Приложение к письму Банка России «О составлении формы отчетности и использовании подсистемы «Фид-Антифрод» АСОИ ФинЦЕРТ»

35% опрошенных кредитных организаций не испытывают трудностей при предоставлении формы 0403203 и работе с ФАФ.

50% опрошенных кредитных организаций заявили о сложностях при использовании ФАФ, в частности:

при заведении инцидентов c использованием личного кабинета зачастую невозможно пользоваться системой в рабочее время. Система очень медленно реагирует, зависает при открытии ранее заведенных инцидентов и запросов (до 5-15 минут). На скачивание фидов уходит до 40 минут. Наиболее комфортная работа в личном кабинете возможна только в утренние часы. Работа АСОИ ФинЦЕРТ особенно замедлилась после обновления 15–16 августа 2020 года. Кредитные организации предполагают, что система не справляется с большой нагрузкой, и просят повысить ее быстродействие и производительность.

Ответ:

Действительно, после проведения обновления 15–16 августа 2020 года выявлялись замедления в работе личного кабинета участника АСОИ ФинЦЕРТ. Проблема была оперативно выявлена, дефектована, и 26 августа 2020 года с 20:00 до 24:00 проведены работы по увеличению ресурсов системы, что позволило снять проблему.

Отсутствует оперативное информирование кредитных организаций о временной неработоспособности системы или части ее функционала. В частности, ФАФ периодически бывает недоступен в ночное время без предупреждений. Кредитные организации просят внедрить сервис оперативного уведомления о временной недоступности системы.

Ответ:

Для оперативного уведомления участников обмена информация о текущем режиме функционирования и о плановых работах в АСОИ ФинЦЕРТ и АС «Фид-Антифрод» размещается на инфопортале АСОИ ФинЦЕРТ (доступен участникам обмена по адресу https://portal.fincert.cbr.ru).

О всех работах, при которых АСОИ ФинЦЕРТ и АС «Фид-Антифрод» недоступны для участников обмена, проводится соответствующее информирование о кратковременном прерывании доступа путем сообщения на инфопортале, о длительном – путем сообщения на инфорпортале с дублированием информации в виде соответствующего бюллетеня в адрес всех участников обмена.

С учетом вышеуказанного полагаем, что часть участников, уведомивших Ассоциацию, не ознакомилась с информацией, представленной на инфорпортале. Если со стороны Ассоциации есть предложения по его дополнению, готовы рассмотреть конкретные предложения.

Справочно. На инфопортале АСОИ ФинЦЕРТ, доступном всем участникам обмена, размещается следующая информация об АСОИ ФинЦЕРТ и АС «Фид-Антифрод»:

текущий режим функционирования и информация о плановых работах в АСОИ ФинЦЕРТ и АС «Фид-Антифрод»;

документация на системы в части, передаваемой участникам обмена и разработчикам;

информация по использованию API;

порядок подключения и использования системы;

часто задаваемые вопросы/ответы (FAQ) и другая справочная информация.

Возникают трудности выбора категорий, к которым подходит конкретный инцидент. Например, клиенту позвонили мошенники (тип «социальная инженерия»), затем прислали с использованием WhatsApp (тип «социальная инженерия») ссылку на фишинговую страницу, на которой произошла операция без согласия клиента (тип – «фишинговая атака»). В данном случае, если инцидент занести как «социальная инженерия», то невозможно будет завести URL-адрес фишинговой страницы, а если указать тип инцидента «фишинговая атака», тогда не получится указать номера телефонов. Необходима возможность выбора комбинации категорий инцидентов.

Ответ:

В настоящее время информирование по инцидентам построено на основе стандарта Банка России СТО БР БФБО-1.5-2018 «О формах и сроках взаимодействия Банка России с участниками информационного обмена при выявлении инцидентов, связанных с нарушением требований к обеспечению защиты информации», не предполагающего выбор одновременно двух типов атаки. Данное предложение будет рассмотрено при корректировке нормативной базы и развитии систем АСОИ ФинЦЕРТ и АС «Фид-Антифрод».

Из-за смены на стороне ФинЦЕРТ формата данных возникают проблемы с обработкой JSON-файлов. Вследствие этого кредитным организациям необходимо либо заполнять информацию об инцидентах вручную (эффективность снижается более чем в 3 раза), либо оперативно вносить изменения в формат данных. Кредитные организации просят заблаговременно предупреждать о смене формата взаимодействия для внесения изменений в свои автоматизированные системы.

Ответ:

Начиная с 1 июня 2020 года осуществлялось информирование всех участников обмена.

1. На инфопортале сформирована и опубликована статья, посвященная изменениям в АСОИ-2 (https://portal.fincert.cbr.ru/Content/1129/информация-по-изменениям-в-асои-финцерт-второй-очереди.pdf).
2. Актуализированы четыре документа (статьи на инфопортале) для участников по обновлению АСОИ ФинЦЕРТ и соответствующим изменениям в АС «Фид-Антифрод»:

руководство Участника по работе с АСОИ ФинЦЕРТ ([https://portal.fincert.cbr.ru/Content/1136/руководство\_участника.pdf](https://portal.fincert.cbr.ru/Content/1136/%D1%80%D1%83%D0%BA%D0%BE%D0%B2%D0%BE%D0%B4%D1%81%D1%82%D0%B2%D0%BE_%D1%83%D1%87%D0%B0%D1%81%D1%82%D0%BD%D0%B8%D0%BA%D0%B0.pdf));

описание схемы инцидентов АСОИ ФинЦЕРТ-2 ([https://portal.fincert.cbr.ru/Content/1138/схема-3014.zip](https://portal.fincert.cbr.ru/Content/1138/%D1%81%D1%85%D0%B5%D0%BC%D0%B0-3014.zip));

временная инструкция по заполнению карточки инцидента для операций без согласия клиента ([https://portal.fincert.cbr.ru/Content/1132/инструкция-по-заполнению-карточки-инцидента.pdf](https://portal.fincert.cbr.ru/Content/1132/%D0%B8%D0%BD%D1%81%D1%82%D1%80%D1%83%D0%BA%D1%86%D0%B8%D1%8F-%D0%BF%D0%BE-%D0%B7%D0%B0%D0%BF%D0%BE%D0%BB%D0%BD%D0%B5%D0%BD%D0%B8%D1%8E-%D0%BA%D0%B0%D1%80%D1%82%D0%BE%D1%87%D0%BA%D0%B8-%D0%B8%D0%BD%D1%86%D0%B8%D0%B4%D0%B5%D0%BD%D1%82%D0%B0.pdf));

комплект предварительно заполненных json-файлов ([https://portal.fincert.cbr.ru/Content/1133/комплект-json.zip](https://portal.fincert.cbr.ru/Content/1133/%D0%BA%D0%BE%D0%BC%D0%BF%D0%BB%D0%B5%D0%BA%D1%82-json.zip)).

1. Опубликованы две новости, посвященные обновлению АСОИ-2 ([https://portal.fincert.cbr.ru/news/изменения-в-функционале-асои-финцерт-2/](https://portal.fincert.cbr.ru/news/%D0%B8%D0%B7%D0%BC%D0%B5%D0%BD%D0%B5%D0%BD%D0%B8%D1%8F-%D0%B2-%D1%84%D1%83%D0%BD%D0%BA%D1%86%D0%B8%D0%BE%D0%BD%D0%B0%D0%BB%D0%B5-%D0%B0%D1%81%D0%BE%D0%B8-%D1%84%D0%B8%D0%BD%D1%86%D0%B5%D1%80%D1%82-2/), [https://portal.fincert.cbr.ru/news/приостановка-доступа-к-лк-асои-финцерт-продуктивного-сегмента-боевая-асои-финцерт-15082020-16082020/](https://portal.fincert.cbr.ru/news/%D0%BF%D1%80%D0%B8%D0%BE%D1%81%D1%82%D0%B0%D0%BD%D0%BE%D0%B2%D0%BA%D0%B0-%D0%B4%D0%BE%D1%81%D1%82%D1%83%D0%BF%D0%B0-%D0%BA-%D0%BB%D0%BA-%D0%B0%D1%81%D0%BE%D0%B8-%D1%84%D0%B8%D0%BD%D1%86%D0%B5%D1%80%D1%82-%D0%BF%D1%80%D0%BE%D0%B4%D1%83%D0%BA%D1%82%D0%B8%D0%B2%D0%BD%D0%BE%D0%B3%D0%BE-%D1%81%D0%B5%D0%B3%D0%BC%D0%B5%D0%BD%D1%82%D0%B0-%D0%B1%D0%BE%D0%B5%D0%B2%D0%B0%D1%8F-%D0%B0%D1%81%D0%BE%D0%B8-%D1%84%D0%B8%D0%BD%D1%86%D0%B5%D1%80%D1%82-15082020-16082020/)).
2. Направлены два бюллетеня (FINCERT-20200730-info, FinCERT-20200601-info).

Начиная с 6 июня 2020 года обновление было доступно на тестовых ресурсах АСОИ ФинЦЕРТ.

С учетом описанной ситуации ясно, что двух месяцев на проведение опытной эксплуатации и адаптации участников обмена оказалось недостаточно, вероятно, данная проблема вызвана состоянием кредитных организаций в условиях ограничений, связанных с коронавирусной инфекцией. В будущем при проведении обновлений АСОИ ФинЦЕРТ и АС «Фид-Антифрод» данный негативный опыт будет учтен.

Отмечается высокая трудоемкость в связи с необходимостью постоянно (по несколько раз в день) проверять личный кабинет и в ручном режиме скачивать фиды. По мнению кредитных организаций, рассылка информации по электронной почте значительно упрощает и ускоряет использование фидов.

Ответ:

Рассылка фидов по электронной почте не является доверенным и безопасным каналом доставки информации. Для обеспечения оперативного получения фидов, сформированных по результатам анализа операций, совершенных без согласия клиентов, в системе начиная с 1 ноября 2018 года имеется механизм скачивания фидов с использованием API (прикладного программного интерфейса). Функционал работы со всеми данными бюллетеней по API был заложен в функционал АСОИ ФинЦЕРТ второй очереди, и с 17 августа 2020 года он доступен для всех участников обмена.

В целях исключения проблем при загрузке фидов в системы кредитных организаций в автоматизированном режиме просим рассмотреть возможность использования кодировки UTF-8 при передаче данных посредством ФАФ, а также увеличения срока уведомления (до 30 дней) о проведении работ по смене сертификатов доступа к ресурсам продуктивного сегмента АСОИ ФинЦЕРТ.

Ответ:

Начиная с 1 ноября 2018 года АС «Фид-Антифрод» использует кодировку UTF-8. В связи с обращениями участников обмена о том, что открытие фидов стандартными средствами не всегда проходит успешно (т.к. csv-файлы фидов не распознаются автоматически как файлы с кодировкой UTF-8, например, Microsoft Excel в случае отсутствия спецсимвола BOM), был предусмотрен вариант использования UTF-8 с BOM. Данный вариант программного обеспечения был размещен в зоне опытной эксплуатации с 1 июля 2020 года. С учетом отсутствия обращений участников во время опытной эксплуатации по этому вопросу данный функционал вошел в обновление, и в настоящее время (с 17 августа 2020 года) АС «Фид-Антифрод» использует кодировку UTF‑8 с BOM (спецсимволы для определения кодировки UTF-8). В соответствии с Вашим предложением, а также появившимися обращениями кредитных организаций 19–20 сентября 2020 года система была обновлена и проведен обратный переход на использование кодировки UTF-8 (без BOM).

Предложение об увеличении срока уведомления (до 30 дней) о проведении работ по смене сертификатов доступа к ресурсам продуктивного сегмента АСОИ ФинЦЕРТ принято, при последующих обновлениях на данную операцию будет предусмотрено 30 дней.

Периодически в фиды добавляются реквизиты крупных публичных компаний, например, операторов связи. При автоматической загрузке реквизитов в систему мониторинга кредитных организаций начинают массово отклоняться легитимные операции клиентов, что вызывает обоснованные претензии с их стороны. Кредитные организации просят автоматизировать процесс на стороне АСОИ ФинЦЕРТ для исключения некорректного добавления в базу индикаторов крупных публичных компаний.

Ответ:

Данное предложение будет учтено при развитии системы. Для более четкого формирования предложения на доработку системы просим прислать контактные данные инициатора и/или более подробное описание желаемой возможности.

При пользовании ФАФ выявляются случаи некорректной записи ИНН клиентов (состоял из набора нулей). Такие записи вызывают сбой при загрузке в системы мониторинга. Кредитные организации просят автоматизировать на стороне АСОИ ФинЦЕРТ проверку на наличие недопустимых значений.

Ответ:

Технологически появление такого значения происходит из-за того, что такой ИНН является валидным (по алгоритму формирования и проверки ИНН) и он был указан кредитной организацией в реквизитах операции без согласия клиента. Данное предложение будет учтено при развитии системы. Для более четкого формирования предложения на доработку системы просим прислать контактные данные инициатора и/или более подробное описание желаемой возможности.

До реализации автоматической блокировки возможности ввода таких значений в соответствии с Вашим обращением на стороне ФинЦЕРТ будет применяться компенсирующая мера по контролю появления в фидах значений ИНН соответственно 0000000000 и 000000000000, а после доработок будет обеспечена невозможность ввода некорректных ИНН.

При получении информации в фидах о своем клиенте кредитные организации ограничивают проведение его расходных операций. При этом при обращении такого клиента с требованием закрыть счет и получить денежные средства кредитная организация не имеет возможности отказать в закрытии счета только на основании полученной информации в фидах. Предлагается в целях противодействия мошенничеству рассмотреть возможность разработки механизма по отказу таким клиентам в закрытии счета до выяснения оснований его попадания в фиды.

Ответ:

Данное предложение будет учтено при развитии системы. Для более четкого формирования предложения на доработку системы просим прислать контактные данные инициатора и/или более подробное описание желаемой возможности.

При заполнении полей инцидентов не предусмотрены все возможные значения показателей, некоторые из полей, помеченные как обязательные, не всегда бывают обязательными. Например, обязательное поле «Атакованные сервисы» – тип атакованного сервиса – обязательно (перечислены значения ДБО, АБС, файловый сервер, электронная почта), при этом при использовании методов социальной инженерии атакованного сервиса нет как такового. Аналогичная ситуация с полем «Вектор инцидента». Также не все возможные варианты предусмотрены в справочнике События вектора EXT – Последствия от реализации компьютерной атаки на клиента участника информационного обмена. Наиболее частые типы инцидентов – это такие инциденты, когда клиент думает, что с его карты списаны денежные средства мошенниками, и пишет заявление в кредитную организацию, а на самом деле никакого мошенничества нет – это сам клиент подписался на платные услуги в сети Интернет и забыл про них или невнимательно читал акцептованные им условия использования сервиса (просмотр фильмов, прослушивание музыки, сервисы знакомств, платные сервисы социальных сетей и т.д.), который в безакцептном порядке списывает ежемесячно абонентскую плату за пользование сервисом.

Ответ:

В данном случае с помощью методов социальной инженерии злоумышленником была предпринята попытка получить персональные данные пользователя, в том числе и банковские. Если клиент вовремя осознал, что злоумышленник хочет получить его конфиденциальные данные, и положил трубку (попытки доступа к ДБО клиента осуществлено не было), то участник информационного обмена в поле «атакованные сервисы» выбирает «иная система». В случае если доступ к ДБО был получен, поле заполняется значением «Клиентская система ДБО».

Для случаев, когда клиент сообщает об операциях без согласия клиента по вопросам «подписок», предусмотрено несколько этапов информирования. В случае если при первичном информировании Банк не выявил факта «подписки», о данном факте можно сообщить в промежуточном или конечном информировании с указанием «неактуальности» ранее направленных операций. Данная информация будет обработана ФинЦЕРТ и принята к сведению.

В личном кабинете несанкционированные списания денежных средств и попытки несанкционированных списаний (когда на самом деле сами списания не удались и мошеннические транзакции не были совершены) никак друг от друга не отличаются, т.е. признака попытки списания просто не предусмотрено, в результате информация об общей сумме несанкционированных списаний не соответствует действительности. При этом кредитные организации обязаны передавать в АСОИ ФинЦЕРТ информацию о попытках несанкционированных списаний денежных средств.

Ответ:

В текущей версии АСОИ ФинЦЕРТ используется временная схема передачи информации о неуспешных попытках проведения операций без согласия (ОБС) клиента, а именно с помощью указания нулевой суммы операции.

Информация о порядке информирования Банка России о попытках несанкционированных списаний будет отражена в новой редакции стандарта Банка России СТО БР БФБО-1.5-2018 «О формах и сроках взаимодействия Банка России с участниками информационного обмена при выявлении инцидентов, связанных с нарушением требований к обеспечению защиты информации».

Возникают сложности при заполнении электронной формы инцидента, отсутствуют подсказки для заполнения полей, а также по форматам вводимых данных.

Ответ:

Данное предложение будет учтено при развитии системы. Для более четкого формирования предложения на доработку системы просим прислать контактные данные инициатора и/или более подробное описание желаемой возможности.

Отсутствует возможность загрузки текстовой информации из файлов в отдельные сегменты запросов и расчета хэш в системе (паспорт, СНИЛС).

Ответ:

Данное предложение будет учтено при развитии системы. Для более четкого формирования предложения на доработку системы просим прислать контактные данные инициатора и/или более подробное описание желаемой возможности. Однако следует отметить, что наиболее технологичным решением является направление информации автоматизированным способом с использованием API (это также позволяет снизить нагрузку на операторов и избежать ошибки при заполнении данных).

Нет функционала по копированию ранее внесенных данных – приходится каждый раз при заполнении инцидента вносить данные вручную, хотя на практике бывает множество операций по одинаковым реквизитам.

Ответ:

Данное предложение будет учтено при развитии системы. Для более четкого формирования предложения на доработку системы просим прислать контактные данные инициатора и/или более подробное описание желаемой возможности. Однако следует отметить, что наиболее технологичным решением является направление информации автоматизированным способом с использованием API (это также позволяет снизить нагрузку на операторов и избежать ошибки при заполнении данных).

Отсутствует единый справочник систем электронных кошельков, что не позволяет в полном объеме настроить обработку платежей по данному параметру.

Ответ:

Данное предложение будет учтено при развитии системы. Для более четкого формирования предложения на доработку системы просим прислать контактные данные инициатора и/или более подробное описание желаемой возможности.

Неудобно просматривать список операций: раньше они отображались как вложение в задаче, а сейчас идут сплошным списком без разграничений, стало сложно визуально сверять правильность реквизитов.

Ответ:

Данное предложение будет учтено при развитии системы. Для более четкого формирования предложения на доработку системы просим прислать контактные данные инициатора и/или более подробное описание желаемой возможности.

Возникают сложности при поиске по инцидентам – необходимо знать его точный номер. Кредитные организации предлагают доработать систему поиска: разделить входящие/исходящие, отвеченные/неотвеченные, фильтровать по дате, искать по ИНН, номеру счета и т.п.

Ответ:

Данное предложение будет учтено при развитии системы. Для более четкого формирования предложения на доработку системы просим прислать контактные данные инициатора и/или более подробное описание желаемой возможности.

Недостаточно прозрачен процесс проставления в форме инцидента «Помощь требуется». Кредитные организации просят формализовать этот вопрос и отразить его в соответствующей документации.

Ответ:

Флаг «Помощь требуется» проставляется участником в случаях, когда необходимо оказание содействия ФинЦЕРТ в анализе произошедшего инцидента и/или получение рекомендаций в части противодействия выявленной атаке.

Информация о порядке применения/неприменения флага «Помощь требуется» указана для операций без согласия во Временной инструкции по заполнению карточки инцидента для операций без согласия клиента ([https://portal.fincert.cbr.ru/Content/1132/инструкция-по-заполнению-карточки-инцидента.pdf](https://portal.fincert.cbr.ru/Content/1132/%D0%B8%D0%BD%D1%81%D1%82%D1%80%D1%83%D0%BA%D1%86%D0%B8%D1%8F-%D0%BF%D0%BE-%D0%B7%D0%B0%D0%BF%D0%BE%D0%BB%D0%BD%D0%B5%D0%BD%D0%B8%D1%8E-%D0%BA%D0%B0%D1%80%D1%82%D0%BE%D1%87%D0%BA%D0%B8-%D0%B8%D0%BD%D1%86%D0%B8%D0%B4%D0%B5%D0%BD%D1%82%D0%B0.pdf)).

Информация о порядке применения флага «Помощь требуется» будет отражена в новой редакции стандарта Банка России СТО БР БФБО-1.5-2018 «О формах и сроках взаимодействия Банка России с участниками информационного обмена при выявлении инцидентов, связанных с нарушением требований к обеспечению защиты информации».

При использовании API для взаимодействия с АСОИ ФинЦЕРТ созданы сложные форматы обмена, из-за этого возникают ошибки. При обновлении появляются новые опции для отчета об инцидентах, но новые инструкции и новые спецификации в кредитные организации не предоставляются.

Ответ:

Вся необходимая участникам информация размещается на инфопортале АСОИ ФинЦЕРТ, доступном всем участникам обмена. На инфопортале размещается следующая информация об АСОИ ФинЦЕРТ и АС «Фид-Антифрод»:

текущий режим функционирования и информация о плановых работах в АСОИ ФинЦЕРТ и АС «Фид-Антифрод»;

документация на системы в части, передаваемой участникам обмена и разработчикам;

информация по использованию API;

порядок подключения и использования системы;

часто задаваемые вопросы/ответы (FAQ) и другая справочная информация.

С учетом вышеуказанного полагаем, что часть участников, уведомивших Ассоциацию, не ознакомилась с информацией, представленной на инфорпортале. Если со стороны Ассоциации есть предложения по ее дополнению, готовы рассмотреть конкретные предложения.

При взаимодействии через API с АСОИ ФинЦЕРТ необходимо указывать, кем является получатель: юридическим или физическим лицом. У кредитных организаций и на портале нет спецификаций, по которым можно было бы автоматически сформировать нужный ответ. В связи с этим возникают ситуации, когда при указании ИНН юридического лица возвращается результат с необходимостью указания хэш паспорта физического лица.

Ответ:

Вся необходимая участникам информация размещается на инфопортале АСОИ ФинЦЕРТ, доступном всем участникам обмена. На инфопортале размещается следующая информация об АСОИ ФинЦЕРТ и АС «Фид-Антифрод»:

текущий режим функционирования и информация о плановых работах в АСОИ ФинЦЕРТ и АС «Фид-Антифрод»;

документация на системы в части, передаваемой участникам обмена и разработчикам;

информация по использованию API;

порядок подключения и использования системы;

часто задаваемые вопросы/ответы (FAQ) и другая справочная информация.

С учетом вышеуказанного полагаем, что часть участников, уведомивших Ассоциацию, не ознакомилась с информацией, представленной на инфорпортале.

После обновления в конце 2019 года некоторые кредитные организации не могут отчитываться об операциях по кредитным счетам, приходят ежедневные уведомления об ошибке (из-за того, что больше нельзя указывать «/» в номере счета).

Ответ:

В настоящее время информирование по инцидентам построено на основе стандарта Банка России СТО БР БФБО-1.5-2018 «О формах и сроках взаимодействия Банка России с участниками информационного обмена при выявлении инцидентов, связанных с нарушением требований к обеспечению защиты информации». Использование символа «/» в номере счета не предусмотрено стандартом, однако с учетом потребности данное предложение будет рассмотрено при корректировке нормативной базы и развитии систем АСОИ ФинЦЕРТ и АС «Фид-Антифрод».

Отсутствует утвержденная дорожная карта/план мероприятий по развитию ФАФ, что препятствует повышению степени автоматизации использования индикаторов из этой подсистемы.

Ответ:

Данное предложение будет учтено при развитии систем АСОИ ФинЦЕРТ и АС «Фид-Антифрод». Однако следует отметить, что для использования индикаторов (фидов) из системы АС «Фид-Антифрод» (в контексте письма упомянутой как ФАФ) технологичным решением является получение фидов с использованием API, данный функционал доступен с ноября 2018 года, порядок его использования описан в документации, размещенной на инфопортале.

Необходима доработка АСОИ ФинЦЕРТ в части обработки информации об инцидентах, возникших при использовании СБП. Предлагается в способе реализации сразу выбирать «Система быстрых платежей», а не «Телефон», описать способ реализации «Система быстрых платежей» с детальной инструкцией по заполнению полей, а также перенести поле уникального идентификатора операции из раздела «Дополнительно» в форму инцидента.

Ответ:

В настоящее время информирование по инцидентам построено на основе стандарта Банка России СТО БР БФБО-1.5-2018 «О формах и сроках взаимодействия Банка России с участниками информационного обмена при выявлении инцидентов, связанных с нарушением требований к обеспечению защиты информации», не предполагающего выбор одновременно двух типов атаки. Данное предложение будет рассмотрено при корректировке нормативной базы и развитии систем АСОИ ФинЦЕРТ и АС «Фид-Антифрод». Для более четкого формирования предложения на доработку системы просим прислать контактные данные инициатора и/или более подробное описание желаемой возможности.

Ввиду отсутствия в нормативных документах описания процедуры исключения из базы данных ФинЦЕРТ информации о клиенте по инициативе кредитной организации, в которой он обслуживается (так называемый процесс «обеления клиентов»), в случае если эта процедура будет осуществляться через АСОИ ФинЦЕРТ, кредитные организации просят пояснить механизм ее работы.

Ответ:

Данное предложение будет рассмотрено при корректировке нормативно-методической базы и развитии АС «Фид-Антифрод».

Кредитные организации также просят по возможности ускорить процесс перехода на отчет об инцидентах исключительно через автоматизированную систему обработки инцидентов Центра мониторинга и реагирования на компьютерные атаки в кредитно-финансовой сфере (далее – АСОИ ФинЦЕРТ), что позволит отменить обязательность предоставления отчетности по форме 0403203 «Сведения о событиях, связанных с нарушением защиты информации при осуществлении переводов денежных средств» (далее – форма отчетности 0403203) и сократить издержки кредитных организаций на составление отчетности.

Ответ:

В настоящее время Банк России осуществляет доработку формы отчетности 0403203, в которой будет учтен переход на информирование Банка России об инцидентах через АСОИ ФинЦЕРТ.

18% опрошенных кредитных организаций сообщили о следующих трудностях при предоставлении информации в рамках отчетности по форме 040323, в частности:

согласно пункту 6.2 методики составления отчетности в графе 3 строки 5 указывается общая сумма денежных средств, переведенных (списанных) с банковских счетов клиентов при использовании всех типов электронных средств платежа. Просим пояснить, каким образом следует учитывать суммы по операциям с полным/ частичным возвратом, переводы между счетами одного клиента внутри кредитной организации (в том числе с целью погашения кредита), опротестованные в платежных системах операции и другие подобные операции.

Ответ:

В соответствии с пунктом 6.2 методики составления отчетности по форме 0403203 Указания Банка России от 9 июня 2012 года № 2831-У «Об отчетности по обеспечению защиты информации при осуществлении переводов денежных средств операторов платежных систем, операторов услуг платежной инфраструктуры, операторов по переводу денежных средств» в графе 3 строки 5 указывается общая сумма денежных средств, переведенных (списанных) с банковских счетов клиентов при использовании всех типов электронных средств платежа, в которую необходимо включать сумму всех операций по переводу, по которым наступила окончательность перевода денежных средств в соответствии с пунктом 16 статьи 3 Федерального закона от 27 июня 2011 года № 161-ФЗ «О национальной платежной системе».

В подразделе 2.1 необходимо указать «количество событий, связанных с получением уведомлений от клиентов, из них в результате побуждения клиентов к совершению операции путем обмана или злоупотребления доверием». Данный подвид операций не предусмотрен в АСОИ ФинЦЕРТ, соответственно в системах учета инцидентов кредитных организаций приходится вести раздельный учет инцидентов, когда хищение произошло без ведома клиентов и когда они сами совершали операцию путем обмана или злоупотребления доверием.

Ответ:

Значение показателя «Количество событий, связанных с получением уведомлений от клиентов, из них в результате побуждения клиентов к совершению операции путем обмана или злоупотребления доверием» в форме отчетности 0403203 предусмотрено АСОИ ФинЦЕРТ как идентификатор блока данных «социальная инженерия» в соответствии с пунктом 12.3.3 стандарта 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».

Кроме того, кредитные организации направили вопросы по заполнению отчетности по форме 040323:

Для занесения сведений об инцидентах в отчет необходимо предварительно конвертировать сумму денежного перевода из валюты в рубли. Какую сумму необходимо вносить в отчет: по курсу валют на дату списания или дату авторизации?

Ответ:

В случае возникновения необходимости конвертации суммы денежных средств из валюты в рубли при заполнении формы отчетности 0403203 указывается сумма по курсу на дату авторизации.

В случае инцидента с несанкционированным списанием средств у клиента с использованием реквизитов карты в сети «Интернет» и посредством системы ДБО в отчете заполняются строки 2 и 3 (или 4, если использовалось ДБО юридических лиц) подраздела 2.1. Как в таком случае заносить инцидент в отчет, если уведомление от клиента получено одно, но инцидент можно занести сразу в две строки?

Ответ:

В случае заполнения информации об инциденте, содержащем уведомление от клиентов об использовании электронных средств платежа без их согласия с использованием реквизитов платежной карты при оплате товаров и услуг через информационно-телекоммуникационную сеть «Интернет» и посредством системы дистанционного банковского обслуживания (ДБО), в форме отчетности 0403203 заполняется только строка 2 подраздела 2.1.

Какую сумму следует указать в столбце 6 подраздела 2.1 («Сумма денежных средств, в отношении которой получены уведомления от клиентов, тыс. руб.), когда клиент сообщил о неудачных попытках списания денежных средств? Какую сумму указывать в столбце 7 подраздела 2.1. («Сумма денежных средств, возмещенная (возвращенная) клиентам, тыс. руб.»), в случае если фактического списания денежных средств не произошло?

Ответ:

В графах 6 и 7 подраздела 2.1 формы отчетности 0403203 указывается сумма денежных средств (в отношении которой получены уведомления от клиентов и которая возмещена (возвращена) клиентам) по операциям, по которым наступила окончательность перевода денежных средств в соответствии с пунктом 16 статьи 3 Федерального закона от 27 июня 2011 года № 161-ФЗ «О национальной платежной системе», при этом попытки списания не учитываются.

Какую сумму следует указать в столбце 6 подраздела 2.1 («Сумма денежных средств, в отношении которой получены уведомления от клиентов, тыс. руб.), когда клиент сообщил о несанкционированном переводе денежных средств с одного счета на другой, при условии, что оба счета принадлежат клиенту и открыты в одном банке? Какую сумму указывать в столбце 7 подраздела 2.1 («Сумма денежных средств, возмещенная (возвращенная) клиентам, тыс. руб.»), в случае если фактического списания денежных средств не произошло (например, при своевременном реагировании и остановке платежа перед выводом на сторонний счет)?

Ответ:

В графах 6 и 7 подраздела 2.1 формы отчетности 0403203 указывается сумма денежных средств (в отношении которой получены уведомления от клиентов и которая возмещена (возвращена) клиентам) по операциям, по которым наступила окончательность перевода денежных средств в соответствии с пунктом 16 статьи 3 Федерального закона от 27 июня 2011 года № 161-ФЗ «О национальной платежной системе», независимо от принадлежности счета клиента.

Необходимо ли в строке 1 подраздела 2.1 («Платежные карты (за исключением предоплаченных платежных карт) при использовании непосредственно в банкоматах, электронных терминалах, импринтерах») учитывать уведомления о невыдаче денежных средств в банкоматах, в том числе сторонних банков?

Ответ:

В строке 1 подраздела 2.1 формы отчетности 0403203 учитывать уведомления о невыдаче денежных средств в банкоматах, в том числе сторонних банков, не требуется.

Необходимо ли вносить в отчет информацию об операциях, которые изначально расценивались как несанкционированные, но в процессе расследования операции были признаны клиентом как легитимные?

Ответ:

В форму отчетности 0403203 необходимо вносить информацию обо всех операциях, связанных с получением уведомлений от клиентов, по которым наступила окончательность перевода денежных средств, независимо от результатов расследования.

Необходимо ли в сумме оспариваемой операции указывать комиссию?

Ответ:

В случае если в состав операции по переводу денежных средств без согласия клиента входит комиссия, она указывается в сумме указанной операции.