"Положение о требованиях к защите информации в платежной системе Банка России" (утв. Банком России 24.08.2016 № 552-П)

Зарегистрировано в Минюсте России 06.12.2016 № 35989

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, ст. 50; № 27, ст. 4225, ст. 4273, ст. 4295), статьи 20 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; 2016, № 27, ст. 4221, ст. 4223) и с учетом требований Положения 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», зарегистрированного 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), устанавливает требования к защите информации в платежной системе Банка России (далее - ПС БР) при осуществлении переводов денежных средств.

Глава 1. Общие положения

1.1. Действие настоящего Положения распространяется на участников ПС БР, являющихся клиентами Банка России (далее - участники).

1.2. Участники обеспечивают защиту следующей информации в ПС БР:
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 защиты информации в ПС БР

2.1. Для защиты информации при осуществлении доступа к объектам информационной инфраструктуры 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. В целях фиксации решения о необходимости применения организационных мер защиты информации и (или) использования технических средств защиты информации и обеспечения применения указанных мер 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 процедуры по информационной безопасности, должны быть согласованы со службой информационной безопасности участника.

2.3. Документы, указанные в пункте 2.2 настоящего Положения, должны определять порядок обеспечения защиты информации и предусматривать меры по обеспечению защиты информации на всех стадиях создания, эксплуатации (использования по назначению, технического обслуживания и ремонта), модернизации, снятия с эксплуатации объектов информационной

инфраструктуры участка ПС БР.

2.4. Участники должны обеспечивать выполнение требований эксплуатационной 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, в течение всего срока их эксплуатации, в том числе при установке и настройке, а также обеспечить восстановление указанных технических средств защиты информации в случаях сбоев и (или) отказов в их работе.

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

3.1. Участники осуществляют контроль физического доступа к объектам информационной инфраструктуры в целях предотвращения физического воздействия на средства вычислительной техники, применяемые для осуществления переводов денежных средств, с использованием организационных мер или технических средств контроля и управления доступом в помещения, в которых формируются, обрабатываются, контролируются и передаются (принимаются) ЭС (далее - помещения).

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 и контроля доступа.

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

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

4.1. Процедуры идентификации, аутентификации и авторизации при логическом доступе работников к участку ПС БР должны осуществляться с использованием персонифицированных уникальных учетных записей в соответствии с действующим перечнем субъектов доступа, которым предоставлен логический доступ к участку ПС БР.

4.2. В целях регистрации действий при осуществлении логического доступа работников к участку ПС БР и действий, связанных с назначением и распределением прав логического доступа, а также обеспечения хранения указанной информации 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 трех лет.

4.3. В целях защиты информации от несанкционированного доступа журналы логического доступа и журналы операций должны быть доступны работникам службы информационной безопасности и работникам службы информатизации, осуществляющим обслуживание объектов информационной инфраструктуры на участке ПС БР. Журналы средств защиты информации должны быть доступны только работникам службы информационной безопасности. Внесение исправлений в журналы операций не допускается.

Глава 5. Требования к использованию технологических мер защиты информации

5.1. В целях обеспечения идентификации, аутентификации и авторизации клиента в системе Интернет-банкинга, а также определения перечня устройств, с использованием которых может осуществляться доступ к системе Интернет-банкинга при переводе денежных средств посредством передачи ЭС в ПС БР, функции формирования, обработки, контроля и передачи (приема) ЭС должны осуществляться с использованием АРМ обмена ЭС с ПС БР или с использованием специальной компоненты автоматизированной банковской системы (далее - АБС) участников.

5.2. Для защиты ЭС от искажения, фальсификации, переадресации, несанкционированного ознакомления, уничтожения и ложной авторизации программным обеспечением АРМ обмена ЭС с ПС БР или специальной компоненты АБС участника должны выполняться только функции, предусмотренные пунктом 5.1 настоящего Положения.

5.3. Контроль (мониторинг) соблюдения установленной технологии при подготовке, обработке, передаче и хранении ЭС осуществляется участником путем регистрации всех операций в платежных технологических процессах, осуществляемых на участке ПС БР, в которых осуществляется взаимодействие работников с объектами информационной инфраструктуры.

5.4. В целях обеспечения возможности восстановления информации об остатках денежных средств на банковских счетах в случае умышленного (случайного) разрушения (искажения) или выхода из строя средств вычислительной техники, а так же обеспечения сверки выходных ЭС с соответствующими входными и обработанными ЭС при осуществлении расчетов в платежной системе

участники должны хранить все входящие и исходящие ЭС. Сроки хранения входящих и исходящих ЭС должны составлять не менее пяти лет.

Глава 6. Требования к контролю программного обеспечения, установленного и (или) используемого на средствах вычислительной техники участка ПС БР

6.1. В целях контроля несанкционированного внесения изменений в состав установленного и (или) используемого на средствах вычислительной техники участка ПС БР программного обеспечения должен осуществляться контроль целостности программного обеспечения АРМ обмена ЭС с ПС БР при каждом включении.

6.2. В целях учета и контроля состава установленного и (или) используемого на средствах вычислительной техники участка ПС БР программного обеспечения участники должны вести актуальный перечень указанного программного обеспечения.

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

7.1. На участке ПС БР участники должны использовать СЗ от ВВК различных производителей и обеспечивать их раздельную установку на персональных электронных вычислительных машинах и серверах.

7.2. Участники должны проводить предварительную проверку программного обеспечения и средств вычислительной техники (далее - СВТ) на отсутствие вредоносного кода перед их включением в участок ПС БР.

7.3. В целях информирования участников ПС БР об обнаружении вредоносного кода или факта воздействия вредоносного кода участники должны вести статистику событий, связанных с воздействиями вредоносного кода на участке ПС БР.

7.4. Сроки хранения данных о событиях, связанных с воздействиями вредоносного кода на участке ПС БР и их анализе, должны составлять не менее трех лет.

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

8.1. Для защиты информации при осуществлении переводов денежных средств на технических средствах участка ПС БР должны быть установлены СКЗИ.

8.2. В целях предотвращения несанкционированного использования криптографических ключей 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 в случае возникновения или подозрения на возникновение события, определяемого владельцем криптографического ключа как ознакомление неуполномоченного лица (лиц) с его криптографическим ключом, и инициирование действий по внеплановой смене криптографического ключа;
исключение возможности выполнения следующих действий:
изготовления несанкционированных копий с носителей криптографических ключей;
ознакомления с содержанием носителей криптографических ключей или передача носителей криптографических ключей лицам, не имеющим прав доступа к носителям криптографических ключей;
вывода криптографических ключей на дисплей электронной вычислительной машины (далее - ЭВМ) или устройства вывода (печати) текстовой или графической информации;
установки 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;
записи на носители криптографических ключей любой информации, за исключением криптографического ключа.

8.3. В целях обеспечения безопасности процессов изготовления криптографических ключей 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.

Глава 9. Требования к повышению осведомленности работников в области обеспечения защиты информации

9.1. В целях обеспечения повышения осведомленности работников в области обеспечения защиты информации участниками должно проводиться и документально фиксироваться обучение работников по вопросам обеспечения информационной безопасности на участке ПС БР с привлечением службы информационной безопасности.

9.2. Участниками должны быть назначены лица, ответственные за разработку, реализацию планов и программ обучения по вопросам информационной безопасности на участке ПС БР.

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

10.1. Участники осуществляют информирование Банка России о выявленных инцидентах, связанных с нарушением требований к обеспечению защиты информации на участке ПС БР (далее - инциденты), в том числе о несанкционированных переводах денежных средств участника через ПС БР, а также о подозрениях, о возникновении или о возможности возникновения инцидентов на участке ПС БР. Информирование осуществляется в произвольной форме путем отправки сообщения 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. В целях анализа обеспечения в ПС БР защиты информации при осуществлении переводов денежных средств участники должны документально фиксировать всю информацию об инцидентах, включая результаты анализа причин возникновения инцидентов, информацию о действиях, принятых для минимизации негативных последствий инцидентов и иную информацию, связанную с инцидентами.

10.3. Срок хранения информации об инцидентах должен составлять не менее трех лет с даты возникновения инцидента.

Глава 11. Требования к обеспечению восстановления функционирования технических средств на участке ПС БР в случаях сбоев и (или) отказов в их работе

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 на участке ПС БР в случаях сбоев и (или) отказов в их работе.

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

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

12.1. В целях обеспечения проведения оценки требований к обеспечению защиты информации при осуществлении переводов денежных средств участники должны проводить и документально подтверждать проведение контроля выполнения требований к защите информации (далее - контроль ТЗИ), установленных настоящим Положением. Контроль ТЗИ и его анализ должен проводиться участниками не реже одного раза в квартал.

12.2. Срок хранения информации о результатах проведения контроля ТЗИ и решениях, принятых по результатам указанного контроля, должен составлять не менее трех 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 24 августа 2016 года № 552-П "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	*2*
1.	Назначение куратора по информационной безопасности
2.	Создание подразделений (назначение работников), ответственных за организацию и контроль обеспечения защиты информации, а также 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 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 ВВК
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 неиспользуемой 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 администрирование 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 для проведения контроля и объекта контроля ТЗИ

защита информации в национальной платежной системе

From:
http://www.sps-ib.ru/ - **Справочно-правовая система по информационной безопасности**

Permanent link:
http://www.sps-ib.ru/npa:cb552-p_24.08.2016

Last update: **2016/12/27 09:45**