Подробнее о 684-П

На какие организации распространяется?

Положение Банка России от 17.04.2019 №684-П (далее – 684-П) распространяется на все некредитные финансовые организации.
Большая часть требований, установленных 684-П, распространяется только на некредитные финансовые организации, реализующие усиленный или стандартный уровень защиты информации, предусмотренный ГОСТ Р 57580.1 (далее – усиленный или стандартный уровень защиты информации).

В отношении каких объектов применяются требования?

Под требования 684-П попадают автоматизированные системы, используемые некредитными финансовыми организациями для осуществления финансовых операций.

На какую информацию распространяются требования?

1. информация, содержащаяся в документах, составленных при осуществлении финансовых операций в электронном виде, формируемых работниками и (или) клиентами некредитных финансовых организаций;
2. информация, необходимая для авторизации клиентов при совершении действий в целях осуществления финансовых операций и удостоверения права клиентов распоряжаться имуществом;
3. информация об осуществленных финансовых операциях;
4. ключевая информация СКЗИ, используемая при осуществлении финансовых операций.

Какие требования 684-П нужно выполнять некредитным финансовым организациям, для которых не установлена обязательная необходимость реализации усиленного или стандартного уровня?

Некредитные финансовые организации, для которых не установлена обязательная необходимость реализации усиленного или стандартного уровня, следует выполнить следующие действия:

- сформировать и довести до клиентов рекомендации по защите информации;
- обеспечить защиту информации с помощью СКЗИ в соответствии с технической документацией на СКЗИ и требованиями нормативных актов;
- принять решение о необходимости проведения сертификации или анализа уязвимостей в отношении программного обеспечения и приложений.

С 01.01.2021 каждая некредитная финансовая организация должна ежегодно определять применимый к ней в течение календарного года уровень защиты информации, предусмотренный ГОСТ Р 57580.1. При этом некредитные организации, для которых не установлена обязательная необходимость реализации усиленного или стандартного уровня защиты информации, могут принять решение об отсутствии необходимости реализовывать один из уровней защиты, определенный в ГОСТ Р 57580.1.

USSC.RU