Защита финансовой информации

написано GlobalTrust.ru | 20.08.2023

Требования Банка России, предъявляемым к финансовым организациям

Компания GlobalTrust реализует комплекс услуг по обеспечению соответствия кредитных и некредитных финансовых организаций, включая операторов платежных систем, требованиям по обеспечению информационной безопасности, установленных Банком России.

Требования по обеспечению информационной безопасности и операционной надежности для кредитных организаций устанавливаются следующими положениями Банка России:

- Положение Банка России от 17 апреля 2019 г. № 683-П “Об установлении обязательных для кредитных организаций требований к обеспечению защиты информации при осуществлении банковской деятельности в целях противодействия осуществлению переводов денежных средств без согласия клиента”.
- Положение Банка России от 25 июня 2020 г. № 716-П “О требованиях к системе управления операционным риском в кредитной организации и банковской группе”
- Положение Банка России от 12 января 2022 г. № 787-П “Об обязательных для кредитных организаций требованиях к операционной надежности при осуществлении банковской деятельности в целях обеспечения непрерывности оказания банковских услуг”

Требования по обеспечению информационной безопасности и операционной надежности для некредитных финансовых организаций устанавливаются следующими положениями Банка России:

- Положение Банка России от 20 апреля 2021 г. № 757-П “Об установлении обязательных для некредитных финансовых организаций требований к обеспечению защиты информации при осуществлении деятельности в сфере финансовых рынков в целях противодействия осуществлению незаконных финансовых операций”
- Положение Банка России от 8 апреля 2022 г. № 779-П “Об установлении обязательных для некредитных финансовых организаций требований к операционной надежности при осуществлении видов деятельности, предусмотренных частью первой статьи 761 Федерального закона от 10 июля 2002 года № 86-ФЗ “О Центральном банке Российской Федерации (Банке России)”, в целях обеспечения непрерывности оказания финансовых услуг (за исключением банковских услуг)”

Требования по обеспечению защиты информации при осуществлении переводов денежных средств устанавливаются следующими положениями Банка России:

- Положение Банка России от 5 октября 2020 г. № 719-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”

Организации, реализующие усиленный и стандартный уровень защиты информации, должны осуществлять **тестирование объектов информационной инфраструктуры на предмет проникновений и анализ уязвимостей ИБ**.

Организации, реализующие усиленный и стандартный уровни защиты информации, должны обеспечить использование для осуществления финансовых операций прикладного ПО АС и приложений сертифицированных в системе сертификации ФСТЭК России на соответствие требованиям по безопасности информации, в том числе на наличие уязвимостей или недекларированных возможностей, или в отношении которых проведен анализ уязвимостей по требованиям к оценочному уровню доверия не ниже

чем **ОУД 4, предусмотренного пунктом 7.6 национального стандарта РФ 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»**.

Кроме этого, финансовые организации, реализующие усиленный и стандартный уровни защиты информации, должны информировать Банк России:

- О выявленных инцидентах защиты информации, включенных в перечень типов инцидентов
- О планируемых мероприятиях, включая выпуск пресс-релизов и проведение пресс-конференций, размещение информации на официальных сайтах в сети «Интернет», в отношении инцидентов защиты информации не позднее одного рабочего дня до дня проведения мероприятия

Требования ГОСТ Р 57580.1-2017

Защита информации в отношении автоматизированных систем, программного обеспечения, средств вычислительной техники, телекоммуникационного оборудования в финансовых организациях должна осуществляться в соответствии с требованиями национального стандарта РФ ГОСТ Р 57580.1-2017 «Безопасность финансовых (банковских) операций. Защита информации финансовых организаций. Базовый состав организационных и технических мер».

Оценка определенного уровня защиты информации должна осуществляться в соответствии с требованиями национального стандарта РФ ГОСТ Р 57580.2-2018 «Безопасность финансовых (банковских) операций. Защита информации финансовых организаций. Методика оценки соответствия».

Перечни защищаемой информации

В указанных Положениях определены перечни защищаемой информации и

требования по защите информации в отношении объектов информационной инфраструктуры, прикладного ПО, технологии обработки защищаемой информации. Требования дифференцированы в зависимости от применяемого к организации уровня защиты информации.

Кредитные организации должны осуществлять защиту следующей информации, подготавливаемой, обрабатываемой и хранимой в автоматизированных системах, входящих в состав объектов информационной инфраструктуры и используемых для осуществления банковских операций, связанных с осуществлением перевода денежных средств:

- Информации, содержащейся в документах, составленных при осуществлении банковских операций в электронном виде (далее — электронные сообщения), формируемых работниками кредитных организаций (далее — работники) и (или) клиентами кредитных организаций (далее — клиенты)
- Информации, необходимой для авторизации клиентов при совершении действий в целях осуществления банковских операций и удостоверения права клиентов распоряжаться денежными средствами
- Информации об осуществленных банковских операциях
- Ключевой информации средств криптографической защиты информации (далее — СКЗИ), используемой при осуществлении банковских операций (далее — криптографические ключи)

Некредитные финансовые организации должны осуществлять защиту следующей информации, получаемой, подготавливаемой, обрабатываемой, передаваемой и хранимой в автоматизированных системах:

- Информации, содержащейся в документах, составляемых при осуществлении финансовых операций в электронном виде работниками НФО и (или) клиентами НФО
- Информации, необходимой НФО для авторизации своих клиентов в целях осуществления финансовых операций и удостоверения права клиентов распоряжаться денежными средствами, ценными бумагами

или иным имуществом
- Информации об осуществленных НФО и их клиентами финансовых операциях
- Ключевой информации средств криптографической защиты информации (далее — СКЗИ), используемой НФО и их клиентами при осуществлении финансовых операций (далее — криптографические ключи)

В случае если защищаемая информация содержит персональные данные, финансовые организации должны применять меры по обеспечению безопасности персональных данных при их обработке в соответствии со статьей 19 Федерального закона от 27 июля 2006 года № 152-ФЗ «О персональных данных».

Обеспечение соответствия финансовых организаций требованиям Банка России

Обеспечение соответствия финансовых организаций требованиям Банка России включает в себя решение следующих задач:

- Оценка соответствия организации требованиям Положений Банка России
- Оценка соответствия организации требованиям национального стандарта РФ ГОСТ Р 57580.1-2017 «Безопасность финансовых (банковских) операций. Защита информации финансовых организаций. Базовый состав организационных и технических мер».
- Тестирование объектов информационной инфраструктуры организации на предмет проникновений и анализ уязвимостей ИБ.
- Оценка соответствия организации требованиям Федерального закона РФ № 152-ФЗ и Положения Правительства РФ № 1119 (**в случае если защищаемая информация содержит персональные данные**).
- Анализ уязвимостей прикладного ПО по требованиям к оценочному уровню доверия не ниже чем ОУД 4, предусмотренного пунктом 7.6 национального стандарта РФ 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» (**в случае отсутствия сертификации данного ПО в системе сертификации ФСТЭК России на соответствие требованиям по безопасности информации**).
- Разработка рекомендации и плана мероприятий по обеспечению соответствия организации требованиям Положения Банка России.
- Реализация комплекса организационно-технических мероприятий по приведению организации в соответствии с требованиями, установленными Банком России.

Обеспечение соответствия платежных систем требованиям Банка России

Согласно Федерального закона № 161-ФЗ “О национальной платежной системе” ст. 27 участники национальной платежной системы (операторы по переводу денежных средств, банковские платежные агенты, операторы платежных систем, операторы услуг платежной инфраструктуры) должны обеспечить:

- Защиту информации о средствах и методах обеспечения информационной безопасности, персональных данных и об иной информации, подлежащей обязательной защите в соответствии с законодательством РФ
- Защиту информации при осуществлении переводов денежных средств в соответствии с установленными Банком России требованиями

Согласно Постановление Правительства РФ № 584 “Об утверждении Положения о защите информации в платежной системе” операторами платежных систем должны быть реализованы правовые, организационные и технические меры, направленные:

- На обеспечение защиты информации от неправомерного доступа, уничтожения, модифицирования, блокирования, копирования, предоставления и распространения, а также от иных неправомерных

действий в отношении информации
- На соблюдение конфиденциальности информации
- На реализацию права на доступ к информации в соответствии с законодательством РФ

Комплекс услуг GlobalTrust по обеспечению информационной безопасности платежных систем в соответствии с требованиями 161-ФЗ и принятыми на его основе нормативными документами по защите информации включает в себя следующее:

1. Оценка соответствия платежной системы требованиям по безопасности информации и разработка плана мероприятий по обеспечению соответствия:

- Сбор и анализ свидетельств аудита
- Анализ документации организации и бизнес-процессов, в части функционирования платежной системы
- Интервьюирование представителей организации
- Анализ полноты и эффективности реализуемых мер по защите информации
- Оценка выполнения требований
- Вычисление обобщающих показателей соответствия и итогового показателя соответствия
- Документирование результатов оценки соответствия
- Разработка плана организационно-технических мероприятий по обеспечению соответствия платежной системы требованиям по безопасности информации

2. Анализ защищенности платежной системы

- Идентификация и анализ организационных уязвимостей ИБ платежной системы
- Идентификация и анализ технических уявзвимостей ИБ платежной

системы для внешнего периметра корпоративной сети и внутренний ИТ-инфраструктуры
- Анализ защищенности программных модулей и сервисов платежной системы
- Оценка уровня защищенности платежной системы
- Разработка рекомендаций по повышению уровня защищенности платежной системы и совершенствованию механизмов защиты

3. Оценка и обработка рисков информационной безопасности платежной системы

- Инвентаризация активов платежной системы
- Разработка моделей угроз и нарушителей информационной безопасности платежной системы
- Оценка информационных активов, угроз, уязвимостей и механизмов контроля ИБ платежной системы
- Формирование реестра информационных рисков платежной системы
- Определение допустимого уровня остаточных рисков
- Подготовка и согласование решений по обработки рисков платежной системы
- Разработка и согласование плана обработки рисков платежной системы

4. Разработка комплекса организационно-распорядительных документов для обеспечения соответствия платежной системы организации требованиям по безопасности информации

- Определение требований к процессам обеспечения информационной безопасности в платежной системе
- Определение ролей и ответственности персонала

- Определение порядка взаимодействия между подразделениями для реализации мер по защите информации в платежной системе
- Разработка и согласование проектов организационно-распорядительных документов по обеспечению информационной безопасности платежной системы

5. Разработка и внедрение технических решений по комплексу программно-технических средств защиты информации в платежной системе

- Проектирование архитектуры обеспечения ИБ платежной системы
- Выбор основных технических решений по защите информации в платежной системе
- Определение состава сертифицированных СЗИ по каждой подсистеме защиты и анализ их технической совместимости
- Разработка проектной документации, описание процессов и механизмов функционирования СЗИ
- Поставка и внедрение СЗИ
- Проведение приемо-сдаточных испытаний подсистемы информационной безопасности платежной системы
- Проведение аттестационных испытаний платежной системы по требованиям безопасности информации (опционально)

Заказ услуг

- по телефону: +7 (925) 203-95-11
- по e-mail: info@globaltrust.ru
- через web-форму