Мероприятия, направленные на повышение уровня защищенности объектов инфраструктуры

В соответствии с рекомендациями Банка России для повышения уровня защищенности объектов инфраструктуры юридических лиц, являющихся клиентами кредитных организаций, рекомендуется:

– использовать решения для мониторинга и выявления киберугроз и оперативного реагирования на инциденты (MDR-решений);
– с помощью аппаратных или программных средств сетевой защиты (Firewall, корпоративные прокси-серверы) ограничить доступ в сеть «Интернет». Маршрутизировать трафик таким образом, чтобы разрешать соединения только с доверенными ресурсами;
– не допускать использования работниками организации рабочих устройств для личного использования, в том числе посещения развлекательных ресурсов, личной электронной почты или общения в мессенджерах;
– с учетом перехвата вредоносным программным обеспечением SMS-сообщений, по возможности использовать в качестве второго фактора подтверждения операции протокол TOTP;
– соблюдать требования безопасности при эксплуатации аппаратного ключа (токена), производить его извлечение из USB-порта сразу после подписания платежных поручений.

При выявлении инцидентов информационной безопасности рекомендуется:

– не перезагружать компьютер, не запускать антивирусные решения, извлечь токены доступа и съемные носители информации;
– отключить устройство от локальной сети и сети Интернет;
– выполнить процедуры создания образов оперативной памяти и жесткого диска с использованием специализированного программного обеспечения для дальнейшего проведения расследования;
– сохранить образец вредоносного программного обеспечения для проведения анализа и последующей передачи его в Банк (в рамках анализа компьютерного инцидента);
– в случае заражения мобильного устройства, включить авиа-режим и извлечь SIM-карту. Если в устройстве используется электронная сим-карта, допустимо выключить устройство. Не рекомендуется сбрасывать устройство до заводских настроек, так как это приведет к удалению следов вредоносной активности и затруднит дальнейшее проведение расследования.