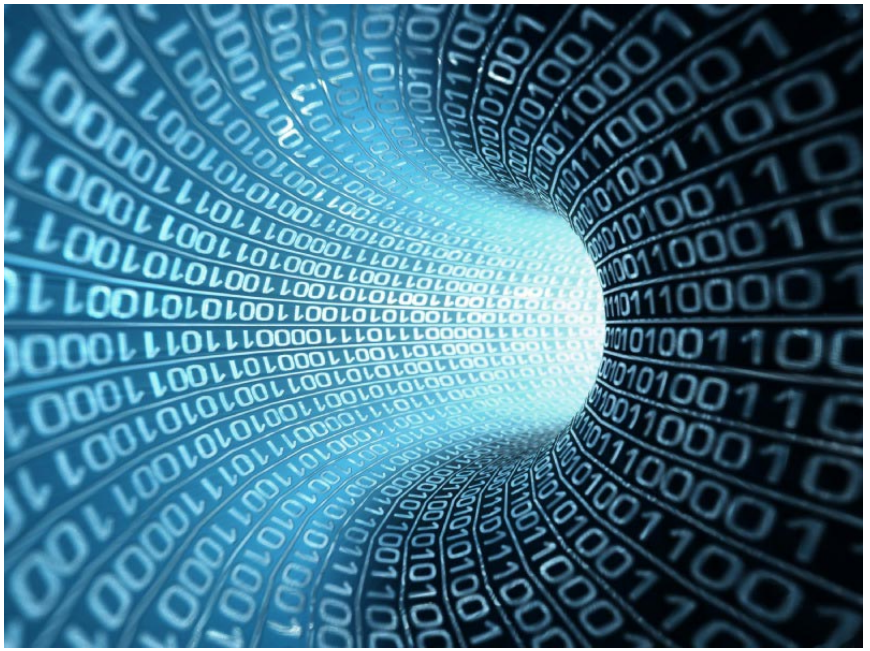
Система антифрода в банке: требования регулятора эффективность противодействия экономическая эффективность

Как сдвинуть воз?



АНДРЕЙ ЛУЦКОВИЧ
ГЕНЕРАЛЬНЫЙ ДИРЕКТОР,
ООО ФРОДЕКС
e-mail: **ceo@frodex.ru**

ФРОДЕКС | эффективные технологии противодействия мошенничеству

Федеральный закон от 27.06.2018 N 167-ФЗ "О внесении изменений в отдельные законодательные акты Российской Федерации в части противодействия хищению денежных средств

- обязал информировать Банк России об инцидентах

- закрепил за ЦБ роль по установке требований к ЗИ для противодействия мошенничеству

- регламентировал процедуры (выявление/ приостановка/подтверждение)

Операторы обязаны:

1. Реализовать меры по противодействию мошенничеству

2. Направлять информацию обо всех случаях и/или попытках

Операторы в праве

получать от Банка России информацию, содержащуюся в базе данных о случаях и попытках осуществления переводов денежных средств без согласия клиента

ФРОДЕКС | эффективные технологии противодействия мошенничеству

РЕАЛИЗАЦИЯ МЕР

1. **Определение соответствия признакам определенным банком России**

2. Приостановка платежа (до списания) до 2-х рабочих дней

3. Запрос у клиента подтверждения платежа

4. Приостановка использования клиентом электронного средства платежа

Отечественная новейшая история борьбы с мошенничеством

1. Активное противодействие было только от самых страдающих

2. Начальная стадия эволюция методов борьбы и выявления

3. Попытки объединения усилий противодействия

Особенности законодательства

1. Не делаются различия в типе клиента юрики/физики

2. Не ограничиваются системы выполнения перевода средств

3. Наблюдается интеграция требований от разных направлений (атифрод, ПОД/ФТ)

ФРОДЕКС | эффективные технологии противодействия мошенничеству

Необходим КОМПЛЕКСНЫЙ подход

Предотвращение кражи средств в системах ДБО

ПОД/ФТ

Борьба с внутренним мошенничеством (платежи в АБС)

Предотвращение кражи средств через АРМ КБР

Требования регулятора

ФРОДЕКС | эффективные технологии противодействия мошенничеству

Признаки осуществления перевода денежных средств без согласия клиента

1. Черный список получателя средств

2. Совпадение информации о параметрах устройства

3. Несоответствие операции обычно совершаемым клиентом

Черный список получателя средств

1. Совпадение информации о получателе средств с информацией о получателе средств по переводам денежных средств без согласия клиента, полученной из базы данных о случаях и попытках осуществления перевода денежных средств без согласия клиента, формируемой Банком России в соответствии с частью 5 статьи 27 Федерального закона от 27 июня 2011 года № 161-ФЗ «О национальной платежной системе» (далее – база данных).

«Живые» черные списки, актуальные для систем ДБО

Антидроп – клуб
(межбанковский обмен по e-mail)

- **автоматический** импорт данных о мошенниках, передаваемых в Excel-файлах (сразу же при получении письма)
- **автоматическая** корректировка значений полей из-за «умного» редактора Excel
- формирование Excel-файла в формате обмена антидроп-клуба

Fraudmonitor
(разработчик: Group-IB)

- **автоматический** импорт данных о мошенниках, зарегистрированных в базе Fraudmonitor (ежечасно)
- **автоматическая** передача данных в Fraudmonitor о мошенниках, выявленных в банке (по желанию банка)
- выявление реального получателя из полей (если он указан в назначении)

все автоматизировано – участия человека не требуется!

ЦЕНТРАЛЬНЫЙ БАНК РОССИЙСКОЙ ФЕДЕРАЦИИ (БАНК РОССИИ)

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

Дата введения: 2018-11-01

Издание официальное

Эффективность противодействия

ФРОДЕКС | эффективные технологии противодействия мошенничеству

Совпадение информации о параметрах устройства

2. Совпадение информации о параметрах устройств, с использованием которых осуществлен доступ к автоматизированной системе, программному обеспечению с целью осуществления перевода денежных средств, с информацией о параметрах устройств, с использованием которых был осуществлен доступ к автоматизированной системе, программному обеспечению с целью осуществления перевода денежных средств без согласия клиента, полученной из базы данных.

Несоответствие операции обычно совершаемым клиентов

2. Фиды собираются по атрибутам получателей в рамках операции без согласия.
Список атрибутов операций:

- **a. хэш паспорта получателя,**
- **b. хэш снилс получателя,**
- **c. инн получателя,**
- **d. номер телефона получателя**
- **e. БИК + лицевой счет получателя**
- **f. номер карты получателя**
- **g. номер кошелька получателя + эмитент кошелька**

Несоответствие операции обычно совершаемым клиентом

3. Несоответствие характера, и (или) параметров, и (или) объема проводимой операции (время (дни) осуществления операции, место осуществления операции, устройство, с использованием которого осуществляется операция и параметры его использования, сумма осуществления операции, периодичность (частота) осуществления операций, получатель средств) операциям, обычно совершаемым клиентом оператора по переводу денежных средств (осуществляемой клиентом деятельности).

Несоответствие операции обычно совершаемым клиентом

Описание встроенных правил антифрод-системы FraudWall (на 14 ноября 2018г.):

Правило (№ и описание)	Уровень встроенных правил	Диапазон сумм активации проверки правила	Доступность правила для типа антифрода		
			Антифрод для ЮЛ	Внутренний антифрод	Антифрод для ФЛ
Правила, применяемые только к плательщикам, в свойствах которых указано «только персональный белый список»					
183 (проверка по 167-ФЗ) - "Получатель не находится в персональном белом списке плательщика"	Проверка по 167-ФЗ	К данным правилам НЕ применяются диапазоны сумм из настроек «Система» → «Профили	+	+	+

Автоматизация процессов подтверждения платежа клиентом

Экономическая эффективность

Аутсорсинг процессов противодействия мошенничеству

1. **Аутсорсинг логики обнаружения**

2. **Системо и канало независимость**

3. **Аусорсинг процессов**

Спасибо, за внимание!

АНДРЕЙ ЛУЦКОВИЧ
ГЕНЕРАЛЬНЫЙ ДИРЕКТОР,
ООО ФРОДЕКС
e-mail: **ceo@frodex.ru**

ФРОДЕКС | эффективные технологии противодействия мошенничеству