Методические рекомендации
по выполнению требований Положения Банка России от 24 августа 2016 года № 552-П «О требованиях по защите информации в платежной системе Банка России»

Настоящие Методические рекомендации являются методической основой для организации безопасной эксплуатации рабочих мест обмена электронными сообщениями (далее – ЭС) с платежной системой Банка России (далее – ПС БР) при переводе денежных средств в рамках ПС БР участниками ПС БР, являющимися клиентами Банка России (далее – участники), и носят рекомендательный характер.

Термины, предусмотренные настоящими Методическими рекомендациями, применяются в значении, установленном Положением Банка России от 24 августа 2016 года № 552-П «О требованиях по защите информации в платежной системе Банка России» (далее – Положение).

1. Общие положения

1.1. При выполнении требований пункта 1.1 Положения рекомендуется учитывать, что действие Положения не распространяется на клиентов кредитных организаций, не являющихся участниками платежной системы Банка России.

1.2. Базовые требования к защите информации в ПС БР для участника устанавливаются договором об обмене ЭС при переводе денежных средств в рамках ПС БР, заключаемым между Банком России и участником.

1.4. При организации защиты информации рекомендуется руководствоваться требованиями законодательства Российской Федерации, нормативно-правовых актов Правительства Российской Федерации, нормативных документов Банка России, комплекса стандартов Банка России СТО ИББС.

2. Рекомендации к организационному и документационному обеспечению защиты информации в ПС БР

2.1. Действие Положения распространяется только на сегмент локальной вычислительной сети автоматизированной банковской системы участника (далее – АБС), в котором размещено автоматизированное рабочее место (далее – АРМ) обмена ЭС с ПС БР (далее - участок ПС БР).

2.2. В целях документирования границ и состава участка ПС БР рекомендуется разработать схему сегмента вычислительной сети участка ПС БР с приложением перечня и описания объектов информационной инфраструктуры, а также перечня средств защиты информации.

2.3. Доступ уполномоченных работников к АРМ обмена ЭС с ПС БР обеспечивается только путем предоставления им физического доступа с соблюдением требований, изложенных в пункте 4.1 Положения. Удаленный (логический) доступ работников к объектам информационной инфраструктуры не рекомендуется.

2.4. Взаимодействие АРМ обмена ЭС с ПС БР и устройства, с которого осуществляется загрузка/выгрузка данных, может быть организовано путем использования отчуждаемого машинного носителя информации, подключаемого к выделенному USB–порту (при этом рекомендуется осуществлять контроль подключения носителя и выгрузки/загрузки данных с использованием средств защиты от несанкционированного доступа, а также контроль на предмет выявления вредоносного кода) организации сетевого взаимодействия (при этом данное взаимодействие рекомендуется организовывать с использованием межсетевого экрана, сертифицированного по 4 классу, с указанием конкретных адресов, портов и протоколов, используемых для такого взаимодействия).

Выгрузку/загрузку данных из/в АРМ обмена ЭС с ПС БР рекомендуется осуществлять по инициативе АРМ обмена ЭС с ПС БР.

2.5. При подготовке требуемого перечня документов, определенного Положением, допускается их объединение и оформление в виде единого документа.

3. Рекомендации по защите информации при физическом доступе к участку ПС БР

3.1. Реализация мер, предусмотренных главой 3 Положения, включая видеорегистрацию физического доступа работников в помещения, в которых находятся средства вычислительной техники (далее – СВТ) участка ПС БР, а также СВТ, входящие в состав АБС и задействованные в процессе перевода денежных средств (формирование (подготовка, включая ввод распоряжения), обработка, контроль и передача/прием ЭС) (далее – помещения), может осуществляться общими системами охранной сигнализацией, видеонаблюдения и контроля доступа, установленными на объекте на момент вступления в силу Положения, с учетом требований, прямо установленных главой 3 Положения.

3.2. Контроль физического доступа работников в помещения может осуществляться с использованием средств системы контроля и управления доступом (далее – СКУД) с учетом выполнения требований, установленных в пункте 3.2 Положения. Списки доступа, вводимые в СКУД, рекомендуется составлять с учетом следующего: они должны быть актуальны, утверждены руководителем участника или уполномоченным им лицом и находиться в помещениях на визуально доступном месте.

Настройки датчиков времени систем видеонаблюдения и СКУД и АБС рекомендуется контролировать и обеспечивать их совпадение.

4. Рекомендации по защите информации при логическом доступе к участку ПС БР

4.1 С целью выполнения требований пункта 4.2 Положения на оборудовании, включенном в состав участка ПС БР, рекомендуется обеспечивать аудит файловых папок, задействованных в формировании, отправке и получении ЭС.

4.2. Рекомендуется обеспечивать регистрацию следующего минимального набора событий с фиксацией времени их возникновения:

вход (выход) пользователя в систему (из системы);

управление учетными записями пользователей (групп пользователей);

назначение (изменение) системных привилегий (ролей) и их использование;

факты обращения к программному обеспечению обмена ЭС, другому программному обеспечению (по решению участника обмена ЭС);

факты попыток несанкционированного доступа;

информация о сбоях и других нештатных ситуациях.

5. Рекомендации по использованию технологических мер защиты информации

5.1. При выполнении требований пункта 5.1 Положения рекомендуется руководствоваться следующим.

В случае, если у участника реализована схема с использованием участка ПС БР, в целях обеспечения идентификации, аутентификации и авторизации участника функции формирования, обработки, контроля и передачи (приема) ЭС осуществляются с использованием АРМ обмена ЭС с ПС БР.

В случае, если у участника реализована схема с использованием специальной компоненты АБС, в целях обеспечения идентификации, аутентификации и авторизации участника функции формирования, обработки, контроля и передачи (приема) ЭС осуществляются с использованием специальной компоненты АБС.

Рекомендуется распространять на специальную компоненту АБС требования Положения, а также настоящие Методические рекомендации.

5.2. С целью выполнения требований пункта 5.3 Положения на всем оборудовании, выполняющем операции по подготовке, обработке, передаче и хранению ЭС (включая рабочие места работников, выполняющих данные технологические операции) рекомендуется обеспечивать аудит файловых папок, задействованных в этих операциях.

С целью повышения качества аутентификации, а также обеспечения надежного подтверждения совершаемых операций по переводу денежных средств, рекомендуется использовать для этих целей двухфакторную (многофакторную) аутентификацию с дополнительным подтверждением.

6. Рекомендации по защите информации от воздействий вредоносного кода на участке ПС БР

6.1. В дополнение к изложенным в главе 7 Положения требованиям по защите информации от воздействия вредоносного кода рекомендуется установка на АБС системы обнаружения аномальной сетевой активности, предназначенной для выявления и блокирования вредоносного кода, попавшего в АБС в результате пропуска средствами антивирусной защиты, а также системы централизованного мониторинга и управления этими средствами.

6.2. В случае переноса СКЗИ из АРМ обмена ЭС с ПС БР за пределы участка ПС БР и установки их на технические средства, входящие в состав АБС, на эти средства должны распространяться требования Положения Банка России с учетом настоящих Методических рекомендаций.

7. Рекомендации по повышению осведомленности работников в области обеспечения защиты информации

7.1. С целью выполнения требований главы 9 Положения для поддержания необходимого уровня осведомленности работников в вопросах, связанных с эксплуатацией АРМ обмена ЭС с ПС БР и его защитой, рекомендуется обеспечивать доступность для работников эксплуатационной документации применяемых средств (в электронном виде и/или на бумажном носителе), доводить под роспись содержание указанных документов.

7.2. В целях организации и проведения учебных мероприятий по повышению осведомленности работников в области обеспечения защиты информации целесообразно разрабатывать планы периодического (например, на ежегодной основе) проведения обучения работников участка ПС БР.

Рекомендуется включать в программы обучения по вопросам информационной безопасности на участке ПС БР вопросы, раскрывающие содержание Положения, настоящих рекомендаций, а также документов, регламентирующих процедуры по информационной безопасности.

7.3. Учебные мероприятия рекомендуется завершать проверкой степени усвоения материала по теме проведенного занятия. Формы контроля знаний выбираются участником самостоятельно (контрольный опрос, тесты, собеседование с работниками и др.).

7.4. Для работника, впервые приступающего к работе на участке ПС БР, а также при назначении новых ролей ранее допущенным работникам, рекомендуется провести обучение по вопросам обеспечения информационной безопасности на участке ПС БР.

7.5. Факт участия работника в учебном мероприятии рекомендуется фиксировать в специальных журналах (ведомостях), ведущихся в электронном виде и/или на бумажном носителе, с проставлением работником, принявшим участие в мероприятии, собственноручной подписи или иной отметки, подтверждающей его участие и (или) получение соответствующего сертификата.

8. Рекомендации по информированию Банка России о выявленных инцидентах и хранению информации об инцидентах

8.1. С целью выполнения требований пункта 10.1 Положения рекомендуется включать в состав передаваемой в Банк России информации, следующие данные:

8.1.1. В части идентификации инцидента информационной безопасности (далее – ИИБ), источника получения информации о нем:

дата и время регистрации ИИБ (получения информации об инциденте);

источник информации об ИИБ – работник, заметивший первичные признаки инцидента, или средства защиты (например, средства защиты от воздействий вредоносного кода);

роль работника, выявившего ИИБ (пользователь, администратор, администратор ИБ, работник службы ИБ);

наименование, тип, версия средство защиты, с помощью которого был выявлен инцидент или его первичные признаки.

8.1.2 В части описания события ИБ:

текстовое описание сущности нарушения, включая описание характера воздействия;

факт нарушения требований к обеспечению ИБ;

факт нарушения работы средств защиты информации;

факт нарушения свойств безопасности (целостность, конфиденциальность, доступность);

наличие или отсутствие преднамеренности возникновения инцидента (случайный, преднамеренный, ошибочный).

8.1.3. В части воздействия на составляющие информационной инфраструктуры организации и оценки ущерба:

тип информационных активов, затронутых ИИБ (ЭС, управляющая и/или вспомогательная информация);

затронутые единицы информационной инфраструктуры (программное обеспечение, сетевое оборудование и др.);

степень тяжести последствий ИИБ (в том числе, оценка материального ущерба, оценка времени восстановления после инцидента);

сохранение возможности осуществления перевода денежных средств путем обмена ЭС (обмен ЭС нарушен не был или потребовался переход к технологии обмена распоряжениями о переводе денежных средств на машинных носителях или бумажном носителе).

9. Рекомендации по обеспечению восстановления функционирования технических средств на участке ПС БР в случаях сбоев и (или) отказов в их работе

9.1. С целью выполнения требований пункта 11.1 Положения рекомендуется:

регулярно проводить с работниками участка ПС БР учебно-тренировочные занятия по отработке плана обеспечения непрерывности и восстановления деятельности (далее – ОНиВД);

определять предельно допустимое время восстановления функционирования технических средств на участке ПС БР самостоятельно с учетом оценки рисков нарушения взаимодействия с ПС БР.

9.2. Учебно-тренировочные занятия с работниками участка ПС БР по отработке плана ОНиВД рекомендуется проводить с периодичностью, установленной участником, но не реже 1 раза в год. Факт участия работника в учебно-тренировочном занятии рекомендуется фиксировать в специальных журналах (ведомостях), ведущихся в электронном виде и/или на бумажном носителе, с проставлением работником, принявшим участие в мероприятии, собственноручной подписи или иной отметки, подтверждающей его участие.

10. Рекомендации по контролю выполнения требований к защите информации на участке ПС БР

10.1. С целью выполнения требований пункта 12.1 Положения контроль выполнения требований по защите информации может выполняться в рамках процедур внутреннего контроля, принятых в организации.

10.2. В плановом порядке рекомендуется проводить комплексные (по всем вопросам защиты на участке ПС БР) и тематические (по отдельным, возможно, проблемным вопросам) проверки. При подготовке программ данных проверок в качестве методического материала рекомендуется использовать положения настоящих Методических рекомендаций.

11. Рекомендации по перечню процедур, регламентируемых в целях обеспечения информационной безопасности на участке ПС БР

С целью сокращения числа руководящих документов и обеспечения соответствия требованиям Положения участнику рекомендуется.

11.1. Схема и состав участка ПС БР, метод его выделения, оборудование на котором осуществляется выделение этого сегмента, перечень средств защиты информации, используемых на участке ПС БР, а также кандидатуры работников, ответственных за выполнение настроек и поддержание их в актуальном состоянии, рекомендуется согласовывать со службой

информатизации, информационной безопасности и обеспечивать утверждение куратором.

11.2. Вопросы организации защиты от воздействий вредоносного кода, криптографической защиты, состав и порядок применения организационных мер и технических средств защиты информации на участке ПС БР, а также порядок учета и контроля программного обеспечения, установленного на СВТ участка ПС БР, рекомендуется включить отдельным разделом в соответствующие положения и инструкции участника.

11.3. Рекомендуется разработать, согласовать службой информатизации, информационной безопасности и куратором и утвердить руководящим органом участника Порядок уничтожения неиспользуемой защищаемой информации на стадиях жизненного цикла объектов информационной инфраструктуры участка ПС БР. Рекомендуется выпускать общий Порядок уничтожения неиспользуемой защищаемой информации в организации, упомянутые вопросы включать в Порядок отдельным разделом.

11.4. К модели угроз ИБ участника рекомендуется прикладывать утвержденный его руководителем Перечень лиц, обладающих правами по воздействию на объекты информационной инфраструктуры участка ПС БР, которое может привести к нарушению предоставления услуг по осуществлению переводов денежных средств.