrollment" (поле данных)	идентификатор приостановления операции	Выбирается один код из ограниченного множества возможных значений: - [successful] - успешное приостановление зачисления денежных средств на банковский счет получателя средств или увеличения остатка электронных денежных средств получателя средств; - [unsuccessful] - невозможность приостановления зачисления денежных средств на банковский счет получателя средств или приостановления увеличения остатка электронных денежных средств получателя средств
1.7.4.3.4.2	"dateTimeAt" (поле данных)	дата и время приостановления (невозможности приостановления) зачисления денежных средств на банковский счет получателя средств или приостановления (невозможности приостановления) увеличения остатка электронных денежных средств получателя средств	формат представления данных в соответствии со спецификацией RFC 3339 [11]
1.7.4.4	"phoneNumber" (подблок данных)	при осуществлении переводов денежных средств по абонентскому номеру телефона	
1.7.4.4.1	"number" (поле данных)	номер телефона получателя средств	в формате KKKXXXNNNNNNNN, где: KKK - от одного до трех символов кода страны; XXX - код оператора; NNNNNNN - 7 знаков номера. Номер телефона представляется без знака плюс (+), пробелов (_) и знаков разделения (-).
1.7.4.4.2	"sum" (поле данных)	"sum" (поле данных)	сумма операции
1.7.4.4.3	"currency" (поле данных)	"currency" (поле данных)	валюта операции
1.7.4.4.4	"status1" (подблок данных)	статус приостановления операции	

1.7.4.4.4.1	"enrollment" (поле данных)	идентификатор приостановления операции	Выбирается один код из ограниченного множества возможных значений: - [successful] - успешное приостановление зачисления денежных средств на банковский счет получателя средств или увеличения остатка электронных денежных средств получателя средств; - [unsuccessful] - невозможность приостановления зачисления денежных средств на банковский счет получателя средств или приостановления увеличения остатка электронных денежных средств получателя средств
1.7.4.4.4.2	"dateTimeAt" (поле данных)	дата и время приостановления (невозможности приостановления) зачисления денежных средств на банковский счет получателя средств или приостановления (невозможности приостановления) увеличения остатка электронных денежных средств получателя средств	формат представления данных в соответствии со спецификацией RFC 3339 [11]
1.7.4.5	"idNumber" (подблок данных)	при изменении остатка электронных денежных средств	
1.7.4.5.1	"number" (поле данных)	идентификационный номер получателя средств, в частности номер электронного кошелька получателя средств, используемого им на основании договора банковского счета и (или) договора об использовании электронного средства платежа, заключенного с оператором по переводу денежных средств	текстовое поле (textarea)
1.7.4.5.2	"sum" (поле данных)	сумма операции	текстовое поле (textarea)
1.7.4.5.3	"currency" (поле данных)	валюта операции	текстовое поле (textarea)
1.7.4.5.4	"status1" (подблок данных)	статус приостановления операции	

1.7.4.5.4.1	"enrollment" (поле данных)	идентификатор приостановления операции	Выбирается один код из ограниченного множества возможных значений: - [successful] - успешное приостановление зачисления денежных средств на банковский счет получателя средств или увеличения остатка электронных денежных средств получателя средств; - [unsuccessful] - невозможность приостановления зачисления денежных средств на банковский счет получателя средств или приостановления увеличения остатка электронных денежных средств получателя средств
1.7.4.5.4.2	"dateTimeAt" (поле данных)	дата и время приостановления (невозможности приостановления) зачисления денежных средств на банковский счет получателя средств или приостановления (невозможности приостановления) увеличения остатка электронных денежных средств получателя средств	формат представления данных в соответствии со спецификацией RFC 3339 [11]

9. Форма информационного сообщения Банка России к участнику информационного обмена, обслуживающему плательщика

Форма информационного сообщения Банка России к участнику информационного обмена, обслуживающему плательщика, применяется:

при направлении уведомления об успешном приостановлении зачисления денежных средств на банковский счет получателя средств или увеличения остатка электронных денежных средств получателя средств [20];

при направлении уведомления о невозможности приостановления зачисления денежных средств на банковский счет получателя средств или увеличения остатка электронных денежных средств получателя средств [20];

9.1. Идентификационные данные информационного сообщения Банка России к участнику информационного обмена, обслуживающему плательщика. Блок данных [HEADER]

Номер блока (поля) данных	Идентификатор блока (поля) данных	Содержание блока (поля) данных	Формат поля данных	Формат электронного сообщения
1.1	"schemaType" (поле данных)	тип электронного сообщения	Указывается значение [antifraudReturn] - дополнительный запрос участнику информационного обмена - "получателю средств" несанкционированной операции	{"header": {"schemaType": "antifraudReturn","schemaVersion": "1","version": "1","memberId": "9527dd0c-0765-4f1c-8f5f-70a02cf4046c","publishedAt": "2002-10-02T15:00:00.05Z"},
1.2	"schemaVersion" (поле данных)	версия схемы типа электронного сообщения	текстовое поле (textarea)	
1.3	"version" (поле данных)	номер версии электронного сообщения в процессе информационного обмена	числовое значение (int)	
1.4	"memberId" (поле данных)	идентификатор участника информационного обмена, присвоенный Банком России	128-битный идентификатор (GUID), сформированный в соответствии со спецификацией RFC 4122 [16], присвоенный Банком России	
1.5	"publishedAt" (поле данных)	дата и время первичного информирования	формат представления данных в соответствии со спецификацией RFC 3339 [11]	

10. Форма представления в Банк России запроса от участников информационного обмена, использующих сервис срочного перевода и сервис несрочного перевода для осуществления перевода денежных средств, не являющихся подразделениями Банка России, об установлении (или снятии) на их банковские (корреспондентские) счета (субсчета) ограничения в виде запрета на списание денежных средств при выявлении инцидентов, связанных с нарушением требований к обеспечению защиты информации при осуществлении переводов денежных средств, на объектах информационной инфраструктуры участников информационного обмена

Условия обязательности информирования:

[O] - информация блока (поля) данных представляется в обязательном порядке;

[N] - информация блока (поля) данных представляется в случае наличия технической возможности.

Временные характеристики информирования:

Информация об установлении на банковские (корреспондентские) счета (субсчета) ограничения в виде запрета на списание денежных средств при выявленных инцидентах, связанных с нарушением требований к обеспечению защиты информации при осуществлении переводов денежных средств, на объектах информационной инфраструктуры участников информационного обмена, направляется незамедлительно при выявлении соответствующего инцидента.

Форма представления данных, используемая участниками информационного обмена для направления запроса в Банк России об установлении на их банковские (корреспондентские) счета (субсчета) ограничения в виде запрета на списание денежных средств при выявлении инцидентов, связанных с нарушением требований к обеспечению защиты информации, применяется:

при информировании Банка России участниками информационного обмена, использующими сервис срочного перевода и сервис несрочного перевода для осуществления перевода денежных средств, не являющимися подразделениями Банка России, об установлении на их банковские (корреспондентские) счета (субсчета) ограничения в виде запрета на списание денежных средств при выявлении инцидентов, связанных с нарушением требований к обеспечению защиты информации при осуществлении переводов денежных средств, на объектах информационной инфраструктуры участников обмена [21];

при информировании Банка России участниками информационного обмена, использующими сервис срочного перевода и сервис несрочного перевода для осуществления перевода денежных средств, не являющимися подразделениями Банка России, о снятии с их банковских (корреспондентских) счетов (субсчетов) ограничения в виде запрета на списание денежных средств при выявлении инцидентов, связанных с нарушением требований к обеспечению защиты информации при осуществлении переводов денежных средств, на объектах информационной инфраструктуры участников обмена [21].

10.1. Идентификационные данные запроса участников информационного обмена в Банк России об установлении (или снятии) на их банковские (корреспондентские) счета (субсчета) ограничения в виде запрета на списание денежных средств при выявлении инцидентов, связанных с нарушением требований к обеспечению защиты информации. Блок данных [HEADER]

Номер блока (поля) данных	Идентификатор блока (поля) данных	Содержание блока (поля) данных	Формат поля данных	Формат электронного сообщения	Обязательность информирования
1.1	"schemaType" (поле данных)	тип электронного сообщения	Указывается значение [lockRequest] - запрос участников информационного обмена об установлении или снятии ограничения на списание денежных средств с их банковских (корреспондентских) счетов (субсчетов)	{"header": {"schemaType": "lockRequest","schemaVersion": "1","version": "1","memberId": "9527dd0c-0765-4f1c-8f5f-70a02cf4046c","sourceId": "f34030ef-358a-445c-8567-25985ce6d91c","publishedAt": "2002-10-02T15:00:00.05Z"},	[O]
1.2	"schemaVersion" (поле данных)	версия схемы типа электронного сообщения	текстовое поле (textarea)		[O]
1.3	"version" (поле данных)	номер версии электронного сообщения в процессе информационного обмена	числовое значение (int)		[O]
1.4	"memberId" (поле данных)	идентификатор участника информационного обмена, присвоенный Банком России	128-битный идентификатор (GUID), сформированный в соответствии со спецификацией RFC 4122 [16], присвоенный Банком России		[O]
1.5	"sourceId" (поле данных)	идентификатор, присвоенный участником информационного обмена	128-битный идентификатор (GUID), сформированный в соответствии со спецификацией RFC 4122 [16], присвоенный участником информационного обмена		[N]
1.6	"publishedAt" (поле данных)	дата и время направления запроса в Банк России	формат представления данных в соответствии со спецификацией RFC 3339 [11]		[O]

10.2. Описание формы запроса участников информационного обмена в Банк России об установлении (или снятии) на их банковские (корреспондентские) счета (субсчета) ограничения в виде запрета на списание денежных средств при выявлении инцидентов, связанных с нарушением требований к обеспечению защиты информации. Блок данных [lockRequest]

Номер блока (поля) данных	Идентификатор блока (поля) данных	Содержание блока (поля) данных	Формат поля данных	Формат электронного сообщения	Обязательность информирования
2.1	"sourceId" (поле данных)	идентификатор, присвоенный участником информационного обмена	128-битный идентификатор (GUID), сформированный в соответствии со спецификацией RFC 4122 [16], присвоенный участником информационного обмена	"lockRequest": [{"sourceId": "f34030ef-358a-445c-8567-25985ce6d91c","orgBik": "123456789","regNumber": "123456789","uniqIdentifier": "1234567891","actionStatus": "статус ограничения на списание денежных средств","dateAt": "20180101","text": "дополнительное описание","persons": [{"lastName": "фамилия","firstName":	[O]
2.2	"orgBik" (поле данных)	БИК участника информационного обмена	в формате AAAAAAAAA		[O]
2.3	"regNumber" (поле данных)	регистрационный номер из книги государственной регистрации кредитных организаций	текстовое поле (textarea)		[O]
2.4.	"uniqIdentifier" (поле данных)	уникальный идентификатор составителя электронного сообщения (УИС) [22]	в формате XXXXXXXXXX		[O]

2.5	"actionStatus" (поле данных)	статус ограничения на списание денежных средств	Выбирается один код из ограниченного множества возможных значений: - [on] - обращение об установлении ограничения в виде запрета на списание денежных средств с банковских (корреспондентских) счетов (субсчетов); - [off] - обращение о снятии ограничения в виде запрета на списание денежных средств с банковских (корреспондентских) счетов (субсчетов)	{"lastName": "фамилия","firstName": "имя","middleName": "отчество","landlineNumber": "1212312345678","mobileNumber": "1212312345678","email": "qwerty1@example.ru","position": "должность"},"attachment": {"sourceId": "f34030ef-358a-445c-8567-25985ce6d91c","comment": "описание вложения","dateTimeAt": "2018-03-22T08:14:38Z","file": {"name": "имя файла","size": "размер файла в байтах","base64": "вложение в формате base64"}}}]}	[O]
2.6	"dateAt" (поле данных)	календарная дата, с которой необходимо приостановить обмен электронными сообщениями при переводе денежных средств в рамках платежной системы Банка России в связи с выявлением проблем в обеспечении защиты информации и осуществлением (подозрением на осуществление) несанкционированных переводов денежных средств	формат представления данных в соответствии со стандартом ISO 8601:2004 [23]		[O]
2.7	"text" (поле данных)	дополнительное описание	текстовое поле (textarea)		[N]
2.8	"person" (блок данных)	идентификаторы контактного лица, направившего запрос об установлении или снятии на банковские (корреспондентские) счета (субсчета) ограничения в виде запрета на списание денежных средств			[O]
2.8.1	"lastName" (поля данных)	фамилия	текстовое поле (textarea)		[O]
2.8.2	"firstName" (поля данных)	имя	текстовое поле (textarea)		[O]
2.8.3	"middleName" (поля данных)	отчество	текстовое поле (textarea)		[O]
2.8.4	"landlineNumber" (поля данных)	городской телефон	текстовое поле (textarea)		[O]
2.8.5	"mobileNumber" (поля данных)	мобильный телефон	текстовое поле (textarea)		[O]
2.8.6	"email" (поля данных)	электронный адрес	текстовое поле (textarea)		[O]
2.8.7	"position" (поля данных)	должность	текстовое поле (textarea)		[O]
2.9	"attachment" (блок данных)	дополнительные данные для подтверждения установления или снятия ограничения в виде запрета на списание денежных средств			[O]

2.9.1	"sourceId" (поле данных)	идентификатор, присвоенный участником информационного обмена	128-битный идентификатор (GUID), сформированный в соответствии со спецификацией RFC 4122 [16], присвоенный участником информационного обмена		[O]
2.9.2	"comment" (поле данных)	описание вложения	текстовое поле (textarea)		[O]
2.9.3	"dateTimeAt" (поле данных)	дата и время добавления файла	формат представления данных в соответствии со спецификацией RFC 3339 [11]		[O]
2.9.4	"file" (блок данных)	файл данных	Указывается наименование, размер файла (не более 5 Мб), выполняется кодировка в формате Base64		[O]

11. Форма информационного сообщения Банка России об установлении (или снятии) на банковские (корреспондентские) счета (субсчета) участников информационного обмена ограничения в виде запрета на списание денежных средств

Форма информационного сообщения Банка России об установлении (или снятии) на банковские (корреспондентские) счета (субсчета) участников обмена ограничения в виде запрета на списание денежных средств применяется:

при направлении уведомления участнику информационного обмена в случае положительного результата контроля целостности и принятия к исполнению запросов на установление или снятие ограничения в виде запрета на списание денежных средств [21];

при направлении уведомления участнику информационного обмена в случае отрицательного результата контроля целостности и непринятия к исполнению запросов на установление или снятие ограничения в виде запрета на списание денежных средств [21].

11.1. Идентификационные данные информационного сообщения Банка России об установлении (или снятии) на банковские (корреспондентские) счета (субсчета) участников информационного обмена ограничения в виде запрета на списание денежных средств. Блок данных [HEADER]

Номер блока (поля) данных	Идентификатор блока (поля) данных	Содержание блока (поля) данных	Формат поля данных	Формат электронного сообщения
1.1	"schemaType" (поле данных)	тип электронного сообщения	Указывается значение [lockResponse] - информационное сообщение Банка России об установлении (или снятии) на банковские (корреспондентские) счета (субсчета) участников информационного обмена ограничения в виде запрета на списание денежных средств	{"header": {"schemaType": "lockResponse","schemaVersion": "1","version": "1","memberId": "9527dd0c-0765-4f1c-8f5f-70a02cf4046c","sourceId": "f34030ef-358a-445c-8567-25985ce6d91c","publishedAt": "2002-10-02T15:00:00.05Z"},
1.2	"schemaVersion" (поле данных)	версия схемы типа электронного сообщения	текстовое поле (textarea)	
1.3	"version" (поле данных)	номер версии электронного сообщения в процессе информационного обмена	числовое значение (int)	
1.4	"memberId" (поле данных)	идентификатор участника информационного обмена, присвоенный Банком России	128-битный идентификатор (GUID), сформированный в соответствии со спецификацией RFC 4122 [16], присвоенный Банком России	
1.5	"sourceId" (поле данных)	идентификатор, присвоенный участником информационного обмена	128-битный идентификатор (GUID), сформированный в соответствии со спецификацией RFC 4122 [16], присвоенный участником информационного обмена	
1.6	"publishedAt" (поле данных)	дата и время информирования участника информационного обмена	формат представления данных в соответствии со спецификацией RFC 3339 [11].	

11.2. Описание формы информационного сообщения Банка России об установлении (или снятии) на банковские (корреспондентские) счета (субсчета) участников информационного обмена ограничения в виде запрета на списание денежных средств. Блок данных [lockResponse]

Номер блока (поля) данных	Идентификатор блока (поля) данных	Содержание блока (поля) данных	Формат поля данных	Формат электронного сообщения
2.1	"sourceId" (поле данных)	идентификатор, присвоенный участником информационного обмена	128-битный идентификатор (GUID), сформированный в соответствии со спецификацией RFC 4122 [16], присвоенный участником информационного обмена	
2.2	"orgBik" (поле данных)	БИК участника информационного обмена	в формате AAAAAAAAA	
2.3	"regNumber" (поле данных)	регистрационный номер из книги государственной регистрации кредитных организаций	текстовое поле (textarea)	
2.4	"uniqIdentifier" (поле данных)	уникальный идентификатор составителя электронного сообщения (УИС) [22]	в формате XXXXXXXXXX	

"lockResponse": [{"sourceId": "f34030ef-358a-445c-8567-25985ce6d91c","orgBik":

2.5	"actionStatus" (поле данных)	статус ограничения на списание денежных средств	Выбирается один код из ограниченного множества возможных значений: - [on] - обращение об установлении ограничения в виде запрета на списание денежных средств с банковских (корреспондентских) счетов (субсчетов); - [off] - обращение о снятии ограничения в виде запрета на списание денежных средств с банковских (корреспондентских) счетов (субсчетов)	"123456789","regNumber": "123456789","uniqIdentifier": "1234567891","actionStatus": "статус ограничения на списание денежных средств","coordinationStatus": "статус выполнения контроля целостности запроса на установление или снятие ограничения в виде запрета на списание денежных средств","dateAt": "20180101","text": "дополнительное описание","attachment": {"sourceId": "f34030ef-358a-445c-8567-25985ce6d91c","comment": "описание вложения","dateTimeAt": "2018-03-22T08:14:38Z","file": {"name": "имя файла","size": "размер файла в байтах","base64": "вложение в формате base64"}}}]}
2.6	"coordination Status" (поле данных)	статус выполнения контроля целостности запроса на установление (или снятие) на банковские (корреспондентские) счета (субсчета) участников информационного обмена ограничения в виде запрета на списание денежных средств	Выбирается один код из ограниченного множества возможных значений: - [accepted] - положительный результат контроля целостности и принятие к исполнению запроса на установление (или снятие) ограничения в виде запрета на списание денежных средств; - [rejected] - отрицательный результат контроля целостности и непринятие к исполнению запроса на установление (или снятие) ограничения в виде запрета на списание денежных средств	
2.7	"dateAt" (поле данных)	календарная дата, с которой необходимо отменить приостановление обмена электронными сообщениями при переводе денежных средств в рамках платежной системы Банка России в связи с выявлением проблем в обеспечении защиты информации и осуществлением (подозрением на осуществление) несанкционированных переводов денежных средств	формат представления данных в соответствии со стандартом ISO 8601:2004 [23]	
2.8	"text" (поле данных)	дополнительное описание	текстовое поле (textarea)	
2.9	"attachment" (блок данных)	дополнительные данные, содержащие информацию об осуществленных операциях по банковским (корреспондентским) счетам (субсчетам) участника информационного обмена		
2.9.1	"sourceId" (поле данных)	идентификатор, присвоенный участником информационного обмена	128-битный идентификатор (GUID), сформированный в соответствии со спецификацией RFC 4122 [16], присвоенный участником информационного обмена	

2.9.2	"comment" (поле данных)	описание вложения	текстовое поле (textarea)	
2.9.3	"dateTimeAt" (поле данных)	дата и время добавления файла	формат представления данных в соответствии со спецификацией RFC 3339 [11]	
2.9.4	"file" (блок данных)	файл данных	Указывается наименование, размер файла (не более 5 Мб), выполняется кодировка в формате Base64	

12. Форма распространения Банком России среди участников информационного обмена данных о выявленных инцидентах, связанных с нарушением требований к обеспечению защиты информации

12.1. Идентификационные данные информационного бюллетеня. Блок данных [HEADER]

Номер блока (поля) данных	Идентификатор блока (поля) данных	Содержание блока (поля) данных	Формат поля данных	Формат электронного сообщения
1.1	"schemaType" (поле данных)	тип электронного сообщения	Указывается значение [REACTION] - информационный бюллетень Банка России	{"header": {"schemaType": "reaction","schemaVersion": "1","version": "1","publishedAt": "2002-10-02T15:00:00.05Z"},
1.2	"schemaVersion" (поле данных)	версия схемы типа электронного сообщения	текстовое поле (textarea)	
1.3	"version" (поле данных)	номер версии электронного сообщения в процессе информационного обмена	числовое значение (int)	
1.4	"publishedAt" (поле данных)	дата и время информирования	формат представления данных в соответствии со спецификацией RFC 3339 [11]	

12.2. Описание формы информационного бюллетеня. Блок данных [REACTION]

Номер блока (поля) данных	Идентификатор блока (поля) данных	Содержание блока (поля) данных	Формат поля данных	Формат электронно
1.1	"fixationAt" (поле данных)	дата и время реализации инцидента у участника информационного обмена	формат представления данных в соответствии со спецификацией RFC 3339 [11]	
1.2	"rootCause" (поле данных)	ключевые причины возникновения инцидента	текстовое поле (textarea)	
1.3	"vectorCode" (поле данных)	идентификатор вектора компьютерной атаки	Выбирается один код из ограниченного множества возможных значений: - вектор [INT] - направленный на инфраструктуру участника информационного обмена; - вектор [EXT] - направленный на клиента участника информационного обмена	
1.4	"serviceType" (блок данных)	идентификатор объекта информационной инфраструктуры	В случае необходимости указания нескольких значений полей данных (type, name, version, description) указывается один или несколько объектов в блоке данных "serviceType"	

1.4.1	"type" (поле данных)	тип атакуемого объекта	Выбирается один код из ограниченного множества возможных значений: 1) системные уровни: - [hw] - аппаратное обеспечение, - [net] - сетевое оборудование, - [net_s] - сетевые приложения и сервисы, - [hw_s] - серверные компоненты виртуализации, программные инфраструктурные сервисы, - [os] - операционные системы, системы управления базами данных, серверы приложений; 2) уровень АС и приложений, эксплуатируемых для предоставления услуг в рамках бизнес-процессов или технологических процессов участника информационного обмена: - [rbs] - система дистанционного банковского обслуживания, - [front-office] - система обработки транзакций, осуществляемых с использованием платежных карт, - [web] - информационные ресурсы сети Интернет, - [abs] - автоматизированная банковская система, - [back-office] - система посттранзакционного обслуживания операций, осуществляемых с использованием платежных карт; - [participant_w] - автоматизированные системы используемые работниками участника информационного обмена 3) уровень АС и приложений клиента участника информационного обмена: - [cfs] - файловый сервер, - [crbs] - система дистанционного банковского обслуживания, - [ecs] - сервер электронной почты; - [clien_w] - автоматизированные системы используемые работниками клиента участника информационного обмена; 4) иная система: - [oth] - иная система	"reaction": {"fixationAt": "2002-10-02T15:00:00.05 возникновения инцидента","vectorCode": "идент атаки","serviceType": [{"type": "тип атакуемого с программного/аппаратного обеспечения","versic обеспечения","description": "дополнительное оп объекта"}],"typeOfAttack": "код типа компьютер [{"device": {"ip": "127.0.0.1","imsi": "международ (индивидуальный номер абонента)","imei": "меж оборудования",aiic": "acquiring institution identific acceptor terminal identification (41 поле ISO 8583) (42 поле ISO 8583)"},"payee": {"bik": "123456789 "P79969612A71BAB224C7CB534FD7A0D3C1C78A "B49087832A71BAB224C7CB534FD7A0D3C1C78A "123456789000","transferId": {"paymentCard": {"r "123412341234123412"},"settlement": {"number" "12345123451234512345"},"phoneNumber": {"nu {"number": "1KoX6AA5VTdbBTkw27YEqKFaTtEQq9 "идентификатор трансграничности","additionalT дополнительного подтверждения операции"]}}

1.4.2	"name" (поле данных)	наименование программного/аппаратного обеспечения	текстовое поле (textarea)
1.4.3	"version" (поле данных)	версия программного/аппаратного обеспечения	текстовое поле (textarea)
1.4.4	"description" (поле данных)	дополнительное описание типа атакуемого объекта	текстовое поле (textarea)
			Выбирается один код из ограниченного множества возможных значений: - [trafficHijackAttacks] - компьютерные атаки, связанные с изменением маршрутно-адресной информации; - [malware] - компьютерные атаки, связанные с использованием вредоносного программного обеспечения применительно к объектам информационной инфраструктуры участников информационного обмена и их клиентов; - [socialEngineering] - компьютерные атаки, возникшие в результате побуждения клиентов к осуществлению операций по переводу денежных средств путем обмана или злоупотребления доверием; - [ddosAttacks] - компьютерные атаки типа "отказ в обслуживании" (DDoS-атаки) применительно к информационной инфраструктуре участников информационного обмена; - [atmAttacks] - компьютерные атаки, связанные с реализацией несанкционированного доступа к банкоматам и платежным терминалам участников информационного обмена; - [vulnerabilities] - компьютерные атаки, связанные с эксплуатацией уязвимостей информационной инфраструктуры участников информационного обмена и их клиентов; - [bruteForces] - компьютерные атаки, связанные с подбором (взломом), компрометацией аутентификационных (учетных) данных; - [spams] - компьютерные атаки, связанные с реализацией спам-

1.5	"typeOfAttack" (поле данных)	идентификатор типа компьютерной атаки	рассылки, осуществляемой в отношении участников информационного обмена и их клиентов; - [controlCenters] - компьютерные атаки, связанные с выявлением взаимодействия объектов информационной инфраструктуры участников информационного обмена с командными центрами Ботнет; - [sim] - компьютерные атаки, связанные с изменением (подменой) идентификатора мобильного абонента (IMSI) номера сим-карты, а также с заменой идентификатора мобильного оборудования (IMEI); - [phishingAttacks] - компьютерные атаки, связанные с информацией, вводящей участников информационного обмена и их клиентов, а также иных лиц, взаимодействующих с ними, в заблуждение относительно принадлежности информации, распространяемой посредством сети Интернет, вследствие сходства доменных имен, оформления или содержания; - [prohibitedContents] - компьютерные атаки, связанные с распространением информации, касающейся предложения и (или) предоставления на территории Российской Федерации финансовых услуг лицами, не имеющими права их оказывать в соответствии с законодательством Российской Федерации. Размещение в сети Интернет запрещенного контента; - [maliciousResources] - компьютерные атаки, связанные с размещением в сети Интернет информации, позволяющей осуществить неправомерный доступ к информационным системам участников информационного обмена и их клиентов, используемым при предоставлении (получении) финансовых услуг, в том числе путем

			неправомерного доступа к конфиденциальной информации клиентов. Размещение в сети Интернет вредоносного ресурса; - [changeContent] - компьютерные атаки, связанные с изменением контента; - [scanPorts] - компьютерные атаки, связанные со сканированием программных портов объектов информационной инфраструктуры участников информационного обмена лицами, не обладающими соответствующими полномочиями; - [other] - иные компьютерные атаки, направленные на объекты информационной инфраструктуры участников информационного обмена и их клиентов	
	"antifraudDistribution" (блок данных)		В случае необходимости указания нескольких значений полей данных (device, payee, additional Status) указывается один или несколько объектов в блоке данных "antifraudDistribution"	
1.6	"device" (подблок данных)	идентификаторы устройства, с которого осуществлялась несанкционированная операция		
1.6.1	"ip" (поле данных)	сетевой адрес компьютера и (или) коммуникационного устройства (маршрутизатора) (IP)	Логический адрес IPv4 должен соответствовать спецификации RFC 791 [12]	
1.6.2	"imsi" (поле данных)	International Mobile Subscriber Identity (IMSI) - международный идентификатор мобильного абонента (индивидуальный номер абонента (клиента - физического лица), по которому система распознает пользователя мобильной связи, использующего стандарты GSM и UMTS	число (15-разрядное в десятичном представлении) AA-BBBBBB-CCCCCC-EE	
1.6.3	"imei" (поле данных)	International Mobile Equipment Identity (IMEI) - международный идентификатор мобильного оборудования (мобильного устройства клиента - физического лица)	число (15-разрядное в десятичном представлении) AA-BBBBBB-CCCCCC-EE	

1.6.4	"aiic" (поле данных)	идентификатор участника, являющегося банком-эквайрером при осуществлении операций по переводу денежных средств с использованием платежных карт	идентификатор участника, являющегося банком-эквайрером при осуществлении операций по переводу денежных средств с использованием платежных карт (Acquiring institution identification code) - поле "F032" стандарта финансовых сообщений ISO 8583 [7], [8], [9]	
1.6.5	"cati" (поле данных)	идентификатор банкомата и (или) электронного терминала, на котором осуществляется операция по переводу и (или) снятию денежных средств	идентификатор банкомата и (или) электронного терминала, на котором осуществляется операция по переводу и (или) снятию денежных средств (Card acceptor terminal identification), - поле " F 0 4 1 " стандарта финансовых сообщений ISO 8583 [7], [8], [9] Значение идентификатора терминала должно быть выровнено влево и дополнено пробелами справа до 8 символов	
1.6.6	"caic" (поле данных)	идентификатор банкомата и (или) электронного терминала, на котором осуществляется операция по переводу и (или) снятию денежных средств, по его географическому местоположению	идентификатор банкомата и (или) электронного терминала, на котором осуществляется операция по переводу и (или) снятию денежных средств, по его географическому местоположению (Card acceptor identification code) - поле "F042" стандарта финансовых сообщений ISO 8583 [7], [8], [9] Значение идентификатора пункта обслуживания должно быть выровнено влево и дополнено пробелами справа до 15 символов	
1.7	"payee" (блок данных)	информация, определяющая получателя перевода денежных средств без согласия клиента (далее - информация о получателе средств)		
1.7.1	"bik" (поле данных)	БИК оператора по переводу денежных средств, обслуживающего получателя средств	в формате AAAAAAAAA	
			Последовательность символов, полученных в результате вычисления хэш-функции SHA-256 от серии и номера документа удостоверяющего личность.	

1.7.2	"hash" (поле данных)	последовательность символов, полученных в результате вычисления хэш-функции SHA-256 от серии и номера документа удостоверяющего личность	Серия и номер документа удостоверяющего личность представляется для вычисления хэш-функции: без пробелов (_), знака номера (N), букв (при их наличии) в верхнем регистре (ABC).
			Для российского паспорта это XXXXYYYYYY, где: XXXX - четырехзначная серия паспорта; YYYYYY - шестизначный номер паспорта.
			Кодировка исходного текста (до хэширования) - Windows-1251; Кодировка текста хэша - Windows-1251.
1.7.3	"hashSnils" (поле данных)	номер СНИЛС в виде хэш-функции SHA-256	Последовательность символов, полученных в результате вычисления хэш-функции SHA-256 от СНИЛС плательщика.
			СНИЛС представляется для вычисления хэш-функции: без пробелов (_) и знаков разделения (-). СНИЛС вида: XXXXXXXXXXX
			Кодировка исходного текста (до хэширования) - Windows-1251; Кодировка текста хэша - Windows-1251.
1.7.4	"inn" (поле данных)	ИНН получателя средств - юридического лица	в формате XXXXXXXXXX - для юридических лиц, в формате XXXXXXXXXX или XXXXXXXXXXX - для индивидуальных предпринимателей и (или) физических лиц, занимающихся в установленном законодательством Российской Федерации порядке частной практикой
1.7.5	"transferId" (подблок данных)	идентификационные данные в зависимости от способа реализации перевода денежных средств	
1.7.5.1	"paymentCard" (подблок данных)	при осуществлении операций по переводу денежных средств с использованием платежных карт	В случае необходимости указания нескольких значений поля данных (number) указывается один или несколько объектов в подблоке данных "paymentCard"
1.7.5.1.1	"number" (поле данных)	номер платежной карты получателя средств, выданной ему и (или) лицу, уполномоченному получателем средств, оператором по переводу денежных средств - эмитентом	в формате XXXXXXXXXXXXXXXXXX
			номер платежной карты представляется без пробелов (_) и знаков разделения (-).

1.7.5.2	"settlement" (подблок данных)	при осуществлении переводов денежных средств по банковским счетам посредством списания денежных средств с банковских счетов плательщиков	В случае необходимости указания нескольких значений поля данных (number) указывается один или несколько объектов в подблоке данных "settlement"
1.7.5.2.1	"number" (поле данных)	номер банковского счета получателя средств, открытого у оператора по переводу денежных средств, обслуживающего получателя средств	в формате XXXXXXXXXXXXXXXXXXX номер банковского счета представляется без пробелов (_) и знаков разделения (-).
1.7.5.3	"phoneNumber" (подблок данных)	при осуществлении переводов денежных средств по абонентскому номеру телефона	В случае необходимости указания дополнительного значения поля данных (number) указывается один или несколько объектов в подблоке данных "phoneNumber"
1.7.5.3.1	"number" (поле данных)	номер телефона получателя средств	в формате KKKXXXNNNNNNNN, где: KKK - от одного до трех символов кода страны; XXX - код оператора; NNNNNNN - 7 знаков номера. Номер телефона представляется без знака плюс (+), пробелов (_) и знаков разделения (-).
1.7.5.4	"idNumber" (подблок данных)	при изменении остатка электронных денежных средств	В случае необходимости указания дополнительного значения поля данных (number) указывается один или несколько объектов в подблоке данных "idNumber"
1.7.5.4.1	"number" (поле данных)	идентификационный номер получателя средств, в частности номер электронного кошелька получателя средств, используемого им на основании договора банковского счета и (или) договора об использовании электронного средства платежа, заключенного с оператором по переводу денежных средств	текстовое поле (textarea)
1.8	"crossBorder" (поле данных)	идентификатор трансграничности	Выбирается один код из ограниченного множества возможных значений: - [CRB] - трансграничный перевод; - [DOM] - перевод внутри страны

1.9	"additionalTrans-actionApprove" (поле данных)	идентификатор дополнительного подтверждения операции	Выбирается один или несколько кодов из ограниченного множества возможных значений: - [3DS] - операция подтверждена с использованием 3D Secure; - [DCS] - реализация технологических мер по использованию раздельных технологий [3]; - [NAA] - операция без подтверждения; - [SMS] - подтверждение операции выполнено с применением коротких текстовых сообщений (СМС); - [LTR] - операция выполнена в соответствии со списком доверенных получателей средств; - [TEL] - операция подтверждена по телефону; - [OAA] - иной способ подтверждения

12.3. Информация о технических данных, описывающих компьютерные атаки, направленные на объекты информационной инфраструктуры участников информационного обмена и их клиентов, а также соответствующие формы электронных сообщений. Блок данных [IMPACTS]

12.3.1. Компьютерные атаки, связанные с изменением маршрутно-адресной информации [trafficHijackAttacks] (для вектора [INT], [EXT])

Номер блока (поля) данных	Идентификатор блока (поля) данных	Содержание блока (поля) данных	Формат поля данных	Формат электронного сообщения
1.1	"legalAsPath" (поле данных)	Штатный AS-Path	текстовое поле (textarea)	"impacts": {"trafficHijackAttacks": [{"legalAsPath": "Штатный AS-Path","wrongAsPath": "Подставной AS-Path","lookingGlass": "Ссылка на используемый Looking Glass для проверки AS-Path","legalPrefix": "Штатный prefix","wrongPrefix": "Подставной prefix"}],
1.2	"wrongAsPath" (поле данных)	Подставной AS-Path	текстовое поле (textarea)	
1.3	"lookingGlass" (поле данных)	Ссылка на используемый Looking Glass для проверки AS-Path	текстовое поле (textarea)	
1.4	"legalPrefix" (поле данных)	Штатный prefix	текстовое поле (textarea)	
1.5	"wrongPrefix" (поле данных)	Подставной prefix	текстовое поле (textarea)	

12.3.2. Компьютерные атаки, связанные с использованием вредоносного программного обеспечения применительно к объектам информационной инфраструктуры участников информационного обмена и их клиентов [malware] (для вектора [INT], [EXT])

Номер блока (поля) данных	Идентификатор блока (поля) данных	Содержание блока (поля) данных	Формат поля данных	Формат электронного сос
2.2	"sources" (блок данных)	идентификаторы источников вредоносных ресурсов в сети Интернет, с которыми взаимодействует атакуемый объект	В случае необходимости указания нескольких значений полей данных (ip, domain, url) указывается один или несколько объектов в блоке данных "sources".	
2.2.1	"ip" (поле данных)	IP-адрес	Логический адрес IPv4 должен соответствовать спецификации RFC 791 [12]	

2.2.2	"domain" (поле данных)	доменное имя	Доменное имя согласно спецификации RFC 1034 [14], а также международной иерархии доменных зон в соответствии со спецификацией RFC 5890 [13]	"malware": [{"sources": [{"ip": "127.0.0.1","domain": "exan "http://example.com"}],"classifications": [{"vendorName": " участником информационного обмена средства от ВВК" соответствии со средством от ВВК участника информац [{"hash": {"md5": "4BA5139A444538479D9D750E2E2779B "D2B063763378A8CB38B192B2F71E78BC13783EFE","sha2 "E25059612A71BAB224C7CB438FD7A0D3C1C78AD40664C {"sourceId": "f34030ef-358a-445c-8567-25985ce6d91c","co вложению","dateTimeAt": "2018-03-22T08:14:38Z","file": { файла в байтах","base64": "вложение в формате base64 "http://domain.com/archive.rar"}}],"malwareMessageSende "qwerty@example.ru","server": "127.0.0.1"}],"malwareMes "f34030ef-358a-445c-8567-25985ce6d91c","comment": "пр "2018-03-22T08:14:38Z","file": {"name": "имя файла","size
2.2.3	"url" (поле данных)	URL-адрес	URL в соответствии со спецификацией RFC 3986 [15]	
2.3	"classifications" (блок данных)	классификация вредоносного кода	В случае необходимости указания нескольких значений полей данных (vendorName, vendorVerdict) указывается один или несколько объектов в блоке данных "classifications"	
2.3.1	"vendorName" (поле данных)	наименование используемого участником информационного обмена средства от ВВК	текстовое поле (textarea)	
2.3.2	"vendorVerdict" (поле данных)	класс ВК в соответствии со средством от ВВК участника информационного обмена	текстовое поле (textarea)	
2.4	"malwareSamples" (блок данных)	указываются образцы ВК, который может характеризоваться хэш-функцией или прикрепленным вложением	В случае необходимости указания нескольких значений подблоков данных (hash, attachment) указывается один или несколько объектов в блоке данных "malwareSamples"	
2.4.1	"hash" (подблок данных)	образец ВК в виде хэш-функций (для каждого образца ВК вычисляется хэш-функция MD5, SHA-1, SHA-256)		
2.4.1.1	"md5" (поле данных)	образец ВК в виде хэш-функции MD5	последовательность символов, полученных в результате вычисления хэш-функции MD5	
2.4.1.2	"sha1" (поле данных)	образец ВК в виде хэш-функции SHA-1	последовательность символов, полученных в результате вычисления хэш-функции SHA-1	
2.4.1.3	"sha256" (поле данных)	образец ВК в виде хэш-функции SHA-256	последовательность символов, полученных в результате вычисления хэш-функции SHA-256	
2.4.2	"attachment" (подблок данных)	образец ВК в виде файла		
2.4.2.1	"sourceId" (поле данных)	идентификатор, присвоенный участником информационного обмена	128-битный идентификатор (GUID), сформированный в соответствии со спецификацией RFC 4122 [16], присвоенный участником информационного обмена	"base64": "вложение в формате base64"},"fileLink": "http://domain.com/archive.rar"},"harmfulResourceAddress "example.com","url": "http://example.com"}],"iocs": [{"net" компрометирующего идентификатора","comment": "доп [{"impact": "тип выявленного компрометирующего иден "дополнительное описание"}],"reg": [{"impact": "тип выя идентификатора","comment": "дополнительное описани выявленного компрометирующего идентификатора","co описание"}],"oth": [{"impact": "тип выявленного компром идентификатора","comment": "дополнительное описани предполагаемого способа заражения","comment": "прим
2.4.2.2	"comment" (поле данных)	описание вложения	текстовое поле (textarea)	
2.4.2.3	"dateTimeAt" (поле данных)	дата и время добавления файла	формат представления данных в соответствии со спецификацией RFC 3339 [11]	
2.4.2.4.1	"file" (подблок данных)	дополнительные материалы, содержащие образцы ВК	Указывается наименование, размер файла (не более 5 Мб), выполняется кодировка в формате Base64	

2.4.2.5	"fileLink" (поле данных)	дополнительные материалы, содержащие образцы ВК	Указывается URL-адрес для скачивания файла, в случае если его размер превышает 5 Мб, в соответствии со спецификацией RFC 3986 [15]
2.5	"malwareMessage Senders" (блок данных)	идентификаторы электронных почтовых ящиков, с которых поступило письмо с вложенным ВК	В случае необходимости указания нескольких значений полей данных (email, server) указывается один или несколько объектов в блоке данных "malwareMessage"
2.5.1	"email" (поле данных)	адрес электронного почтового ящика отправителя	Адрес электронного почтового ящика отправителя представляется в формате в соответствии со спецификацией RFC 5322 [18]
2.5.2	"server" (поле данных)	IP-адрес последнего почтового сервера	Логический адрес IPv4 должен соответствовать спецификации RFC 791 [12]
2.6	malwareMessage-Attachment (подблок данных)	файл с исходным кодом электронного письма (в случае если ВК был прислан на электронный почтовый ящик)	
2.6.1	"sourceId" (поле данных)	идентификатор, присвоенный участником информационного обмена	128-битный идентификатор (GUID), сформированный в соответствии со спецификацией RFC 4122 [16], присвоенный участником информационного обмена
2.6.2	"comment" (поле данных)	описание вложения	текстовое поле (textarea)
2.6.3	"dateTimeAt" (поле данных)	дата и время добавления файла	формат представления данных в соответствии со спецификацией RFC 3339 [11].
2.6.4.1	"file" (блок данных)	файл данных, содержащий образец ВК	Указывается наименование, размер файла (не более 5 Мб), выполняется кодировка в формате Base64
2.6.4.2	"fileLink" (поле данных)	ссылка для получения (скачивания) файла данных, содержащего образцы ВК	Указывается URL-адрес для скачивания файла, в случае если его размер превышает 5 Мб, в соответствии со спецификацией RFC 3986 [15]
2.7	"harmfulResource-Address" (блок данных)	идентификаторы вредоносного ресурса, с которого было загружен ВК	В случае необходимости указания нескольких значений полей данных (ip, domain, url) указывается один или несколько объектов в блоке данных "harmfulResourceAddress"
2.7.1	"ip" (поле данных)	IP-адрес	Логический адрес IPv4 должен соответствовать спецификации RFC 791 [12]
2.7.2	"domain" (поле данных)	доменное имя	Доменное имя согласно спецификации RFC 1034 [14], а также международной иерархии доменных зон в соответствии со спецификацией RFC 5890 [13]
2.7.3	"url" (поле данных)	URL-адрес	URL в соответствии со спецификацией RFC 3986 [15]

2.8	"iocs" (блок данных)	выявленные индикаторы компрометации	В случае необходимости указания нескольких значений полей данных (net, fil, reg, prc, oth) указывается один или несколько объектов в блоке данных "iocs"
2.8.1	"net" (подблок данных)	сетевые индикаторы	В случае необходимости указания нескольких значений полей данных (impact, comment) указывается один или несколько объектов в блоке данных "net"
2.8.1.1	"impact" (поле данных)	тип выявленного компрометирующего идентификатора	Выбирается один код из ограниченного множества возможных значений: - [CRT] - создание технических данных; - [UPD] - изменение технических данных; - [DLT] - удаление технических данных
2.8.1.2	"comment" (поле данных)	дополнительное описание	текстовое поле (textarea)
2.8.2	"fil" (подблок данных)	файловые индикаторы	В случае необходимости указания нескольких значений полей данных (impact, comment) указывается один или несколько объектов в блоке данных "fil"
2.8.2.1	"impact" (поле данных)	тип выявленного компрометирующего идентификатора	Выбирается один код из ограниченного множества возможных значений: - [CRT] - создание технических данных; - [UPD] - изменение технических данных; - [DLT] - удаление технических данных
2.8.2.2	"comment" (поле данных)	дополнительное описание	текстовое поле (textarea)
2.8.3	"reg" (подблок данных)	индикаторы реестра ОС	В случае необходимости указания нескольких значений полей данных (impact, comment) указывается один или несколько объектов в блоке данных "reg"
2.8.3.1	"impact" (поле данных)	тип выявленного компрометирующего идентификатора	Выбирается один код из ограниченного множества возможных значений: - [CRT] - создание технических данных; - [UPD] - изменение технических данных; - [DLT] - удаление технических данных
2.8.3.2	"comment" (поле данных)	дополнительное описание	текстовое поле (textarea)
2.8.4	"prc" (подблок данных)	индикаторы процессов ОС	В случае необходимости указания нескольких значений полей данных (impact, comment) указывается один или несколько объектов в блоке данных "prc"
2.8.4.1	"impact" (поле данных)	тип выявленного компрометирующего идентификатора	Выбирается один код из ограниченного множества возможных значений: - [CRT] - создание технических данных; - [UPD] - изменение технических данных; - [DLT] - удаление технических данных
2.8.4.2	"comment" (поле данных)	дополнительное описание	текстовое поле (textarea)

2.8.5	"oth" (подблок данных)	индикаторы, не учтенные в (2.8.1 - 2.8.4.2.)	В случае необходимости указания нескольких значений полей данных (impact, comment) указывается один или несколько объектов в блоке данных "oth"	
2.8.5.1	"impact" (поле данных)	тип выявленного компрометирующего идентификатора	Выбирается один код из ограниченного множества возможных значений: - [CRT] - создание технических данных; - [UPD] - изменение технических данных; - [DLT] - удаление технических данных	
2.8.5.2	"comment" (поле данных)	дополнительное описание	текстовое поле (textarea)	
2.9	"infectionMethod" (блок данных)	идентификатор предполагаемого способа "заражения"	В случае необходимости указания нескольких значений полей данных (type, comment) указывается один или несколько объектов в блоке данных "infectionMethod"	
2.9.1	"type" (поле данных)	тип предполагаемого способа заражения	Выбирается один код из ограниченного множества возможных значений: - [EML] - по каналам электронной почты; - [DSD] - с носителя информации; - [LCL] - распространение по локальной сети; - [OTH] - иной способ	
2.9.2	"comment" (поле данных)	примечание к выбранному типу	текстовое поле (textarea)	

12.3.3. Компьютерные атаки, возникшие в результате побуждения клиентов к осуществлению операций по переводу денежных средств путем обмана или злоупотребления доверием [socialEngineering] (для вектора [EXT])

Номер блока (поля) данных	Идентификатор блока (поля) данных	Содержание блока (поля) данных	Формат поля данных	Формат электронного сообщения
3.1	"soiTypes" (поле данных)	идентификаторы методов социальной инженерии	Выбирается один или несколько кодов из ограниченного множества возможных значений: - [MOB] - звонок с мобильного телефонного номера; - [TPH] - звонок с телефонного номера 8-800; - [SMS] - СМС-сообщение; - [SNW] - социальная инженерия с использованием социальных сетей; - [MSG] - социальная инженерия с использованием средств мгновенных сообщений; - [OTH] - иной способ реализации методов социальной инженерии	"socialEngineering": {"soiTypes": ["идентификаторы методов

3.2	"soiSenders" (блок данных)	идентификаторы реализации методов социальной инженерии	В случае необходимости указания нескольких значений полей данных (phoneNumber, email, server) указывается один или несколько объектов в блоке данных "soiSenders"	"socialEngineering": {"soiTypes": ["идентификаторы методов социальной инженерии"],"soiSenders": [{"phoneNumber": "1212312345678","email": "qwerty@yandex.ru","server": "127.0.0.1"}],"messageAttachment": {"sourceId": "f34030ef-358a-445c-8567-25985ce6d91c","comment": "описание вложения","datetimeAt": "2018-03-22T08:14:38Z","file": {"name": "имя файла","size": "размер файла в байтах","base64": "вложение в формате base64"},"fileLink": "http://domain.com/archive.rar"},"description": "дополнительное описание"},
3.2.1	"phoneNumber" (поле данных)	телефонный номер	в формате KKKXXXNNNNNNNN, где: KKK - от одного до трех символов кода страны; XXX - код оператора; NNNNNNN - 7 знаков номера.	
			Номер телефона представляется без знака плюс (+), пробелов (_) и знаков разделения (-).	
3.2.2	"email" (поле данных)	электронный почтовый адрес	Адрес электронного почтового ящика отправителя представляется в формате в соответствии со спецификацией RFC 5322 [18]	
3.2.3	"server" (поле данных)	IP-адрес последнего почтового сервера	Логический адрес IPv4 должен соответствовать спецификации RFC 791 [12]	
3.3	"message Attachment" (блок данных)	файлы данных, описывающих метод социальной инженерии		
3.3.1	"sourceId" (поле данных)	идентификатор, присвоенный участником информационного обмена	128-битный идентификатор (GUID), сформированный в соответствии со спецификацией RFC 4122 [16], присвоенный участником информационного обмена	
3.3.2	"comment" (поле данных)	описание вложения	текстовое поле (textarea)	
3.3.3	"dateTimeAt" (поле данных)	дата и время добавления файла	формат представления данных в соответствии со спецификацией RFC 3339 [11]	
3.3.4.1	"file" (подблок данных)	файлы данных, описывающие метод социальной инженерии	Указывается наименование, размер файла (не более 5 Мб), выполняется кодировка в формате Base64	
3.3.5	"fileLink" (поле данных)	файлы данных, описывающие метод социальной инженерии	Указывается URL-адрес для скачивания файла, в случае если его размер превышает 5 Мб, в соответствии со спецификацией RFC 3986 [15]	
3.4	"description" (поле данных)	дополнительное описание	текстовое поле (textarea)	

12.3.4. Компьютерные атаки типа "отказ в обслуживании" (DDoS-атаки) применительно к информационной инфраструктуре участников информационного обмена [ddosAttacks] (для вектора [INT])

Номер блока (поля) данных	Идентификатор блока (поля) данных	Содержание блока (поля) данных	Формат поля данных	Формат электронного сообщения
4.2	"attackType" (блок данных)	тип атаки		"ddosAttacks": [{"attackType": {"type": "тип атаки (по уровням OSI)","comment": "дополнительное описание""sources": [{"ip": "127.0.0.1"}],"power": {"pps": "количество пакетов в секунду","mps": "количество мегабит в секунду","rps": "количество запросов в секунду"},"startTimeAt": "2018-03-22T08:14:38Z","endTimeAt": "2018-03-22T08:14:38Z","negativeImpact": {"type": "тип негативного влияния","comment": "дополнительное описание"}}],
4.2.1	"type" (поле данных)	тип атаки (по уровням OSI)	Выбирается один код из ограниченного множества возможных значений:[1] - "L2/3: ICMP-flood",[2] - "L2/3: NTP-amplification",[3] - "L2/3: TFTP-amplification",[4] - "L2/3: SENTINEL-amplification",[5] - "L2/3: DNS-amplification",[6] - "L2/3: SNMP-amplification",[7] - "L2/3: SSDP-amplification",[8] - "L2/3: CHARGEN-amplification",[9] - "L2/3: RIPv1-amplification",[10] - "L2/3: BitTorrent-amplification",[11] - "L2/3: QTPD-amplification",[12] - "L2/3: Quake-amplification",[13] - "L2/3: LDAP-amplification",[14] - "L2/3: 49ad34-amplification",[15] - "L2/3: Portmap-amplification",[16] - "L2/3: Kad-amplification",[17] - "L2/3: NetBIOS-amplification",[18] - "L2/3: Steam-amplification",[19] - "L3: DPI-attack",[20] - "L4: LAND-attack",[21] - "L4: TCP-SYN-attack",[22] - "L4: TCP-ACK-attack",[23] - "L4: Smurf-attack",[24] - "L4: ICMP/UDP-frag",[25] - "L4: TCP-frag",[26] - "L6: SSL-attack",[27] - "L7: DNS Water Torture Attack",[28] - "L7: Wordpress Pingback DDoS",[29] - "L7: DNS-flood",[30] - "L7: HTTP/S-flood",[31] - "L7: FTP-flood",[32] - "L7: SMTP-flood",[33] - "L7: VoIP/SIP-attack",[34] - "L7: POP3-flood",[35] - "L7: SlowRate-attack,"[36] - "other"	
4.2.2	"comment" (поле данных)	дополнительное описание	текстовое поле (textarea)	
4.3	"sources" (блок данных)	идентификаторы источников реализации атаки	В случае необходимости указания нескольких значений поля данных (ip) указывается один или несколько объектов в блоке данных "sources"	
4.3.1	"ip" (поле данных)	IP-адрес источника реализации атаки (в случае большого количества источников компьютерной атаки в блоке "sources" указывается топ-100 IP-адресов атакующих, при этом полный перечень прикладывается в текстовом файле)	Логический адрес IPv4 должен соответствовать спецификации RFC 791 [12]	
4.4	"power" (блок данных)	мощность реализации атаки		
4.4.1	"pps" (поле данных)	количество пакетов в секунду	пакет в секунду (Packet per second)	
4.4.2	"mps" (поле данных)	количество мегабит в секунду	мегабит в секунду (Megabit per second)	
4.4.3	"rps" (поле данных)	количество запросов в секунду	запросов в секунду (Request per second)	
4.5	"startTimeAt" (поле данных)	время начала атаки	формат представления данных в соответствии со спецификацией RFC 3339 [11].	
4.6	"endTimeAt" (поле данных)	время окончания атаки	формат представления данных в соответствии со спецификацией RFC 3339 [11]	
4.7	"negativeImpact" (блок данных)	негативный эффект от реализации атаки		
4.7.1	"type" (поле данных)	тип негативного влияния	Выбирается один код из ограниченного множества возможных значений: - [NAW] - прерывание доступности сервиса; - [OTH] - деградация сервиса; - [NCQ] - негативного влияния на сервис не оказано	
4.7.2	"comment" (поле данных)	дополнительное описание	текстовое поле (textarea)	

12.3.5. Компьютерные атаки, связанные с реализацией несанкционированного доступа к банкоматам и платежным терминалам участников информационного обмена [atmAttacks] (для вектора [INT])

Номер блока (поля) данных	Идентификатор блока (поля) данных	Содержание блока (поля) данных	Формат поля данных	Формат электронного сообщения
5.1	"target" (блок данных)	идентификатор объекта атаки		"atmAttacks": {"target": {"type": "тип объекта атаки","description": "дополнительное описание"},"attackType": [{"type": "тип атаки в зависимости от объекта атаки","description": "дополнительное описание"}],"attackImages": {"sourceId": "f34030ef-358a-445c-8567-25985ce6d91c","comment": "описание вложения","dateTimeAt": "2018-03-22T08:14:38Z","file": {"name": "имя файла","size": "размер файла в байтах","base64": "вложение в формате base64"},"fileLink": "http://domain.com/archive.rar"}},
5.1.1	"type" (поле данных)	тип объекта атаки	Выбирается один код из ограниченного множества возможных значений: - [ATM] - банкомат; - [CIN] - банкомат с возможностью приема наличных денежных средств; - [REC] - банкомат с функцией ресайклинга (recycling); - [POS] - POS-терминал; - [SST] - платежный терминал; - [OTH] - иной объект	
5.1.2	"description" (поле данных)	дополнительное описание	текстовое поле (textarea)	
5.2	"attackType" (блок данных)	тип атаки	В случае необходимости указания нескольких значений полей данных (type, description) указывается один или несколько объектов в блоке данных "sources"	
5.2.1	"type" (поле данных)	тип атаки в зависимости от объекта атаки	Выбирается один код из ограниченного множества возможных значений: - [BBX] - атаки "блэкбокс"; - [DSP] - атаки "прямой диспенс" и их разновидности; - [SKM] - скимминг; - [OTH] - иной способ	
5.2.2	"description" (поле данных)	дополнительное описание	текстовое поле (textarea)	
5.3	attackImage (блок данных)	дополнительные материалы реализации атаки		
5.3.1	"sourceId" (поле данных)	идентификатор, присвоенный участником информационного обмена	128-битный идентификатор (GUID), сформированный в соответствии со спецификацией RFC 4122 [16], присвоенный участником информационного обмена	
5.3.2	"comment" (поле данных)	описание вложения	текстовое поле (textarea)	
5.3.3	"dateTimeAt" (поле данных)	дата и время добавления файла	формат представления данных в соответствии со спецификацией RFC 3339 [11]	

5.3.4.1	"file" (подблок данных)	файл данных, содержащий дополнительные материалы	Указывается наименование, размер файла (не более 5 Мб), выполняется кодировка в формате Base64
5.3.5	"fileLink" (поле данных)	ссылка для получения (скачивания) файла данных, содержащего дополнительные материалы	Указывается URL-адрес для скачивания файла, в случае если его размер превышает 5 Мб, в соответствии со спецификацией RFC 3986 [15]

12.3.6. Компьютерные атаки, связанные с эксплуатацией уязвимостей информационной инфраструктуры участников информационного обмена и их клиентов [vulnerabilities] (для вектора [INT], [EXT])

Номер блока (поля) данных	Идентификатор блока (поля) данных	Содержание блока (поля) данных	Формат поля данных	Формат электронного сообщения
6.2	"sources" (блок данных)	идентификаторы источников, с которых была выявлена эксплуатация уязвимости	В случае необходимости указания нескольких значений полей данных (ip, url) указывается один или несколько объектов в блоке данных "sources"	"vulnerabilities": [{"sources": [{"ip": "127.0.0.1","url": "http://example.com"}],"identifier": "идентификатор уязвимости","CVSS": "метрика CVSS"}],
6.2.1	"ip" (поле данных)	IP-адрес	Логический адрес IPv4 должен соответствовать спецификации RFC 791 [12]	
6.2.2	"url" (поле данных)	URL-адрес	URL в соответствии со спецификацией RFC 3986 [15]	
6.3	"identifier" (поле данных)	идентификатор уязвимости	Если выявлена уязвимость, должен быть указан ее тип в соответствии с классификацией ФСТЭК России, CVE: - ФСТЭК России - https://bdu.fstec.ru/vul; - Common Vulnerabilities and Exposures (CVE) - https://cve.mitre.org/data/downloads/allitems.html	
6.4	"CVSS" (поле данных)	метрика CVSS	Указывается метрика CVSS v 3.0 (The Common Vulnerability Scoring System (CVSS), если определена . Указывается максимально возможное количество метрик из перечисленных: базовая метрика, временная метрика, контекстная метрика, метрика окружения.	
			В случае если метрика не определена, необходимо использовать калькулятор ФСТЭК России - https://bdu.fstec.ru/cvss3	

12.3.7. Компьютерные атаки, связанные с подбором (взломом), компрометацией аутентификационных (учетных) данных [bruteForces] (для вектора [INT])

Номер блока (поля) данных	Идентификатор блока (поля) данных	Содержание блока (поля) данных	Формат поля данных	Формат электронного сообщения
7.2	"sources" (блок данных)	идентификаторы источников реализации атаки	В случае необходимости указания нескольких значений поля данных (ip) указывается один или несколько объектов в блоке данных "sources"	"bruteForces": [{"sources": [{"ip": "127.0.0.1"}]}],
7.2.1	"ip" (поле данных)	IP-адрес источника реализации атаки (в случае большого количества источников компьютерной атаки в блоке данных "sources" указывается топ-100 IP-адресов атакующих, при этом полный перечень прикладывается в текстовом файле)	Логический адрес IPv4 должен соответствовать спецификации RFC 791 [12]	

12.3.8. Компьютерные атаки, связанные с реализацией спам-рассылки, осуществляемой в отношении участников информационного обмена и их клиентов [spams] (для вектора [INT], [EXT])

Номер блока (поля) данных	Идентификатор блока (поля) данных	Содержание блока (поля) данных	Формат поля данных	Формат электронного сообщения
8.1	"receivedAt" (поле данных)	дата и время получения спам-сообщения	формат представления данных в соответствии со спецификацией RFC 3339 [11]	"spams": [{"receivedAt": "2018-03-22T08:14:38Z","sources": [{"ip": "127.0.0.1","domain": "example.com","email": "qwerty@example.ru"}],"spamImages": {"sourceId": "f34030ef-358a-445c-8567-25985ce6d91c","comment": "примечание к вложению","dateTimeAt": "2018-03-22T08:14:38Z","file": {"name": "имя файла","size": "размер файла в байтах","base64": "вложение в формате base64"},"fileLink": "http://domain.com/archive.rar"}}],
8.2	"sources" (блок данных)	идентификаторы источников реализации атаки (отправители спам-сообщения)	В случае необходимости указания нескольких значений полей данных (ip, domain, email) указывается один или несколько объектов в блоке данных "sources"	
8.2.1	"ip" (поле данных)	IP-адрес	Логический адрес IPv4 должен соответствовать спецификации RFC 791 [12]	
8.2.2.	"domain" (поле данных)	доменное имя	Доменное имя согласно спецификации RFC 1034 [14], а также международной иерархии доменных зон в соответствии со спецификацией RFC 5890 [13]	
8.2.3	"email" (поле данных)	электронный почтовый адрес отправителя спам-сообщения	Адрес электронного почтового ящика отправителя представляется в формате в соответствии со спецификацией RFC 5322 [18]	
8.3	"spamImage" (блок данных)	образец спам-сообщения		
8.3.1	"sourceId" (поле данных)	идентификатор, присвоенный участником информационного обмена	128-битный идентификатор (GUID), сформированный в соответствии со спецификацией RFC 4122 [16], присвоенный участником информационного обмена	
8.3.2	"comment" (поле данных)	описание вложения	текстовое поле (textarea)	
8.3.3	"dateTimeAt" (поле данных)	дата и время добавления файла	формат представления данных в соответствии со спецификацией RFC 3339 [11]	
8.3.4	"file" (блок данных)	файл данных, содержащий дополнительные материалы	Указывается наименование, размер файла (не более 5 Мб), выполняется кодировка в формате Base64	
8.3.5	"fileLink" (поле данных)	ссылка для получения (скачивания) файла данных, содержащего дополнительные материалы	Указывается URL-адрес для скачивания файла, в случае если его размер превышает 5 Мб, в соответствии со спецификацией RFC 3986 [15]	

12.3.9. Компьютерные атаки, связанные с выявлением взаимодействия объектов информационной инфраструктуры участников информационного обмена с командными центрами Ботнет [controlCenters] (для вектора [INT])

Номер блока (поля) данных	Идентификатор блока (поля) данных	Содержание блока (поля) данных	Формат поля данных	Формат электронного сообщения
9.2	"hostUrl" (поле данных)	URL, на котором размещен командный центр Ботнет	URL в соответствии со спецификацией RFC 3986 [15]	"controlCenters": [{"hostUrl": "http://example.com","intruderIp": "1.1.1.1","intruderActions": "что предшествовало инциденту","description": "дополнительное описание командного центра Ботнет","nodes": [{"ip": "127.0.0.1","lastRequestRateTime": "2018-03-22T08:14:38Z"}]}],
9.3	"intruderIp" (поле данных)	IP-адрес злоумышленника, разместившего командный центр Ботнет	Логический адрес IPv4 должен соответствовать спецификации RFC 791 [12]	
9.4	"intruderActions" (поле данных)	описание несанкционированной активности в информационной инфраструктуре участника информационного обмена	текстовое поле (textarea)	
9.5	"description" (поле данных)	дополнительное описание командного центра Ботнет	текстовое поле (textarea)	
9.6	"nodes" (блок данных)	идентификаторы обращения к командному центру Ботнет	В случае необходимости указания нескольких значений полей данных (ip, lastRequestRateTimeAt) указывается один или несколько объектов в блоке данных	
9.6.1	"ip" (поле данных)	внешний IP-адрес (участника информационного обмена)	Логический адрес IPv4 должен соответствовать спецификации RFC 791 [12]	
9.6.2	"lastRequest RatetimeAt" (поле данных)	дата и время последнего взаимодействия с командным центром Ботнет	формат представления данных в соответствии со спецификацией RFC 3339 [11]	

12.3.10. Компьютерные атаки, связанные с изменением (подменой) идентификатора мобильного абонента (IMSI) номера сим-карты, а также с заменой идентификатора мобильного оборудования (IMEI) [sim] (для вектора [EXT])

Номер блока (поля) данных	Идентификатор блока (поля) данных	Содержание блока (поля) данных	Формат поля данных	Формат электронного сообщения
9.1	"mobileOperator" (поле данных)	наименование мобильного оператора связи	текстовое поле (textarea)	"sim": {"mobileOperator": "наименование мобильного оператора связи","phoneNumber": "1212312345678","imsi": "уникальный номер сим-карты","imsiChangedAt": "2018-03-22T08:08:49Z"},
9.2	"phoneNumber" (поле данных)	номер мобильного телефона	в формате KKKXXXNNNNNNNN, где: KKK - от одного до трех символов кода страны; XXX - код оператора; NNNNNNN - 7 знаков номера.	
			Номер телефона представляется без знака плюс (+), пробелов (_) и знаков разделения (-).	
9.3	"imsi" (поле данных)	уникальный номер сим-карты (номер imsi)	XXXXXXXXXXXXXXX	
9.4	"imsiChangedAt" (поле данных)	дата и время фиксации смены IMSI	формат представления данных в соответствии со спецификацией RFC 3339 [11]	

12.3.11. Компьютерные атаки, связанные с распространением информации, касающейся предложений и (или) предоставления на территории Российской Федерации финансовых услуг лицами, не имеющими права их оказывать в соответствии с законодательством Российской Федерации. Размещение в сети Интернет запрещенного контента [prohibitedContents] (для вектора [EXT], [INT])

Номер блока (поля) данных	Идентификатор блока (поля) данных	Содержание блока (поля) данных	Формат поля данных	Формат электронного сообщения
12.1	"sources" (блок данных)	идентификаторы источников запрещенного контента	В случае необходимости указания нескольких значений полей данных (ip, url) указывается один или несколько объектов в блоке данных "target"	"prohibitedContents": [{"sources": [{"ip": "127.0.0.1","url": "http://example.com"}],"type": "тип контента"}],
12.1.1	"ip" (поле данных)	IP-адрес	Логический адрес IPv4 должен соответствовать спецификации RFC 791 [12]	
12.1.2	"url" (поле данных)	URL-адрес	URL в соответствии со спецификацией RFC 3986 [15]	
12.2	"type" (поле данных)	тип запрещенного контента	текстовое поле (textarea)	

12.3.12. Компьютерные атаки, связанные с информацией, вводящей участников информационного обмена и их клиентов, а также иных лиц, взаимодействующих с ними, в заблуждение относительно принадлежности информации, распространяемой посредством сети Интернет, вследствие сходства доменных имен, оформления или содержания. Фишинг [phishingAttacks] (для вектора [EXT], [INT])

Номер блока (поля) данных	Идентификатор блока (поля) данных	Содержание блока (поля) данных	Формат поля данных	Формат электронного сообщения
11.2	"harmful" (блок данных)	идентификаторы источников фишинговых ресурсов	В случае необходимости указания нескольких значений полей данных (ip, url) указывается один или несколько объектов в блоке данных "harmful"	"phishingAttacks": [{"harmful": [{"ip": "127.0.0.1","url": "http://example.com"}],"fixationAt": "2018-03-22T08:14:38Z","messageAttachment": {"sourceId": "f34030ef-358a-445c-8567-25985ce6d91c","comment": "описание вложения","dateTimeAt": "2018-03-22T08:14:38Z","file": {"name": "имя файла","size": "размер файла в байтах","base64": "вложение в формате base64"},"fileLink": "http://domain.com/archive.rar"}}],
11.2.1	"ip" (поле данных)	IP-адрес	Логический адрес IPv4 должен соответствовать спецификации RFC 791 [12]	
11.2.2	"url" (поле данных)	URL-адрес	URL в соответствии со спецификацией RFC 3986 [15]	
11.3	"fixationAt" (поле данных)	дата и время фиксирования фишингового сообщения	формат представления данных в соответствии со спецификацией RFC 3339 [11]	
11.4	"messageAttachment" (блок данных)	образец фишингового обращения		
11.4.1	"sourceId" (поле данных)	идентификатор, присвоенный участником информационного обмена	128-битный идентификатор (GUID), сформированный в соответствии со спецификацией RFC 4122 [16], присвоенный участником информационного обмена	
11.4.2	"comment" (поле данных)	описание вложения	текстовое поле (textarea)	
11.4.3	"dateTimeAt" (поле данных)	дата и время добавления файла	формат представления данных в соответствии со спецификацией RFC 3339 [11]	
11.4.4.1	"file" (блок данных)	файл данных, содержащий дополнительные материалы	Указывается наименование, размер файла (не более 5 Мб), выполняется кодировка в формате Base64	
11.4.5	"fileLink" (поле данных)	ссылка для получения (скачивания) файла данных, содержащего дополнительные материалы	Указывается URL-адрес для скачивания файла, в случае если его размер превышает 5 Мб, в соответствии со спецификацией RFC 3986 [15]	

12.3.15. Компьютерные атаки, связанные со сканированием программных портов объектов информационной инфраструктуры участников информационного обмена лицами, не обладающими соответствующими полномочиями [scanPorts] (для вектора [INT])

Номер блока (поля) данных	Идентификатор блока (поля) данных	Содержание блока (поля) данных	Формат поля данных	Формат электронного сообщения
15	"sourceId" (поле данных)	идентификатор, присвоенный участником информационного обмена	128-битный идентификатор (GUID), сформированный в соответствии со спецификацией RFC 4122 [16], присвоенный участником информационного обмена	"scanPorts": [{"sources": [{"ip": "127.0.0.1"}],"ports": ["23"],"method": "информация о методах сканирования или используемом для этого программном обеспечении","startTimeAt": "2018-03-22T08:14:38Z","endTimeAt": "2018-03-22T08:14:38Z"}],
15.2	"sources" (блок данных)	идентификаторы источников вредоносной активности	В случае необходимости указания нескольких значений поля данных (ip) указывается один или несколько объектов в блоке данных "sources"	
15.2.1	"ip" (поле данных)	IP-адрес	Логический адрес IPv4 должен соответствовать спецификации RFC 791 [12]	
15.3	"ports" (поле данных)	номера портов, которые подверглись сканированию	текстовое поле (textarea)	
15.4	"method" (поле данных)	информация о методах сканирования или используемом для этого программном обеспечении	текстовое поле (textarea)	
15.5	"startTimeAt" (поле данных)	время начала сканирования	формат представления данных в соответствии со спецификацией RFC 3339 [11]	
15.6	"endTimeAt" (поле данных)	время окончания сканирования	формат представления данных в соответствии со спецификацией RFC 3339 [11]	

12.3.16. Иные компьютерные атаки, направленные на объекты информационной инфраструктуры участников информационного обмена и их клиентов [other] (для вектора [INT], [EXT])

16.1	"description" (поле данных)	описание компьютерной атаки	текстовое поле (textarea)	"other": {"description": "описание компьютерной атаки","target": {"ip": "127.0.0.1","url": "http://example.com"},"type": "тип контента","attachment": {"sourceId": "f34030ef-358a-445c-8567-25985ce6d91c","comment": "примечание к вложению","dateTimeAt": "2018-03-22T08:14:38Z","file": {"name": "имя файла","size": "размер файла в байтах","base64": "вложение в формате base64"},"fileLink": "http://domain.com/archive.rar"}}},
16.2	"source" (блок данных)	идентификаторы иного источника вредоносного, запрещенного контента/ресурса		
16.2.1	"ip" (поле данных)	IP-адрес	Логический адрес IPv4 должен соответствовать спецификации RFC 791 [12]	
16.2.2	"url" (поле данных)	URL-адрес	URL в соответствии со спецификацией RFC 3986 [15]	
16.2.3	"type" (поле данных)	иной тип запрещенного, вредоносного, измененного контента	текстовое поле (textarea)	
16.3	"attachment" (блок данных)	дополнительные данные для идентификации компьютерной атаки		
16.3.1	"sourceId" (поле данных)	идентификатор, присвоенный участником информационного обмена	128-битный идентификатор (GUID), сформированный в соответствии со спецификацией RFC 4122 [16], присвоенный участником информационного обмена	
16.3.2	"comment" (поле данных)	описание вложения	текстовое поле (textarea)	
16.3.3	"dateTimeAt" (поле данных)	дата и время добавления файла	формат представления данных в соответствии со спецификацией RFC 3339 [11]	
16.3.4	"file" (блок данных)	файл данных, содержащий дополнительные материалы	Указывается наименование, размер файла (не более 5 Мб), выполняется кодировка в формате Base64	
16.3.5	"fileLink" (поле данных)	ссылка для получения (скачивания) файла данных, содержащего дополнительные материалы	Указывается URL-адрес для скачивания файла, в случае если его размер превышает 5 Мб, в соответствии со спецификацией RFC 3986 [15]	

12.4. Технические рекомендации информационного бюллетеня [signatures]

Номер блока (поля) данных	Идентификатор блока (поля) данных	Содержание блока (поля) данных	Формат поля данных	Формат электронного сообщения
2.1	"mainActions" (поле данных)	рекомендованные действия по противодействию компьютерной атаке	текстовое поле (textarea)	"mainActions": "рекомендованные действия по противодействию компьютерной атаке","signatures": [{"identifier": "идентификатор сигнатуры","yara": "yara-правило","snort": ["rule1","rule2"]}]}}
2.2	"signatures" (блок данных)	сигнатура	В случае необходимости указания нескольких значений полей данных (identifier, yara, snort) указывается один или несколько объектов в блоке данных "source"	
2.3	"identifier" (поле данных)	уникальный идентификатор сигнатуры	последовательность символов, полученных в результате вычисления хэш-функции MD5	
2.4	"yara" (поле данных)	YARA-правило	текстовое поле (textarea)	
2.5	"snort" (поле данных)	Snort-правила	формат представления в виде: (ключ_1: значение_1; ключ_2: значение_2; ... ключ_N: значение_N;)	

13. Форма представления данных, используемая участниками информационного обмена для направления в Банк России информации о планируемых мероприятиях по раскрытию информации о выявленных инцидентах, связанных с нарушением требований к обеспечению защиты информации, и сроки их представления в Банк России

13.1. Условия обязательности и временные характеристики информирования

Условия обязательности информирования:

[O] - информация блока (поля) данных представляется в обязательном порядке;

[N] - информация блока (поля) данных представляется в случае наличия технической возможности.

Временные характеристики информирования (этапы информирования):

[1] - информация блока (поля) данных представляется участником информационного обмена в рамках первичного уведомления не позднее одного рабочего дня до проведения мероприятия по раскрытию информации об инцидентах;

[2] - информация блока (поля) данных представляется участником информационного обмена в рамках последующего уведомления в случае изменения информации о возможном проведении мероприятия по раскрытию информации об инцидентах.

13.2. Идентификационные данные о планируемых мероприятиях по раскрытию информации об инцидентах. Блок данных [HEADER]

Номер блока (поля) данных	Идентификатор блока (поля) данных	Содержание блока (поля) данных	Формат поля данных	Формат электронного сообщения	Обязательность информирования	Этапы информирования
1.1	"schemaType" (поле данных)	тип электронного сообщения	Указывается значение [PUB] - публикация	{"header": {"schemaType": "pub","schemaVersion": "1","version": "1","memberId": "9527dd0c-0765-4f1c-8f5f-70a02cf4046c","sourceId": "f34030ef-358a-445c-8567-25985ce6d91c","publishedAt": "2002-10-02T15:00:00.05Z","modifiedAt": "2002-10-02T15:00:00.05Z"}.	[O]	[1], [2]
1.2	"schemaVersion" (поле данных)	версия схемы типа электронного сообщения	текстовое поле (textarea)		[O]	[1], [2]
1.3	"version" (поле данных)	номер версии электронного сообщения в процессе информационного обмена	числовое значение (int)		[O]	[1], [2]
1.4	"memberId" (поле данных)	идентификатор участника информационного обмена, присвоенный Банком России	128-битный идентификатор (GUID), сформированный в соответствии со спецификацией RFC 4122 [16], присвоенный Банком России		[O]	[1], [2]
1.5	"sourceId" (поле данных)	идентификатор, присвоенный участником информационного обмена	128-битный идентификатор (GUID), сформированный в соответствии со спецификацией RFC 4122 [16], присвоенный участником информационного обмена		[O]	[1], [2]
1.6	"publishedAt" (поле данных)	дата и время первичного информирования	формат представления данных в соответствии со спецификацией RFC 3339 [11]		[O]	[1], [2]
1.7	"modifiedAt" (поле данных)	дата и время промежуточного информирования	формат представления данных в соответствии со спецификацией RFC 3339 [11]		[O]	[2]

13.3. Описание планируемых мероприятий по раскрытию информации об инцидентах. Блок данных [PUB]

Номер блока (поля) данных	Идентификатор блока (поля) данных	Содержание блока (поля) данных	Формат поля данных	Формат электронного сообщения	Обязательность информирования	Эта информи

2.1	"orgName" (поле данных)	наименование организации - участника информационного обмена	текстовое поле (textarea)	"pub": {"orgFullName": "полное наименование участника информационного обмена","persons": [{"lastName": "фамилия","middleName": "отчество","firstName": "имя","landlineNumber": "городской телефон","mobileNumber": "мобильный телефон","email": "адрес электронной почты","position": "должность"}],"eventScheduledAt": "2002-10-02T15:00:00.05Z","location": {"subjectOfFederation": "00","locality": "наименование населенного пункта"},"description": "дополнительные сведения по мероприятию","typeOfActivity": ["тип планируемого мероприятия"],"nameOfActivity": "наименование планируемого мероприятия или ресурса, на котором планируется раскрытие информации","text": "текст к планируемому мероприятию","messageAttachment": {"sourceId": "f34030ef-358a-445c-8567-25985ce6d91c","comment": "описание вложения","dateTimeAt": "2018-03-22T08:14:38Z","file": {"name": "имя файла","size": "размер файла в байтах","base64": "вложение в формате base64"},"fileLink": "http://domain.com/archive.rar"}}}	[O]	[1],
2.2	"persons" (блок данных)	контактные данные ответственного лица	В случае необходимости указания нескольких значений полей данных (lastName, middleName, firstName, landlineNumber, mobileNumber, email, position, eventScheduledAt) указывается один или несколько объектов в блоке данных "persons"		[O]	[1],
2.2.1	"lastName" (поле данных)	фамилия	текстовое поле (textarea)		[O]	[1],
2.2.2	"middleName" (поле данных)	отчество	текстовое поле (textarea)		[O]	[1],
2.2.3	"firstName" (поле данных)	имя	текстовое поле (textarea)		[O]	[1],
2.2.4	"landlineNumber" (поле данных)	городской телефон	текстовое поле (textarea)		[O]	[1],
2.2.5	"mobileNumber" (поле данных)	мобильный телефон	текстовое поле (textarea)		[O]	[1],
2.2.6	"email" (поле данных)	электронный адрес	Адрес электронного почтового ящика отправителя представляется в формате в соответствии со спецификацией RFC 5322 [18]		[O]	[1],
2.2.7	"position" (поле данных)	должность	текстовое поле (textarea)		[O]	[1],
2.3	"eventScheduledAt" (поле данных)	дата и время планируемого мероприятия (выступления) либо публикации по раскрытию информации об инцидентах	формат представления данных в соответствии со спецификацией RFC 3339 [11]		[O]	[1],
2.4	"location" (блок данных)	место проведения мероприятия (выступления)			[O]	[1],
2.4.1	"subjectOfFederation" (поле данных)	код ОКТМО верхнего уровня	текстовое поле (textarea)		[O]	[1],
2.4.2	"locality" (поле данных)	наименование населенного пункта	текстовое поле (textarea)		[O]	[1],
2.5	"description" (поле данных)	дополнительные сведения по мероприятию	текстовое поле (textarea)		[O]	[1],

2.6	"typeofActivity" (поле данных)	тип планируемого мероприятия	Выбирается один или несколько кодов из ограниченного множества возможных значений: - [CNF] - конференция; - [PBE] - публикация на внешнем ресурсе (включая печатные издания); - [PBI] - публикация на собственном ресурсе участника информационного обмена (включая печатные издания)		[O]	[1],
2.7	"nameofActivity" (поле данных)	наименование планируемого мероприятия или ресурса, на котором планируется раскрытие информации	текстовое поле (textarea)		[O]	[1],
2.8	"text" (поле данных)	текст к планируемому мероприятию	текстовое поле (textarea)		[O]	[1],
2.9	"messageAttachment" (блок данных)	описание раскрываемой информации			[N]	[1],
2.9.1	"sourceId" (поле данных)	идентификатор, присвоенный участником информационного обмена	128-битный идентификатор (GUID), сформированный в соответствии со спецификацией RFC 4122 [16], присвоенный участником информационного обмена		[N]	[1],
2.9.2	"comment" (поле данных)	описание вложения	текстовое поле (textarea)		[N]	[1],
2.9.3	"dateTimeAt" (поле данных)	дата и время добавления файла	формат представления данных в соответствии со спецификацией RFC 3339 [11]		[N]	[1],
2.9.4	"file" (блок данных)	файл данных	Указывается наименование, размер файла (не более 5 Мб), выполняется кодировка в формате Base64		[N]	[1],
2.9.5	"fileLink" (поле данных)	ссылка для получения (скачивания) файла данных, содержащего дополнительные материалы	Указывается URL-адрес для скачивания файла, в случае если его размер превышает 5 Мб, в соответствии со спецификацией RFC 3986 [15]		[N]	[1],

14. Условия представления Банку России участниками информационного обмена данных о выявленных инцидентах, связанных с нарушением требований к обеспечению защиты информации

14.1. Информирование Банка России о выявленных событиях типа:

[MTR_WC] - получение оператором по переводу денежных средств, обслуживающим плательщика, включая оператора электронных денежных средств, уведомлений в предусмотренной договором форме от клиентов - физических, юридических

лиц, индивидуальных предпринимателей или лиц, занимающихся частной практикой, о случаях и (или) попытках переводов денежных средств без согласия клиента, в том числе об использовании электронных средств платежа;

[A_SC] - получение расчетным центром платежной системы уведомлений от участников платежной системы о списании денежных средств с их корреспондентских счетов без их согласия и (или) с использованием искаженной информации, содержащейся в распоряжениях платежных клиринговых центров или участников платежной системы;

[UO_WC] - выявление оператором по переводу денежных средств, обслуживающим плательщика, включая оператора электронных денежных средств, операций, соответствующих признакам осуществления перевода денежных средств без согласия клиента, установленным Банком России и размещаемым на официальном сайте Банка России в сети Интернет;

[FMA_WC] - получение уведомлений от клиентов - физических лиц, и (или) индивидуальных предпринимателей, и (или) физических лиц, занимающихся в установленном законодательством Российской Федерации порядке частной практикой, и (или) юридических лиц об осуществлении незаконной финансовой операции;

[MTR_UA] - выявление оператором по переводу денежных средств, обслуживающим плательщика, включая оператора электронных денежных средств, операций по переводу денежных средств и получения наличных денежных средств, совершенных в результате несанкционированного доступа к объектам информационной инфраструктуры оператора по переводу денежных средств, в том числе при уменьшении остатка электронных денежных средств, за исключением виртуальных платежных карт;

[FMS_UA] - выявление незаконных финансовых операций, совершенных в результате несанкционированного доступа к объектам информационной инфраструктуры некредитной финансовой организации;

[UPT_PSP] - осуществление несанкционированного снятия денежных средств оператора по переводу денежных средств в банкоматах;

[DT_ALL] - неоказание услуг оператора по переводу денежных средств в период более двух часов в целом по всем субъектам Российской Федерации, в которых оператор по переводу денежных средств осуществляет перевод денежных средств с использованием платежных карт, их реквизитов и (или) систем (средств) дистанционного банковского обслуживания;

[DT_SEL] - неоказание услуг оператора по переводу денежных средств в период более двух часов в целом по отдельным субъектам Российской Федерации, в которых оператор по переводу денежных средств осуществляет перевод денежных средств с использованием платежных карт, их реквизитов и (или) систем (средств) дистанционного банковского обслуживания;

[UPT_EMP] - осуществление несанкционированного снятия денежных средств оператора электронных денежных средств в банкоматах;

[DT_SC] - неоказание расчетным центром расчетных услуг в период более одного операционного дня;

[DTPT_SC] - невыполнение расчетным центром в течение операционного дня расчетов для принятых к исполнению распоряжений платежного клирингового центра или участников платежной системы;

[DT_CC] - прерывание клиринговым центром оказания услуг платежного клиринга на период более чем один операционный день;

[DTPT_CC] - невыполнение клиринговым центром в течение операционного дня платежного клиринга для принятых к исполнению распоряжений участников платежной системы;

[DT_OC] - прерывание операционным центром предоставления операционных услуг на период более двух часов;

[DT_FS_ALL] - неоказание услуг финансовой организацией в период более двух часов в целом по всем субъектам Российской Федерации, в которых финансовая организация предоставляет финансовые услуги;

[DT_FS_SEL] - неоказание услуг финансовой организацией в период более двух часов в целом по отдельным субъектам Российской Федерации, в которых финансовая организация предоставляет финансовые услуги -

осуществляется безусловно по каждому событию отдельно.

14.2. Выявление участником информационного обмена компьютерных атак, последствия от реализации которых могут привести к событиям, указанным в пункте 14.1:

[PSP_CMTR] - выявление оператором по переводу денежных средств, включая оператора электронных денежных средств, и (или) оператором услуг платежной инфраструктуры атак, последствия от реализации которых могут привести к случаям и попыткам осуществления переводов денежных средств без согласия клиента;

[CO_CFS] - выявление кредитной организацией компьютерных атак, последствия от реализации которых могут привести к случаям и попыткам осуществления финансовой (банковской) операции без согласия клиента;

[NCFI_CFS] - выявление некредитной финансовой организацией компьютерных атак, последствия от реализации которых могут привести к случаям и попыткам осуществления операции на финансовом рынке без согласия клиента.

Осуществляется по следующим критериям (V - критерий информирования):

Объекты компьютерных атак	Типы						
	выявление компьютерной атаки на внешнем периметре информационной инфраструктуры	выявление компьютерной атаки на внутреннем или внешнем периметре информа инфраструктуры					
Системные уровни	[ddosAttacks]	[trafficHijackAttacks]	[vulnerabilities]	[spams]	[phishingAttacks]	[maliciousResources]	[malware]
[hw] - аппаратное обеспечение	V		V				V
[net] - сетевое оборудование	V	V	V			V	V

[net_s] - сетевые приложения и сервисы	V		V				V
[hw_s] - серверные компоненты виртуализации, программные инфраструктурные сервисы	V	V	V				V
[os] - операционные системы, системы управления базами данных, серверы приложений	V		V				V
Уровень АС и приложений, эксплуатируемых для предост авления услуг в рамках бизнес-процессов или технологических процессов участника информационного обмена	[ddosAttacks]	[trafficHijackAttacks]	[vulnerabilities]	[spams]	[phishingAttacks]	[maliciousResources]	[malware]
[rbs] - система дистанционного банковского обслуживания	V		V				V
[front-office] - система обработки транзакций, осуществляемых с использованием платежных карт	V		V				V
[web] - информационные ресурсы сети Интернет	V						V
[abs] - автоматизированная банковская система	V		V				V
[back-office] - система посттранзакционного обслуживания операций, осуществляемых с использованием платежных карт	V		V				V
[int-services] - внутренняя информационная инфраструктура, направленная на поддержание бизнес-процессов участника информационного обмена (почтовые серверы, файловые серверы)			V		V	V	V
[participant_w] - оконечное оборудование (АРМ), используемые работниками участника информационного обмена			V	V			
Уровень АС и приложений, эксплуатируемых клиентом участника информационного обмена	[ddosAttacks]	[trafficHijackAttacks]	[vulnerabilities]	[spams]	[phishingAttacks]	[maliciousResources]	[malware]
[cfs] - файловый сервер		V	V				V
[crbs] - система дистанционного банковского обслуживания	V	V	V				V
[ecs] - учетная запись электронной почты					V	V	V

[client_w] - автоматизированные системы, используемые работниками клиента участника информационного обмена			V				
Иная система	[ddosAttacks]	[trafficHijackAttacks]	[vulnerabilities]	[spams]	[phishingAttacks]	[maliciousResources]	[malware]
[oth] - иная система	V	V	V	V	V	V	V

15. Описание технологии подготовки и направления электронных сообщений при информационном обмене с Банком России

15.1. Технология подготовки электронного сообщения[1]

15.1.1. Подготовка электронного сообщения осуществляется с использованием:

* личного кабинета участника (https://lk.fincert.cbr.ru);

* специализированного приложения, устанавливаемого участником информационного обмена (далее - десктоп-приложение) (https://portal.fincert.ru);

15.1.2. Личный кабинет участника информационного обмена предоставляет возможность сформировать электронное сообщение посредством заполнения веб-формы для направления данных в соответствии с положениями настоящего стандарта.

15.1.3. Десктоп-приложение предоставляет возможность сформировать электронное сообщение посредством заполнения формы приложения для направления данных в соответствии с положениями настоящего стандарта.

15.2. Технология отправки электронного сообщения[2]

Передача информации осуществляется посредством информационных ресурсов Банка России в сети Интернет путем предоставления участникам информационного обмена доступа к личному кабинету (https://lk.fincert.cbr.ru).

Резервные способы передачи информации в Банк России используются участником информационного обмена только в случаях отсутствия телекоммуникационной доступности личного кабинета участника информационного обмена и (или) отсутствия технической возможности передачи информации.

К резервным способам передачи информации относятся:

- использование электронной почты (fincert@cbr.ru);

- использование телефонного звонка в Банк России (+7(495) 7727090)[3].

15.2.1. При передаче информации с использованием электронной почты указывается тема обращения, сопроводительный текст, а также прикрепляются следующие файлы:

- электронное сообщение, сформированное в соответствии с разделом 15.1 настоящего стандарта;

- иные файлы, максимальный размер которых не должен превышать 25 Мб (в случае превышения указанного объема допускается возможность отправки файлов несколькими частями с архивированием в нескольких электронных письмах).

15.2.2. При передаче информации с использованием личного кабинета участника информационного обмена должны быть заполнены поля с пометкой "обязательные для заполнения" с возможностью прикрепления вложений объемом до 2 Гб;

15.2.3. В случае передачи на исследование образцов вредоносного программного обеспечения (вирусов) образцы передаются в Банк России в архиве (rar или zip) с одним из следующих паролей: virus или infected. В случае если в передаваемом архиве не установлен пароль, он удаляется автоматически.

---

[1] Защита передаваемой информации реализуется с использованием сертифицированного СКЗИ, устанавливаемого в соответствии с документом БКМД.42 5790.520.ИЗ.2 "Руководство участника по работе с АСОИ ФинЦЕРТ" (используется сертифицированное СКЗИ "Континент-TLS"). Идентификация и аутентификация участника - отправителя информации в ФинЦЕРТ осуществляется на основе информации, переданной в ФинЦЕРТ (информация об участнике).

[2] Защита передаваемой информации реализуется с использованием сертифицированного СКЗИ, устанавливаемого в соответствии с документом БКМД.42 5790.520.ИЗ.2 "Руководство участника по работе с АСОИ ФинЦЕРТ" (используется сертифицированное СКЗИ "Континент-TLS"). Идентификация и аутентификация участника - отправителя информации в ФинЦЕРТ осуществляется на основе информации, переданной в ФинЦЕРТ (информация об участнике).

[3] Защита передаваемой голосовой информации не осуществляется. Идентификация звонящего осуществляется путем опроса звонящего о наименовании организации, ФИО, должности и контактном телефоне, которые сравниваются с карточкой участника.

Приложение 1. Схемы взаимодействия участника информационного обмена с Банком России

Форма представления данных, используемая участниками информационного обмена для регистрации в Банке России	Форма г

{
"header": {
"schemaType":"participant","schemaVersion": "1","version": "1","memberId":
"9527dd0c-0765-4f1c-8f5f-70a02cf4046c",
"sourceId":
"f34030ef-358a-445c-8567-25985ce6d91c",
"publishedAt":
"2002-10-02T15:00:00.05Z",
"modifiedAt":
"2002-10-02T15:00:00.05Z"
},"participant": {"orgId":
"идентификатор типа участника информационного обмена",
"orgBrand":"наименование бренда участника информационного обмена","orgShortName":
"сокращенное наименование участника информационного обмена",
"orgFullName":
"полное наименование участника информационного обмена",
"orgEmails":["qwerty1@example.ru","qwerty2@example.ru"],"orgIncomingEmail":"requestsFromfincert@example.ru","orgBik":
"123456789","orgLegalEntityForm":"12345","orgBin": ["123456","123456"],"orgInn": "1234567890","orgKpp":
"123456789","orgOgrn":"1234567890000","isp": [{"name":"наименование оператора связи","ipAddress":["192.168.1.0",
"192.168.2.0"]}],"software": [{"sourceId":"f34030ef-358a-445c-8567-25985ce6d91c","type":
"тип программного/аппаратного обеспечения участника информационного обмена",
"name":
"наименование программного/аппаратного
обеспечения","version":
"версия используемого программного/аппаратного
обеспечения","description":
"дополнительное описание программного/аппаратного обеспечения"
}],"persons": [{"memberId":"9527dd0c-0765-4f1c-8f5f-70a02cf4046c","sourceId":"f34030ef-358a-445c-8567-
25985ce6d91c","lastName":"фамилия","middleName":"отчество","firstName": "имя","landlineNumber":"городской
телефон","mobileNumber":"мобильный телефон","email": "адресэлектронной почты","position":"должность","active":
"наличие доступа в личный кабинет участника информационного обмена",
"category":
"категория структурного подразделения ответственного лица участника информационного обмена"
}],"id_cii":"идентификатор объекта КИИ","orgType":
"тип участника информационного обмена",
"legalAddress": {"oktmo":"12345678","postalCode":"почтовый индекс","country":"трехбуквенный код
страны","federalDistrict":"код федерального округа","subjectOfFederation": "00","fiasId":"e6668cfd-ae08-4b02-a385-
88179dfb1097","district": "район","city": "город","cityDistrict":"внутригородской район","locality":"населенный
пункт","street": "улица","house": "номер
дома","building":"корпус/строение","room":"комната/кабинет","additionalInformation":"дополнительная
информация"},"postAddress": {"oktmo":"12345678","postalCode":"почтовый индекс","country":"трехбуквенный код
страны","federalDistrict":"код федерального округа","subjectOfFederation": "00","fiasId":"8abe47a7-24dd-4951-ae16-
f2781eba9d93","district": "район","city": "город","cityDistrict":"внутригородской район","locality":"населенный
пункт","street": "улица","house":
"номердома","building":"корпус/строение","room":"комната/кабинет","additionalInfonnation":"дополнительная
информация"},"physicalAddress": [{"oktmo":"12345678","postalCode":"почтовый индекс","country":"трехбуквенный код
страны","federalDistrict":"код федерального округа","subjectOfFederation": "00","fiasId":"8661e93f-6c6a-4b19-b485-
14e27e564169","district": "район","city": "город","cityDistrict":"внутригородской район","locality":"населенный
пункт","street": "улица","house":
"номердома","building":"корпус/строение","room":"комната/кабинет","additionalInformation":"дополнительная
информация"}]}}

{"header":
10-02T15:
"2002-10-
"descriptio
"субъект,
"request":
"информа
"number":
"номер за
"numberTi
"номер та
"dateTime
"дата и вр
},"assistan
"идентиф
"vectorCo
"идентиф
"serviceTy
"наименов
"version":"
"структур
"technical
"техничес
},"typeOfA
"предприн
"text":
"текст при
"attachme
"f34030ef-
"comment
"описание
"dateTime
"2018-03-
"file": {"na
"наименов
},"classific
"способ ф
}],"int": [{
"оценка о
"relative":
"относите
},"schema
"описание
"attachme
байтах","b
"f34030ef-
"victim":"и
{"hash":"E
{"bik": "12
"наименов
"payerTra
"тип спосо
"payment
операции
"currency"
"валюта о
"dateTime
генерируе
},"settlem
"сумма оп
"currency"
"валюта о
"dateTime
{"number"
адресустр
"междуна
"imei":
"междуна
"aiic":
"Acquiring
"cati":
"Card acce
"caic":
"Card acce
}},"payee
"наименов
"payeeTra
"тип спосо
"payment
{"number"

"additional
"идентифі
]}}],"impa
используе
"127.0.0.1
BK"}],"ma
{"md5":"4
},"attachm
байтах","b
"127.0.0.1
"имяфайла
"127.0.0.1
"iocs": [{"r
"тип выяв
"comment
"тип выяв
"comment
"тип выяв
"comment
"тип выяв
"comment
"тип выяв
"comment
"тип пред
"comment
[{"phoneN
"messageA
"размерфа
445c-8567
сервиса","
секунду","
},"startTim
{"sourceId
"тип атаки
"descriptio
{"name": "
25985ce6c
{"name": "
25985ce6c
"ip": "127.
"127.0.0.1
обеспечен
"операцис
"detectedA
уязвимост
"ссылки на
"manufact
"компания
}}],
"bruteForc
{"name":"
"уровень (
}}],"spams
"127.0.0.1
22T08:14:
"fileLink":"
"127.0.0.1
Ботнет","r
связи","ph
25985ce6c
"fixationAt
"имяфайла
25985ce6c
[{"ip": "12
"127.0.0.1
"type": "ти
"информа
"startTime
{"ip": "127
"иной тип
"attachme
байтах","b
закрытия
"идентифі
"descriptio
"дополнит
"rootCause
"предприн
"signature
"количест
}],"snort":
файла","si

Приложение 2. Схемы взаимодействия Банка России с участником информационного обмена

Форма распространения Банком России среди участников информационного обмена данных о выявленных инцидентах, связанных с нарушением требований к обеспечению защиты информации	Форма запроса Банка России к информационного обмена, обслу получателя средств
{"header": {"schemaType": "reaction","schemaVersion": "1","version": "1","publishedAt": "2002-10-02T15:00:00.05Z"},"reaction": {"fixationAt": "2002-10-02T15:00:00.05Z","rootCause": "ключевые причины возникновения инцидента","vectorCode": "идентификатор вектора компьютерной атаки","serviceType": [{"type": "тип атакуемого объекта","name": "наименование программного/аппаратного обеспечения","version": "версия программного/аппаратного обеспечения","description": "дополнительное описание типа атакуемого объекта"}],"typeOfAttack": "код типа компьютерной атаки", "antifraudDestributed": [{"device": {"ip": "127.0.0.1","imsi": "международный идентификатор мобильного абонента (индивидуальный номер абонента)","imei": "международный идентификатор мобильного оборудования","aiic": "acquiring institution identification code (32 поле ISO 8583)","cati": "card acceptor terminal identification (41 поле ISO 8583)","caic": "card acceptor identification code (42 поле ISO 8583)"},"payee": {"bik": "123456789","hash": "P79969612A71BAB224C7CB534FD7A0D3C1C78AD40664C48F12A9AE48FA441E11","hashSnils": "B49087832A71BAB224C7CB534FD7A0D3C1C78AD40664C48F12A9AE48FA441E44","inn": "123456789000","transferId": {"paymentCard": {"number": "123412341234123412"},"settlement": {"number": "12345123451234512345"	{"header": {"schemaType": "antifraudRequest","schemaVersion": "1","memberId": "9527dd0c-0765-4f 70a02cf4046c", "publishedAt": "2002-10-02T15:00:0 },"antifraudRequest": [{"sourceId": " 445c-8567-25985ce6d91c","victim": о субъектном статусе плательщика {"bik": "123456789","inn": "123456789000","namePayer": наи организации, являющейся плательщиком","payerTransferId": {"transferType": "тип способа реали перевода денежных средств","pay {"number": "123412341234123412", операции по осуществлению перев денежных средств с использовани карт","currency": "валюта операции осуществлению перевода денежны средств","dateTimeAt": "2018-01-13T09:14:38Z","rrn": "номер, генери операции по переводу денежных с выполнении ее авторизации"},"set {"number": "1234512345123451234 "сумма операции по переводу дене средств","currency": "валюта опера переводу денежных средств","date "2018-01-13T09:14:38Z"},"phoneNu {"number": "1212312345678","sum" операции","currency": "валюта опер

},"phoneNumber": {"number": "1212312345678"},"idNumber": {"number": "1KoX6AA5VTdbBTkw27YEqKFaTtEQq97AAT"}}},"additionalStatus": {"crossBorder": "идентификатор трансграничности","additionalTransactionApprove": ["идентификатор дополнительного подтверждения операции"]}}],"impacts": {"trafficHijackAttacks": [{"legalAsPath": "Штатный AS-Path","wrongAsPath": "Подставной AS-Path","lookingGlass": "Ссылка на используемый Looking Glass для проверки AS-Path","legalPrefix": "Штатный prefix","wrongPrefix": "Подставной prefix"}],"malware": [{"sources": [{"ip": "127.0.0.1","domain": "example.com","url": "http://example.com"}],"classifications": [{"vendorName": "наименование используемого участником информационного обмена средства от ВВК","vendorVerdict": "класс ВК в соответствии со средством от ВВК участника информационного обмена"}],"malwareSamples": [{"hash": {"md5": "4BA5139A444538479D9D750E2E2779BF","sha1": "D2B063763378A8CB38B192B2F71E78BC13783EFE","sha256": "E25059612A71BAB224C7CB438FD7A0D3C1C78AD40664C48F12A9AE48FA441E44"},"attachment": {"sourceId": "f34030ef-358a-445c-8567-25985ce6d91c","comment": "примечание к вложению","dateTimeAt": "2018-03-22T08:14:38Z","file": {"name": "имя файла","size": "размер файла в байтах","base64": "вложение в формате base64"},"fileLink": "http://domain.com/archive.rar"}}],"malwareMessageSenders": [{"email": "qwerty@example.ru"."server": "127.0.0.1"}],"malwareMessageAttachment": {"sourceId": "f34030ef-358a-445c-8567-25985ce6d91c",

"dateTimeAt": "2018-01-13T09:14:38Z"},"idNumber": {"numb
"1KoX6AA5VTdbBTkw27YEqKFaTtEQ
"сумма операции","currency": "вал
операции","dateTimeAt": "2018-01-13T09:14:38Z"}},"device": {"ip": "ce
устройства","imsi": "международны
идентификатор мобильного абоне
(индивидуальный номер абонента)
"международный идентификатор
оборудования","aiic": "Acquiring ins
identification code (32 поле ISO 858
acceptor terminal identification (41 п
8583)","caic": "Card acceptor identifi
поле ISO 8583)"}},"payee": {"bik":
"123456789","inn": "123456789000"
"наименование организации, явля
получателем средств","payeeTrans
{"transferType": "тип способа реали
перевода денежных средств","pay
{"number": "123412341234123412"
{"number": "номер расчетного счет
средств, открытого у оператора по
денежных средств, обслуживающе
получателя средств"},"phoneNumb
{"number": "1212312345678"},"idN
{"number":
"1KoX6AA5VTdbBTkw27YEqKFaTtEQ

"comment": "примечание к вложению","dateTimeAt": "2018-03-22T08:14:38Z","file": {"name": "имя файла","size": "размер файла в байтах","base64": "вложение в формате base64"},"fileLink": "http://domain.com/archive.rar"},"harmfulResourceAddress": [{"ip": "127.0.0.1","domain": "example.com","url": "http://example.com"}],"iocs": [{"net": [{"impact": "тип выявленного компрометирующего идентификатора","comment": "дополнительное описание"}],"fil": [{"impact": "тип выявленного компрометирующего идентификатора","comment": "дополнительное описание"}],"reg": [{"impact": "тип выявленного компрометирующего идентификатора","comment": "дополнительное описание"}],"prc": [{"impact": "тип выявленного компрометирующего идентификатора","comment": "дополнительное описание"}],"oth": [{"impact": "тип выявленного компрометирующего идентификатора","comment": "дополнительное описание"}]}],"infectionMethod": [{"type": "тип предполагаемого способа заражения","comment": "примечание к выбранному типу"}]}],"socialEngineering": {"soiTypes": ["идентификаторы методов социальной инженерии"],"soiSenders": [{"phoneNumber": "1212312345678","email": "qwerty@yandex.ru"."server": "127.0.0.1"}],"messageAttachment": {"sourceId": "f34030ef-358a-445c-8567-25985ce6d91c","comment": "описание вложения","datetimeAt": "2018-03-22T08:14:38Z","file": {"name": "имя файла","size": "размер файла в байтах","base64": "вложение в формате base64"},"fileLink": "http://domain.com/archive.rar"},"description": "дополнительное описание"},"ddosAttacks": [{"attackType": {"type": "тип атаки (по уровням OSI)","comment": "дополнительное описание"},"sources": [{"ip": "127.0.0.1"}],"power": {"pps": "количество пакетов в секунду","mps": "количество мегабит в секунду","rps": "количество запросов в секунду"},"startTimeAt": "2018-03-22T08:14:38Z","endTimeAt": "2018-03-22T08:14:38Z","negativeImpact": {"type": "тип негативного влияния","comment": "дополнительное описание"

}}],"atmAttacks": {"target": {"type": "тип объекта атаки","description": "дополнительное описание"},"attackType": [{"type": "тип атаки в зависимости от объекта атаки","description": "дополнительное описание"}],"attackImages": {"sourceId": "f34030ef-358a-445c-8567-25985ce6d91c","comment": "описание вложения","dateTimeAt": "2018-03-22T08:14:38Z","file": {"name": "имя файла","size": "размер файла в байтах","base64": "вложение в формате base64"},"fileLink": "http://domain.com/archive.rar"}}"vulnerabilities": [{"sources": [{"ip": "127.0.0.1","url": "http://example.com"}],"identifier": "идентификатор уязвимости","CVSS": "метрика CVSS"}],"bruteForces": [{"sources": [{"ip": "127.0.0.1"}]}],"spams": [{"receivedAt": "2018-03-22T08:14:38Z","sources": [{"ip": "127.0.0.1","domain": "example.com","email": "qwerty@example.ru"}],"spamImages": {
"sourceId": "f34030ef-358a-445c-8567-25985ce6d91c",
"comment": "примечание к вложению","dateTimeAt": "2018-03-22T08:14:38Z","file": {"name": "имя файла","size": "размер файла в байтах","base64": "вложение в формате base64"},"fileLink": "http://domain.com/archive.rar"}}],"controlCenters": [{"hostUrl": "http://example.com","intruderIp": "1.1.1.1","intruderActions": "что предшествовало инциденту",
"description": "дополнительное описание командного центра Ботнет",
"nodes": [{"ip": "127.0.0.1","lastRequestRateTime": "2018-03-22T08:14:38Z"}]}],"sim": {"mobileOperator": "наименование мобильного оператора связи","phoneNumber": "1212312345678","imsi": "уникальный номер сим-карты","imsiChangedAt": "2018-03-22T08:08:49Z"},"prohibitedContents": [{"sources": [{"ip": "127.0.0.1","url": "http://example.com"}],"type": "тип контента"}],"phishingAttacks": [{"harmful": [{"ip": "127.0.0.1","url": "http://example.com"

}],"fixationAt": "2018-03-22T08:14:38Z","messageAttachment": {
"sourceId": "f34030ef-358a-445c-8567-25985ce6d91c",
"comment": "описание вложения","dateTimeAt": "2018-03-22T08:14:38Z","file": {"name": "имя файла","size": "размер файла в байтах","base64": "вложение в формате base64"},"fileLink": "http://domain.com/archive.rar"}}],"maliciousResources": [{"sources": [{"ip": "127.0.0.1","url": "http://example.com"}],"activityType": "тип вредоносной активности"}],"changeContent": [{"targets": [{"ip": "127.0.0.1","url": "http://example.com"}],"type": "тип измененного контента"}],"scanPorts": [{"sources": [{"ip": "127.0.0.1"}],"ports": ["23"],"method": "информация о методах сканирования или используемом для этого программном обеспечении","startTimeAt": "2018-03-22T08:14:38Z","endTimeAt": "2018-03-22T08:14:38Z"}],"other": {"description": "описание компьютерной атаки","target": {"ip": "127.0.0.1","url": "http://example.com"},"type": "тип контента","attachment": {"sourceId": "f34030ef-358a-445c-8567-25985ce6d91c","comment": "примечание к вложению","dateTimeAt": "2018-03-22T08:14:38Z","file": {"name": "имя файла","size": "размер файла в байтах","base64": "вложение в формате base64"},"fileLink": "http://domain.com/archive.rar"}}},"mainActions": "рекомендованные действия по противодействию компьютерной атаке","signatures": [{"identifier": "идентификатор сигнатуры","yara": "yara-правило","snort": ["rule1", "rule2"]}]}}

Приложение 3. Диаграммы процессов взаимодействия участника информационного обмена с Банком России

3.1. Диаграмма регистрации участника информационного обмена и изменения регистрационных данных участника информационного обмена

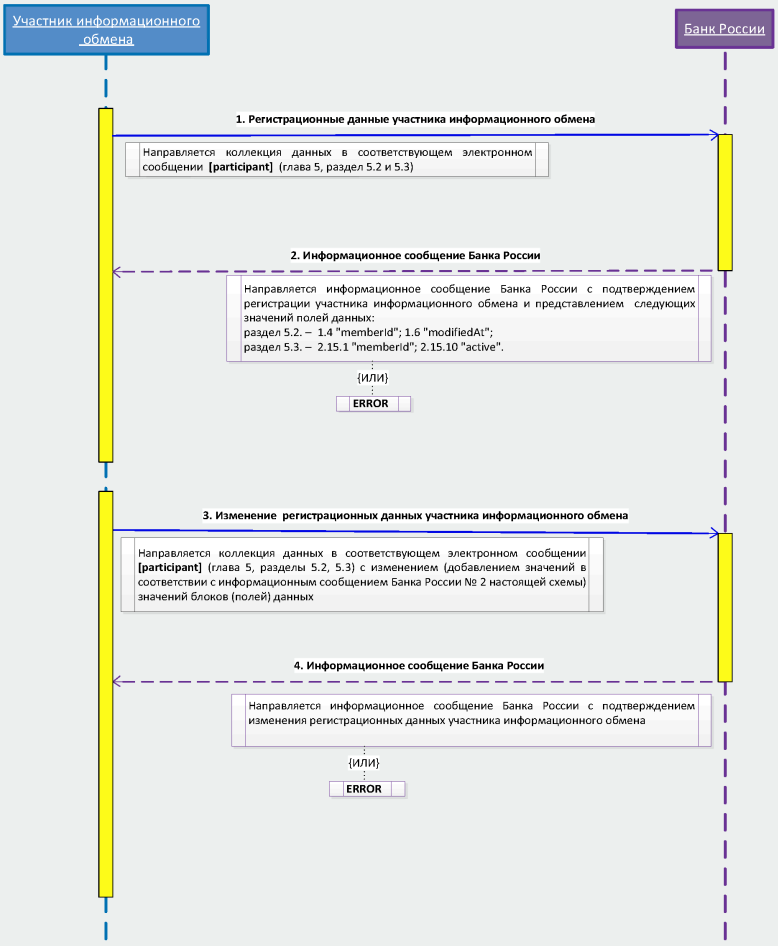

Рисунок 1. Регистрация участника информационного обмена и изменение регистрационных данных участника информационного обмена

3.2. Диаграмма информирования участником информационного обмена Банка России об инцидентах, связанных с нарушением требований к обеспечению защиты информации

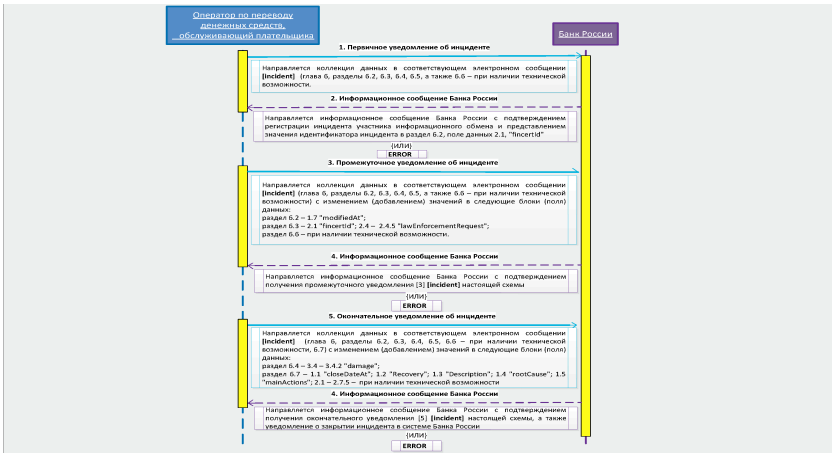

Рисунок 2. Информирование участником информационного обмена Банка России об инцидентах, связанных с нарушением требований к обеспечению защиты информации

3.3. Диаграмма информирования участником информационного обмена Банка России обо всех случаях и (или) попытках осуществления переводов денежных средств без согласия клиента, а также направления операторами по переводу денежных средств уведомлений о приостановлении зачисления денежных средств на банковский счет получателя средств или увеличении остатка электронных денежных средств получателя средств, невозможности приостановления зачисления денежных средств на банковский счет получателя средств или приостановления увеличения остатка электронных денежных средств получателя средств

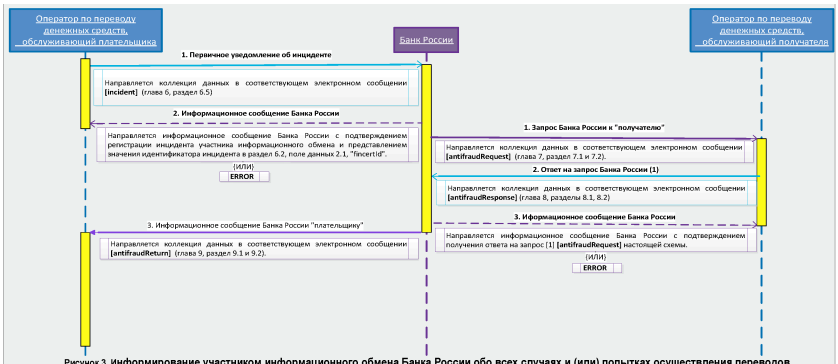

Рисунок 3. Информирование участником информационного обмена Банка России обо всех случаях и (или) попытках осуществления переводов денежных средств без согласия клиента, а также о направлении операторами по переводу денежных средств уведомлений о приостановлении зачисления денежных средств на банковский счет получателя средств или увеличении остатка электронных денежных средств получателя средств, о невозможности приостановления зачисления денежных средств на банковский счет получателя средств или приостановления увеличения остатка электронных денежных средств получателя средств

3.4. Диаграмма информирования Банка России участниками информационного обмена, использующими сервис срочного перевода и сервис несрочного перевода для осуществления перевода денежных средств, не являющимися подразделениями Банка России, об установлении (или снятии) на их банковские (корреспондентские) счета (субсчета) ограничения в виде запрета на списание денежных средств при выявленных инцидентах, связанных с нарушением требований к обеспечению защиты информации при осуществлении переводов денежных средств, на объектах информационной инфраструктуры участников информационного обмена

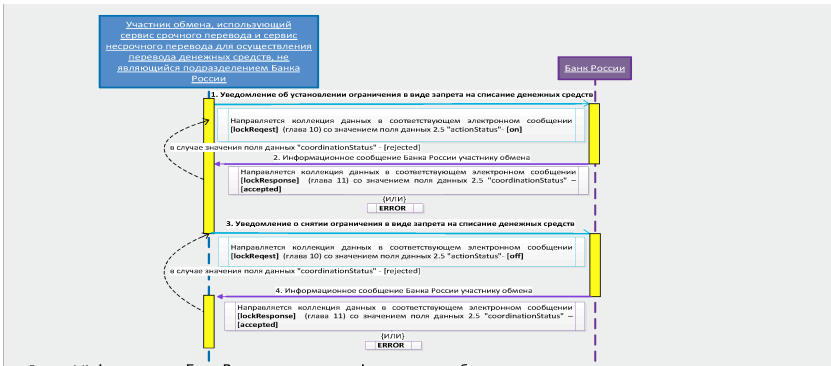

Рисунок 4. Информирование Банка России участниками информационного обмена, использующими сервис срочного перевода и сервис несрочного перевода для осуществления перевода денежных средств, не являющимися подразделениями Банка России, об установлении (или снятии) на их банковские (корреспондентские) счета (субсчета) ограничения в виде запрета на списание денежных средств при выявленных инцидентах, связанных с нарушением требований к обеспечению защиты информации при осуществлении переводов денежных средств, на объектах информационной инфраструктуры участников информационного обмена

3.5. Диаграмма направления Банком России участнику информационного обмена информации о выявленных инцидентах, связанных с нарушением требований к обеспечению защиты информации

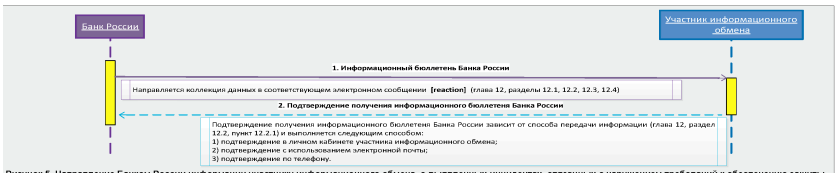

Рисунок 5. Направление Банком России информации участнику информационного обмена о выявленных инцидентах, связанных с нарушением требований к обеспечению защиты информации

3.6. Диаграмма направления участником информационного обмена в Банк России информации о планируемых мероприятиях по раскрытию информации об инцидентах, связанных с нарушением требований к обеспечению защиты информации

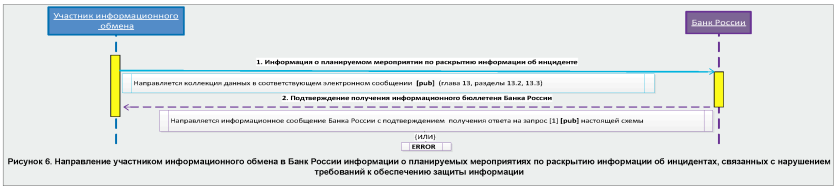

Рисунок 6. Направление участником информационного обмена в Банк России информации о планируемых мероприятиях по раскрытию информации об инцидентах, связанных с нарушением требований к обеспечению защиты информации

3.7. Примечание:

Пунктирными линиями на рисунках 1 - 6 изображены сообщения и компоненты, не являющиеся частью настоящего стандарта. Линии приведены для представления процесса взаимодействия участника информационного обмена и Банка России.

Библиография

1. Федеральный закон от 10 июля 2002 года N 86-ФЗ "О Центральном банке Российской Федерации (Банке России)".

2. Федеральный закон от 27 июня 2011 года N 161-ФЗ "О национальной платежной системе".

3. Положение Банка России от 9 июня 2012 года N 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".

4. Нормативный акт Банка России, устанавливающий формы и порядок направления операторами по переводу денежных средств, операторами платежных систем, операторами услуг платежной инфраструктуры в Банк России информации обо всех

случаях и попытках осуществления переводов денежных средств без согласия клиента и получения ими от Банка России информации, содержащейся в базе данных о случаях и попытках осуществления переводов денежных средств без согласия клиента, а также порядок реализации операторами по переводу денежных средств, операторами платежных систем, операторами услуг платежной инфраструктуры мероприятий по противодействию осуществлению переводов денежных средств без согласия клиента.

5. Нормативный акт Банка России, устанавливающий обязательные для кредитных организаций требования к обеспечению защиты информации при осуществлении банковской деятельности.

6. Нормативный акт Банка России, устанавливающий обязательные для некредитных финансовых организаций требования к обеспечению защиты информации при осуществлении деятельности в сфере финансовых рынков.

7. ISO 8583 - Financial transaction card originated messages - Interchange message specifications - Part 1: Messages, data elements and code values. URL: https://www.iso.Org/obp/ui/#iso:std:iso:8583:-1:ed-1:v1:en (дата обращения: 25.05.2018).

8. ISO 8583 - Financial transaction card originated messages - Interchange message specifications - Part 2: Application and registration procedures for Institution Identification Codes (IIC). URL: https://www.iso.Org/obp/ui/#iso:std:iso:8583:-2:ed-1:v1:en (дата обращения: 24.03.2018).

9. ISO 8583 - Financial transaction card originated messages - Interchange message specifications - Part 3: Maintenance procedures for messages, data elements and code values. URL: https://www.iso.Org/obp/ui/#iso:std:iso:8583:-3:ed-2:v1:en (дата обращения 17.04.2018).

10. ISO 4217 - Codes for the representation of currencies and funds. URL: https://www.iso.Org/obp/ui/#iso:std:iso:4217:ed-8:v1:en (дата обращения 25.02.2018).

11. RFC 3339 - Date and Time on the Internet: Timestamps. URL: https://www.rfc-editor.org/rfc/rfc3339.txt (дата обращения 02.02.2018).

12. RFC 791 - Internet Protocol. URL: https://www.rfc-editor.org/rfc/rfc791.txt (дата обращения 14.05.2018).

13. RFC 5890 - Internationalized Domain Names for Applications (IDNA): Definitions and Document Framework. URL: https://www.rfc-editor.org/rfc/rfc5890.txt (дата обращения 08.02.2018).

14. RFC 1034 - Domain names - concepts and facilities. URL: https://www.rfc-editor.org/rfc/rfc1034.txt (дата обращения: 15.03.2018).

15. RFC 3986 - Uniform Resource Identifier (URI): Generic Syntax. URL: https://www.rfc-editor.org/rfc/rfc3986.txt (дата обращения: 07.03.2018).

16.RFC 4122 - A Universally Unique IDentifier (UUID) URN Namespace. URL: https://www.rfc-editor.org/rfc/rfc4122.txt (дата обращения: 21.04.2018).

17. RFC 997 - Internet numbers. URL: https://www.rfc-editor.org/rfc/rfc997.txt (дата обращения: 23.01.2018).

18. RFC 5322 - Internet Message Format. URL: https://www.rfc-editor.org/rfc/rfc5322.txt (дата обращения: 24.01.2018).

19. Национальный стандарт Российской Федерации ГОСТ Р ИСО/МЭК 15408-3-2013 "Информационная технология. Методы и средства обеспечения безопасности. Критерии оценки безопасности информационных технологий. Часть 3. Компоненты доверия к безопасности".

20. Нормативный акт Банка России, устанавливающий формы и порядок направления операторами по переводу денежных средств уведомлений о приостановлении зачисления денежных средств на банковский счет получателя средств или увеличения остатка электронных денежных средств получателя средств, о невозможности приостановления зачисления денежных средств на банковский счет получателя средств или приостановления увеличения остатка электронных денежных средств получателя средств.

21. Нормативный акт Банка России, устанавливающий требования к обеспечению защиты информации в платежной системе Банка России.

22. Положение Банка России от 06.07.2017 N 595-П "О платежной системе Банка России".

23. ISO 8601:2004 - Data elements and interchange formats - Information interchange - Representation of dates and times. URL: https://www.iso.org/ru/standard/40874.html (дата обращения 29.06.2018).