Проект

ПРАВИТЕЛЬСТВО РОССИЙСКОЙ ФЕДЕРАЦИИ

ПОСТАНОВЛЕНИЕ

от ___ _____г. №____

МОСКВА

Об утверждении Положения
о защите информации в национальной платежной системе

В соответствии со статьей 27 Федерального закона «О национальной платежной системе» (Собрание законодательства Российской Федерации 2011, № 27, ст. 3872) Правительство Российской Федерации **п о с т а н о в л я е т:**

Утвердить прилагаемое Положение о защите информации в национальной платежной системе.

Председатель Правительства
Российской Федерации В.Путин

УТВЕРЖДЕНО

Постановлением Правительства
Российской Федерации
от _____ 2012 г. № _____

Положение
о защите информации в национальной платежной системе

1. Настоящее Положение устанавливает требования к защите информации о средствах и методах обеспечения информационной безопасности, персональных данных и иной информации, подлежащей обязательной защите в соответствии с законодательством Российской Федерации (далее – защита информации), обрабатываемой операторами по переводу денежных средств, банковскими платежными агентами (субагентами), операторами платежных систем, операторами услуг платежной инфраструктуры при осуществлении ими деятельности в национальной платежной системе.

Требования по обеспечению защиты информации при осуществлении переводов денежных средств устанавливаются Центральным банком Российской Федерации по согласованию с Федеральной службой безопасности Российской Федерации и Федеральной службой по техническому и экспортному контролю (далее – требования по защите информации, установленные Банком России).

2. Защита информации в национальной платежной системе обеспечивается разработкой и реализацией операторами по переводу денежных средств, банковскими платежными агентами (субагентами), операторами платежных систем, операторами услуг платежной инфраструктуры правовых, организационных и технических мер по защите информации, направленных на:

обеспечение защиты информации от неправомерного доступа, уничтожения, модифицирования, блокирования, копирования, предоставления, распространения, а также от иных неправомерных действий в отношении такой информации;

соблюдение конфиденциальности информации;

реализацию права на доступ к информации в соответствии с законодательством Российской Федерации.

3. Для обеспечения защиты информации операторами по переводу денежных средств, банковскими платежными агентами (субагентами), операторами платежных систем, операторами услуг платежной инфраструктуры создаются структурные подразделения по защите информации (службы информационной безопасности) или назначаются должностные лица (работники), ответственные за организацию защиты информации.

Для проведения работ по защите информации операторами по переводу денежных средств, банковскими платежными агентами (субагентами), операторами платежных систем, операторами услуг платежной инфраструктуры могут привлекаться на договорной основе организации, имеющие лицензии на деятельность по технической защите конфиденциальной информации и (или) на деятельность по разработке и производству средств защиты конфиденциальной информации.

4. При осуществлении переводов денежных средств разрабатываемые и реализуемые операторами по переводу денежных средств и банковскими платежными агентами (субагентами) правовые, организационные и технические меры по защите информации, в том числе применяемые средства защиты информации, должны соответствовать требованиям по защите информации, установленным Банком России.

Условиями договоров о привлечении к деятельности по оказанию услуг по переводу денежных средств банковских платежных агентов (субагентов), заключаемых между операторами по переводу денежных средств и банковскими платежными агентами и между банковскими платежными агентами и банковскими платежными субагентами предусматривается обязанность сторон по обеспечению защиты информации в соответствии с требованиями по защите информации, установленными Банком России.

5. Защита информации в платежных системах осуществляется операторами платежных систем, операторами услуг платежной инфраструктуры, операторами по переводу денежных средств, являющимися участниками платежных систем, (далее – субъекты платежной системы) в соответствии с требованиями к защите информации, включенными операторами платежных систем в правила платежных систем, установленными в соответствии с законодательством Российской Федерации о национальной платежной системе.

При взаимодействии платежных систем условиями договора о взаимодействии предусматривается обязанность операторов платежных систем обеспечить защиту информации в платежных системах.

6. Требования к защите информации, включаемые в правила платежной системы, определяются оператором платежной системы в соответствии с законодательством Российской Федерации об информации, информационных технологиях и о защите информации, иными нормативными правовыми актами Российской Федерации, требованиями по защите информации, установленными Банком России, национальными стандартами по защите информации, стандартами организаций, принятыми в соответствии с законодательством Российской Федерации о техническом регулировании, и должны включать:

требования к организации функционирования структурного подразделения по защите информации (службы информационной безопасности) или должностного лица (работника), ответственного за организацию защиты информации;

требования к управлению рисками нарушения требований к защите информации в платежной системе, определению методик анализа рисков и проведению анализа рисков нарушения требований к защите информации;

требования к назначению и распределению должностных обязанностей работников субъектов платежной системы, участвующих в обработке защищаемой информации;

требования к обеспечению защиты информации в ходе создания (модернизации), эксплуатации и снятия с эксплуатации информационных (автоматизированных) систем и технических средств, предназначенных для обработки защищаемой информации;

требования к определению угроз безопасности информации, в том числе к анализу уязвимостей, и разработке моделей угроз безопасности информации;

требования к разработке и реализации на основе моделей угроз систем защиты информации информационных (автоматизированных) систем, обеспечивающих нейтрализацию предполагаемых угроз безопасности информации;

требования к применению средств защиты информации (шифровальных (криптографических) средств, средств защиты информации от несанкционированного доступа, включая средства антивирусной защиты, средства межсетевого экранирования, системы обнаружения вторжений, средства

анализа защищенности), в том числе прошедших в установленном порядке процедуру оценки соответствия;

требования к выявлению инцидентов, связанных с нарушениями требований к защите информации, и реагированию на них, а также к информированию участников платежной системы об инцидентах, связанных с нарушениями требований к защите информации;

требования к защите информации при использовании информационно-телекоммуникационных сетей, доступ к которым не ограничен определенным кругом лиц, включая сеть Интернет;

требования к обеспечению доступа к объектам инфраструктуры платежной системы, обрабатывающим защищаемую информацию;

требования к организации и проведению контроля и оценки выполнения требований к защите информации в платежной системе.

7. Субъектами платежной системы в соответствии с требованиями к защите информации в платежной системе утверждаются локальные правовые акты, устанавливающие порядок разработки и реализации правовых, организационных и технических мер по защите информации (внутренние политики обеспечения защиты информации).

Работники субъекта платежной системы, участвующие в обработке защищаемой информации, должны быть ознакомлены с внутренними политиками обеспечения защиты информации субъекта платежной системы.

В должностные обязанности работников субъектов платежной системы, участвующих в обработке защищаемой информации, включается обязанность по выполнению требований к защите информации.

8. Разрабатываемые и реализуемые субъектами платежной системы правовые, организационные и технические меры по защите информации, в том числе применяемые средства защиты информации, должны соответствовать требованиям к защите информации в платежной системе и обеспечивать защиту информации от угроз безопасности информации в платежной системе, определяемых оператором платежной системы в модели угроз безопасности информации.

При выявлении субъектами платежной системы угроз безопасности информации, не включенных в модель угроз безопасности информации оператора, субъекты платежной системы информируют оператора платежной системы о возникновении таких угроз.

9. Субъекты платежной системы в соответствии с требованиями к защите информации в платежной системе устанавливают порядок выявления инцидентов, связанных с нарушением требований к защите информации в платежной системе, и реагирования на них.

Субъекты платежной системы информируют оператора платежной системы об инцидентах, связанных с нарушением требований к защите информации в платежной системе.

Субъектами платежной системы при их взаимодействии разрабатывается порядок совместных действий по реагированию на инциденты, связанные с нарушением требований к защите информации.

10. Защита информации в информационных (автоматизированных) системах субъектов платежной системы обеспечивается с помощью системы защиты информации, включающей совокупность организационных и технических мер по защите информации в информационных (автоматизированных) системах.

Защита информации в информационных (автоматизированных) системах субъектов платежной системы является неотъемлемой частью работ по созданию и эксплуатации информационных (автоматизированных) систем.

При разработке субъектами платежной системы информационных (автоматизированных) систем организационные и технические меры по защите информации разрабатываются и реализуются на всех стадиях жизненного цикла информационных (автоматизированных) систем в соответствии с требованиями к защите информации в платежной системе.

При приобретении субъектами платежной системы информационных (автоматизированных) систем организационные и технические меры по защите информации реализуются на этапе ввода в эксплуатацию информационных (автоматизированных) систем.

11. При использовании субъектами платежной системы для обработки защищаемой информации информационно-телекоммуникационных сетей, доступ к которым не ограничен определенным кругом лиц, включая сеть Интернет (далее – сети общего пользования), в соответствии с требованиями к защите информации в платежной системе определяются цели использования таких сетей. Для иных целей при обработке защищаемой информации использование сетей общего пользования не допускается.

Организационные и технические меры по защите информации при использовании сетей общего пользования разрабатываются и реализуются в соответствии с требованиями к защите информации в платежной системе и, в том числе, предусматривают применение шифровальных (криптографических) средств защиты информации, средств межсетевого экранирования, антивирусной защиты, обнаружения вторжений и анализа защищенности.

12. Применение шифровальных (криптографических) средств защиты информации в платежной системе осуществляется в соответствии с законодательством Российской Федерации.

13. Удостоверение права распоряжаться денежными суммами, находящимися на счете участника платежной системы или его клиента, обеспечивается электронной подписью, аналогами собственноручной подписи, кодами, паролями или иными средствами, позволяющими подтвердить, что распоряжение о переводе денежных средств составлено уполномоченным на это лицом.

14. Субъектами платежной системы организуется и проводится периодический контроль (оценка) выполнения требований к защите информации на собственных объектах инфраструктуры платежной системы.

Контроль (оценка) проводятся субъектом платежной системы самостоятельно и (или) с привлечением на договорной основе организаций, имеющих лицензию на деятельность по технической защите конфиденциальной информации.

Сроки периодического контроля (оценки) выполнения требований к защите информации в платежной системе определяются субъектом платежной системы в соответствии с требованиями к защите информации в платежной системе.

Контроль (оценка) выполнения требований к защите информации в платежной системе должен осуществляться не реже раза в два года.

Контроль (оценка) выполнения требований к защите информации в платежной системе может осуществляться в ходе аудита субъекта платежной системы, проводимого в соответствии с законодательством Российской Федерации об аудиторской деятельности, в случаях, если обеспечение защиты информации включено в перечень сопутствующих аудиту услуг, устанавливаемому федеральными стандартами аудиторской деятельности и (или) стандартами аудиторской деятельности саморегулируемых организаций аудиторов.

15. Защита информации, содержащей персональные данные, осуществляется в соответствии с законодательством Российской Федерации о персональных данных.

16. Контроль и надзор за выполнением требований, установленных настоящим Положением, осуществляется Федеральной службой безопасности Российской Федерации и Федеральной службой по техническому и экспортному контролю в пределах их полномочий и без права ознакомления с защищаемой информацией в соответствии с законодательством Российской Федерации о государственном контроле (надзоре).

17. Контроль за соблюдением требований по обеспечению защиты информации при осуществлении переводов денежных средств осуществляется Центральным банком Российской Федерации в рамках надзора в национальной платежной системе в установленном им порядке, согласованном с Федеральной службой безопасности Российской Федерации и Федеральной службой по техническому и экспортному контролю.