Проект

ЦЕНТРАЛЬНЫЙ БАНК РОССИЙСКОЙ ФЕДЕРАЦИИ

(БАНК РОССИИ)

« » 2016 г. № - П

г. Москва

П О Л О Ж Е Н И Е

О требованиях к защите информации в платежной системе Банка России

Настоящее Положение на основании Федерального закона от 10 июля 2002 года № 86-ФЗ «О Центральном банке Российской Федерации (Банке России)» (Собрание законодательства Российской Федерации, 2002, № 28, ст. 2790; 2003, № 2, ст. 157; № 52, ст. 5032; 2004, № 27, ст. 2711; № 31, ст. 3233; 2005, № 25, ст. 2426; № 30, ст. 3101; 2006, № 19, ст. 2061; № 25, ст. 2648; 2007, № 1, ст. 9, ст. 10; № 10, ст. 1151; № 18, ст. 2117; 2008, № 42, ст. 4696, ст. 4699; № 44, ст. 4982; № 52, ст. 6229, ст. 6231; 2009, № 1, ст. 25; № 29, ст. 3629; № 48, ст. 5731; 2010, № 45, ст. 5756; 2011, № 7, ст. 907; № 27, ст. 3873; № 43, ст. 5973; № 48, ст. 6728; 2012, № 50, ст. 6954; № 53, ст. 7591, ст. 7607; 2013, № 11, ст. 1076; № 14, ст. 1649; № 19, ст. 2329; № 27, ст. 3438, ст. 3476, ст. 3477; № 30, ст. 4084; № 49, ст. 6336; № 51, ст. 6695, ст. 6699; № 52, ст. 6975; 2014, № 19, ст. 2311, ст. 2317; № 27, ст. 3634; № 30, ст. 4219; № 40, ст. 5318; № 45, ст. 6154; № 52, ст. 7543; 2015, № 1, ст. 4, ст. 37; № 27, ст. 3958, ст. 4001; № 29, ст. 4348, ст. 4357; № 41, ст. 5639; № 48, ст. 6699; 2016, № 1, ст. 23, ст. 46) и Федерального закона от 27 июня

2011 года № 161-ФЗ «О национальной платежной системе» (Собрание законодательства Российской Федерации, 2011, № 27, ст. 3872; 2012, № 53, ст. 7592; 2013, № 27, ст. 3477; № 30, ст. 4084; № 52, ст. 6968; 2014, № 19, ст. 2315, ст. 2317; № 43, ст. 5803; 2015, № 1, ст. 8, ст. 14) устанавливает требования к защите информации в платежной системе Банка России (далее – ПС БР) при осуществлении переводов денежных средств.

Глава 1. Общие положения

1.1. Термины, используемые в настоящем Положении, применяются в значениях, определенных Положением Банка России от 9 июня 2012 года №382-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» зарегистрированное Министерством юстиции Российской Федерации 14 июня 2012 года № 24575, 1 июля 2013 года № 28930, 10 сентября 2014 года № 34017 («Вестник Банка России» от 22 июня 2012 года № 32, от 10 июля 2013 года № 37, от 17 сентября 2014 года № 83).

1.2. Действие настоящего положения распространяется на участников ПС БР, являющихся клиентами Банка России (далее – Участники).

1.3. Участники обеспечивают защиту следующей информации:

информации, содержащейся в распоряжениях Участников;

информации о совершенных переводах денежных средств, в том числе информации, содержащейся в извещениях (подтверждениях), касающихся приема к исполнению распоряжений Участников, а также в извещениях (подтверждениях), касающихся исполнения распоряжений Участников;

информации об остатках денежных средств на счетах, открытых у Участников и связанных с осуществлением перевода денежных средств в ПС БР;

информации, необходимой для удостоверения Участниками права распоряжения денежными средствами;

ключевой информации средств криптографической защиты информации (далее - СКЗИ), используемых при осуществлении переводов денежных средств (далее - криптографические ключи);

информации об объектах информационной инфраструктуры, а также информации о конфигурации, определяющей параметры работы технических средств защиты информации;

информации ограниченного доступа, в том числе персональных данных и иной информации, подлежащей обязательной защите в соответствии с законодательством Российской Федерации, обрабатываемой при осуществлении переводов денежных средств.

Глава 2. Требования к организационному и документационному обеспечению

2.1. Участники должны обеспечивать доступ к автоматизированному рабочему месту (далее – АРМ) обмена электронными сообщениями (далее – ЭС) с ПС БР только из сегмента локальной вычислительной сети (далее – ЛВС), в котором расположен АРМ обмена ЭС с ПС БР (далее – Участок ПС БР).

2.2. Участники самостоятельно определяют порядок обеспечения защиты информации на Участке ПС БР в соответствии с требованиями настоящего Положения (далее – порядок обеспечения защиты информации).

В целях определения порядка обеспечения защиты информации Участники должны разработать документы в соответствии с перечнем процедур, регламентируемых в целях обеспечения информационной безопасности на Участке ПС БР (приложение к настоящему Положению). Документы, регламентирующие вопросы, связанные с процедурами по информационной безопасности должны быть согласованы со службой

информационной безопасности Участника (далее – служба информационной безопасности) (далее – внутренние документы).

2.3. Порядок обеспечения защиты информации должен предусматривать меры по обеспечению защиты информации на всех стадиях жизненного цикла (от внедрения до снятия с эксплуатации) объектов информационной инфраструктуры Участка ПС БР.

2.4.Участники должны обеспечивать соблюдение требований и рекомендаций по порядку установки, настройки, эксплуатации, изложенных в документации на системы защиты информации от несанкционированного доступа (далее – СЗИ от НСД), СКЗИ, средства защиты от воздействий вредоносного кода (далее - СЗ от ВВК), применяемые на Участке ПС БР.

Глава 3. Требования к защите информации при физическом доступе к Участку ПС БР

3.1.Участники регламентируют и осуществляют контроль доступа в помещения, в которых формируются, обрабатываются, контролируются и передаются (принимаются) ЭС (далее – Помещения), с использованием организационных мер или технических средств контроля и управления доступом.

3.2.Физический доступ в Помещения должен предоставляться только тем работникам Участника, которые указаны в списке доступа в данные Помещения.

3.3.Помещения должны быть оборудованы охранной сигнализацией, сдаваться под охрану и располагаться в зоне действия системы видеонаблюдения.

3.4.Срок хранения информации систем видеонаблюдения и контроля доступа (в случае использования), предусмотренных пунктом 3.3 настоящего Положения, должен составлять не менее 3 лет.

Глава 4. Требования к защите информации при логическом доступе к Участку ПС БР

4.1.Логический доступ работников к ПС БР должен осуществляться с использованием персонифицированных уникальных учетных записей, в соответствии со списком логического доступа.

4.2.Список логического доступа Участника должен быть актуальным.

4.3.При осуществлении логического доступа работников к Участку ПС БР должно быть обеспечено ведение следующих электронных журналов:

журналов логического доступа к информационным ресурсам ПС БР (далее – журналы логического доступа);

журналов операций, выполненных при осуществлении логического доступа к информационным ресурсам ПС БР (далее – журналы операций);

журналов средств защиты информации.

Сроки хранения журналов логического доступа, журналов операций и журналов средств защиты информации должны составлять не менее 3 лет.

4.4. Журналы логического доступа к информационным ресурсам ПС БР и журналы операций должны быть доступны работникам службы информационной безопасности и работникам службы информатизации, осуществляющим обслуживание объектов информационной инфраструктуры в рамках Участка ПС БР. Журналы средств защиты информации должны быть доступны только работникам службы информационной безопасности. Внесение изменений в журналы операций не допускается.

Глава 5. Требования к обеспечению информационной безопасности платежного технологического процесса на Участке ПС БР

5.1.Формирование, обработка, контроль ЭС должны осуществляться с использованием АРМ обмена ЭС с ПС БР или с использованием

специальной компоненты автоматизированной банковской системы (далее – АБС) Участника. Передача (прием) ЭС должны проводиться с использованием АРМ обмена ЭС с ПС БР.

5.2.Программным обеспечением АРМ обмена ЭС с ПС БР или специальной компоненты АБС Участника должны выполняться только функции, предусмотренные пунктом 5.1.

5.3.Участники должны осуществлять регистрацию и мониторинг всех операций в платежных технологических процессах, осуществляемых в рамках Участка ПС БР в которых осуществляется взаимодействие работников с объектами информационной инфраструктуры.

5.4.Участники должны хранить все входящие и исходящие ЭС. Сроки хранения входящих и исходящих ЭС должны составлять не менее 5 лет.

Глава 6. Требования к контролю программного обеспечения, используемого для взаимодействия с Участком ПС БР

6.1.Программное обеспечение подлежит контролю целостности при каждом включении АРМ обмена ЭС с ПС БР.

6.2.В целях контроля и учета состава программного обеспечения на каждом объекте информационной инфраструктуры Участка ПС БР, должен вестись актуальный перечень программного обеспечения.

Глава 7. Требования к защите от воздействий вредоносного кода на Участке ПС БР

7.1.На технических средствах Участка ПС БР Участников должны быть установлены СЗ от ВВК.

7.2.Участники на Участке ПС БР должны применять СЗ от ВВК различных производителей и обеспечивать их раздельную установку на персональных электронных вычислительных машинах и серверах.

7.3.Участники должны проводить предварительную проверку программного обеспечения и средств вычислительной техники (далее –

СВТ) на отсутствие вредоносного кода перед их включением в Участок ПС БР.

7.4.Участники должны вести статистику событий, связанных с воздействиями вредоносного кода на Участке ПС БР, с целью проведения ее дальнейшего анализа и минимизации рисков информационной безопасности.

7.5. Сроки хранения данных о событиях, связанных с воздействиями вредоносного кода на Участке ПС БР и их анализе, должны составлять не менее 3 лет.

Глава 8. Требования по применению средств криптографической защиты информации на Участке ПС БР

8.1.На технических средствах Участка ПС БР должны быть установлены СКЗИ.

8.2.При организации работы с криптографическими ключами, Участниками должно обеспечиваться выполнение следующих требований:

исключение возможности доступа неуполномоченных лиц к криптографическим ключам;

использование носителей с рабочей копией криптографического ключа при работе с СКЗИ;

использование хранилищ (металлические шкафы, сейфы) для хранения носителей с криптографическими ключами по окончании рабочего дня, а также вне времени работы с СКЗИ (допускается хранение носителей с криптографическими ключами в хранилище вместе с иными документами при условии помещения носителей с криптографическими ключами в отдельный опечатываемый контейнер);

информирование Банка России о подозрении на компрометацию или компрометации криптографического ключа, используемого для обмена ЭС с ПС БР (под компрометацией криптографического ключа понимается

событие, определяемое владельцем криптографического ключа как ознакомление неуполномоченного лица (лиц) с его криптографическим ключом) и инициирование действия по внеплановой смене криптографического ключа.

8.3. При выходе из строя носителя с рабочей копией криптографического ключа необходимо с использованием программного обеспечения СКЗИ изготовить новый носитель с рабочей копией криптографического ключа на основе носителя, содержащего оригинал криптографического ключа.

8.4. При эксплуатации криптографических ключей Участниками должна быть исключена возможность выполнения следующих действий:

изготовление несанкционированных копий с носителей криптографических ключей;

ознакомление с содержанием носителей криптографических ключей или передача носителей криптографических ключей, лицам, не имеющим прав доступа к носителям криптографических ключей;

вывод криптографических ключей на дисплей электронной вычислительной машины (далее – ЭВМ) или устройства вывода (печати) текстовой или графической информации;

установка носителей криптографических ключей в считывающее устройство ЭВМ, на которой осуществляется функционирование СКЗИ в нештатных режимах, а также на другие ЭВМ, не предназначенные для работы с ПС БР;

запись на носители криптографических ключей любой информации, за исключением криптографического ключа.

Глава 9. Требования к обучению работников по вопросам обеспечения информационной безопасности

9.1. Обучение работников по вопросам обеспечения информационной безопасности при взаимодействии с ПС БР должно проводиться с привлечением службы информационной безопасности и документально фиксироваться.

9.2.Участниками должны быть назначены работники, ответственные за разработку, реализацию планов и программ обучения по вопросам информационной безопасности, в том числе в рамках Участка ПС БР.

Глава 10. Требования к информированию Банка России об инцидентах и хранению информации об инцидентах

10.1.Участники осуществляют информирование Банка России о выявленных инцидентах, связанных с нарушением требований к обеспечению защиты информации, (далее – Инциденты) на Участке ПС БР, в том числе о несанкционированных переводах денежных средств Участника через ПС БР, подозрениях о возникновении или о возможности возникновения Инцидентов на Участке ПС БР. Информирование осуществляется в произвольной форме на электронный адрес fincert@cbr.ru, либо инициируется запрос на передачу этих сведений с применением мер и средств защиты информации, не позднее трех часов, после выявления Инцидента.

10.2.Участники должны документально фиксировать всю информацию об Инцидентах, результаты анализа причин возникновения Инцидентов, информацию о действиях, принятых для минимизации последствий Инцидентов и иную информацию, связанную с Инцидентами.

10.3.Срок хранения информации, предусмотренной пунктом 10.2 настоящего Положения, устанавливается не менее 3 лет с даты возникновения Инцидента.

Глава 11. Требования к обеспечению непрерывности и восстановлению деятельности Участников и функционирования технических средств защиты информации на Участке ПС БР

11.1.Участники должны разработать и утвердить план обеспечения непрерывности и восстановления деятельности (далее – ОНиВД), согласованный со службой информационной безопасности и предусматривающий мероприятия по восстановлению функционирования технических средств защиты информации и объектов информационной инфраструктуры Участка ПС БР в случаях сбоев и (или) отказов в их работе.

11.2. Участниками должны быть назначены работники, ответственные за ОНиВД, в том числе функционирование технических средств защиты информации в ПС БР.

Глава 12. Требования по контролю требований к защите информации на Участке ПС БР

12.1.Участники должны осуществлять контроль выполнения требований к защите информации (далее – Контроль ТЗИ), установленных настоящим Положением, а также хранить и анализировать результаты Контроля ТЗИ. Контроль ТЗИ должен проводиться не реже одного раза в квартал.

12.2.Срок хранения информации о результатах Контроля ТЗИ и решениях, принятых по результатам Контроля ТЗИ, устанавливается не менее 3 лет с даты проведения Контроля ТЗИ.

Глава 13. Заключительные положения

13.1.Настоящее Положение вступает в силу по истечении 10 дней после дня его официального опубликования.

13.2. Участникам следует выполнить требования к защите информации на Участке ПС БР в соответствии с настоящим Положением до 30 июня 2017 года.

Председатель
Центрального банка
Российской Федерации Э.С. Набиуллина

Приложение
к Положению Банка России
от «__» _____2016 г. №_____
«О требованиях к защите информации
в платежной системе Банка России»

Перечень процедур, регламентируемых в целях обеспечения информационной безопасности на Участке ПС БР

№	Назначение документа
1.	Назначение куратора по информационной безопасности
2.	Создание подразделений (назначение работников), ответственных за организацию и контроль обеспечения защиты информации, а так же выделение им необходимых ресурсов
3.	Основные положения о службе информационной безопасности (в том числе полномочия)
4.	Назначение работников, ответственных за выполнение порядка обеспечения защиты информации на Участке ПС БР и определение их функций и задач
5.	Организация обеспечения информационной безопасности Участника с учетом требований настоящего Положения
6.	Обеспечение защиты информации при осуществлении переводов денежных средств с использованием

	информационно-телекоммуникационной сети «Интернет»
7.	Определение Участка ПС БР
8.	Функции и задачи работников, при осуществлении Контроля ТЗИ
9.	Организация защиты от воздействий вредоносного кода у Участников
10.	Проведение предварительной проверки программного обеспечения и СВТ на отсутствие вредоносного кода
11.	Перечень и описание объектов информационной инфраструктуры Участка ПС БР
12.	Порядок уничтожения не используемой защищаемой информации на стадиях жизненного цикла объектов информационной инфраструктуры Участка ПС БР
13.	Перечень средств защиты информации, используемых на Участке ПС БР
14.	Учет и контроль программного обеспечения, установленного на средствах вычислительной техники Участка ПС БР
15.	Состав и порядок применения организационных мер и технических средств защиты информации на Участке ПС БР
16.	Функции и задачи работников, ответственных за процессы реагирования на Инциденты на Участке ПС БР
17.	Порядок действий по выявлению и реагированию на инциденты на Участке ПС БР
18.	Перечень и сроки проведения Контроля ТЗИ

19.	Перечень и сроки проведения мероприятий по обучению и повышению информированности работников по вопросам защиты информации
20.	Программа обучения работников по вопросам защиты информации
21.	Перечень лиц, имеющих доступ к объектам информационной инфраструктуры Участка ПС БР и порядок осуществления доступа
22.	Перечень лиц, обладающих правами по воздействию на объекты информационной инфраструктуры, которое может привести к нарушению предоставления услуг по осуществлению переводов денежных средств
23.	Перечень лиц, обладающих правами по формированию электронных сообщений на АРМ обмена ЭС с ПС БР
24.	Описание функций и задач пользователей программных и технических средств, эксплуатируемых на участке ПС БР, а также персонала, обеспечивающего эксплуатацию и администрирования указанных средств
25.	Функции и задачи работников, ответственных за обеспечение непрерывности и восстановление деятельности Участника, в том числе функционирования технических средств защиты информации в ПС БР
26.	План ОНиВД
27.	Порядок действий по обеспечению непрерывности и восстановлению деятельности Участника и функционирования технических средств защиты информации в ПС БР
28.	Технологические процессы подготовки, приема, ввода, обработки и передачи ЭС;
29.	Информация о применяемых на Участке ПС БР СКЗИ, порядок обращения с СКЗИ на всех этапах жизненного цикла СКЗИ, основные положения об обеспечении безопасности криптографических ключей

30.	Перечень работников, обладающих правами по управлению криптографическими ключами
31.	Перечень работников, допущенных к работе со СКЗИ на Участке ПС БР
32.	Назначение лица, ответственного за обеспечение функционирования и безопасности СКЗИ (ответственный пользователь СКЗИ), а также назначение постоянно действующих комиссий по уничтожению СКЗИ, назначение лиц, ответственных за формирование криптографических ключей и обеспечение безопасности криптографических ключей
33.	Перечень работников, обладающих правами доступа в помещения Участка ПС БР
34.	Перечень программного обеспечения для каждого объекта информационной инфраструктуры
35.	Акты установки (настройки) СЗ от ВВК
36.	Акты установки (настройки) СКЗИ на технических средствах Участка ПС БР
37.	Результаты Контроля ТЗИ и решения, принятые по результатам Контроля ТЗИ с указанием участников, оснований и объекта Контроля ТЗИ.