Проект

ЦЕНТРАЛЬНЫЙ БАНК РОССИЙСКОЙ ФЕДЕРАЦИИ

(БАНК РОССИИ)

П О Л О Ж Е Н И Е

«___» _____ 202_ г. № _____ -П

г. Москва

О требованиях к обеспечению защиты информации, содержащейся в Единой системе учета платежных карт

Настоящее Положение на основании части третьей статьи 9^2 Федерального закона от 27 июня 2011 года № 161-ФЗ «О национальной платежной системе» устанавливает требования к обеспечению защиты информации, содержащейся в единой системе учета платежных карт.

1. Оператор единой системы учета платежных карт должен осуществлять защиту информации, содержащейся в единой системе учета платежных карт, указанной в части пятой статьи 9^2 Федерального закона от 27 июня 2011 года № 161-ФЗ «О национальной платежной системе» (далее соответственно – защищаемая информация, Федеральный закон от 27 июня 2011 года № 161-ФЗ), при ее получении, подготовке, обработке, хранении и предоставлении (далее − защита информации).

В случае если защищаемая информация содержит персональные данные, оператор единой системы учета платежных карт должен применять меры по обеспечению безопасности персональных данных при их обработке в соответствии со статьей 19 Федерального закона от 27 июля 2006 года

№ 152-ФЗ «О персональных данных» (далее – Федеральный закон от 27 июля 2006 года № 152-ФЗ).

2. Оператор единой системы учета платежных карт должен обеспечивать применение организационных и технических мер защиты информации в отношении эксплуатируемых им автоматизированных систем, программного обеспечения, средств вычислительной техники, телекоммуникационного оборудования (далее при совместном упоминании − объекты информационной инфраструктуры) в рамках:

обеспечения защиты информации при управлении доступом к объектам информационной инфраструктуры, включая идентификацию, аутентификацию, авторизацию (разграничение доступа) при осуществлении логического доступа;

обеспечения защиты вычислительных сетей, включая защиту информации, передаваемой по вычислительным сетям;

контроля целостности и защищенности объектов информационной инфраструктуры;

защиты объектов информационной инфраструктуры от вредоносного кода;

предотвращения утечек защищаемой информации;

управления инцидентами защиты информации, включая мониторинг и анализ событий защиты информации;

защиты среды виртуализации;

защиты информации при осуществлении удаленного логического доступа с использованием мобильных (переносных) устройств.

Оператор единой системы учета платежных карт должен обеспечить в отношении эксплуатируемых им объектов информационной инфраструктуры осуществление мероприятий по обнаружению, предупреждению, ликвидации последствий компьютерных атак и реагированию на компьютерные инциденты.

3. Оператор единой системы учета платежных карт должен осуществлять защиту информации с помощью средств криптографической защиты информации (далее − СКЗИ) в соответствии с Федеральным законом от 6 апреля 2011 года № 63-ФЗ «Об электронной подписи» (далее – Федеральный закон от 6 апреля 2011 года № 63-ФЗ), Положением о разработке, производстве, реализации и эксплуатации шифровальных (криптографических) средств защиты информации (Положение ПКЗ-2005), утвержденным приказом Федеральной службы безопасности Российской Федерации от 9 февраля 2005 года № 66[1] (далее – Положение ПКЗ-2005), Инструкцией об организации и обеспечении безопасности хранения, обработки и передачи по каналам связи с использованием средств криптографической защиты информации с ограниченным доступом, не содержащей сведений, составляющих государственную тайну, утвержденной приказом Федерального агентства правительственной связи и информации при Президенте Российской Федерации от 13 июня 2001 года № 152[2] и технической документацией на СКЗИ.

Оператор единой системы учета платежных карт должен обеспечивать безопасность персональных данных в том числе в соответствии с Составом и содержанием организационных и технических мер по обеспечению безопасности персональных данных при их обработке в информационных системах персональных данных, утвержденными приказом ФСТЭК России от 18 февраля 2013 г. № 21[3].

Обеспечение защиты персональных данных с использованием СКЗИ осуществляется в соответствии с постановлением Правительства Российской Федерации от 1 ноября 2012 года № 1119 «Об утверждении требований к защите персональных данных при их обработке в информационных системах персональных данных», приказом Федеральной службы безопасности

[1] Зарегистрирован Минюстом России 3 марта 2005 года, регистрационный № 6382, с изменениями, внесенными приказом ФСБ России от 12 апреля 2010 года № 173 (зарегистрирован Минюстом России 25 мая 2010 года, регистрационный № 17350).
[2] Зарегистрирован Минюстом России 6 августа 2001 года, регистрационный № 2848.
[3] Зарегистрирован Минюстом России 14 мая 2013 года, регистрационный № 28375.

Российской Федерации от 10 июля 2014 года № 378 «Об утверждении Состава и содержания организационных и технических мер по обеспечению безопасности персональных данных при их обработке в информационных системах персональных данных с использованием средств криптографической защиты информации, необходимых для выполнения установленных Правительством Российской Федерации требований к защите персональных данных для каждого из уровней защищенности»[1] (далее – приказ ФСБ России № 378) с применением СКЗИ, имеющих подтверждение соответствия требованиям, установленным федеральным органом исполнительной власти, уполномоченным в области обеспечения безопасности при осуществлении регулирования в соответствии с пунктом «ш» части первой статьи 13 Федерального закона от 3 апреля 1995 года № 40-ФЗ «О федеральной службе безопасности» (далее – требования, установленные федеральным органом исполнительной власти, уполномоченным в области обеспечения безопасности).

4. Оператор единой системы учета платежных карт в случаях, предусмотренных технической документацией на СКЗИ, должен проводить оценку влияния аппаратных, программно-аппаратных и программных средств сети (системы), используемых СКЗИ с целью защиты информации при ее передаче по каналам связи и (или) для защиты информации от несанкционированного доступа при ее обработке и хранении, совместно с которыми предполагается штатное функционирование СКЗИ, на выполнение предъявляемых к ним требований в соответствии с Положением ПКЗ-2005 по техническому заданию, согласованному с федеральным органом исполнительной власти, уполномоченным в области обеспечения безопасности при осуществлении регулирования в соответствии с пунктом «ш» части первой статьи 13 Федерального закона от 3 апреля 1995 года № 40-ФЗ «О федеральной службе безопасности». Контроль за выполнением оператором единой системы учета платежных карт мер по защите информации

[1] Зарегистрирован Минюстом России 18 августа 2014 года, регистрационный № 33620.

с использованием СКЗИ может осуществляться федеральным органом исполнительной власти, уполномоченным в области обеспечения безопасности при осуществлении регулирования в соответствии с пунктом «щ» части первой статьи 13 Федерального закона от 3 апреля 1995 года № 40-ФЗ «О федеральной службе безопасности».

Оператор единой системы учета платежных карт должен обеспечивать защиту криптографических ключей СКЗИ, используемых при обмене защищаемой информацией, в том числе ключей электронной подписи и ключей проверки электронной подписи (далее − криптографические ключи СКЗИ).

Безопасность процессов изготовления криптографических ключей СКЗИ должна обеспечиваться комплексом технологических мер защиты информации, организационных мер защиты информации и технических средств защиты информации в соответствии с технической документацией на СКЗИ. Принадлежность физическому или юридическому лицу ключа проверки электронной подписи, изготовленного средствами электронной подписи, подтверждается сертификатом ключа проверки электронной подписи, созданным и выданным удостоверяющим центром в соответствии с Федеральным законом от 6 апреля 2011 года № 63-ФЗ.

5. Оператор единой системы учета платежных карт должен осуществлять не реже одного раза в год тестирование объектов информационной инфраструктуры, обрабатывающих защищаемую информацию при приеме электронных сообщений, содержащих защищаемую информацию (далее − электронные сообщения), в автоматизированных системах и приложениях с использованием сети «Интернет» на предмет возможности несанкционированного доступа к обрабатываемой защищаемой информации.

Оператор единой системы учета платежных карт должен организовать непрерывный процесс управления уязвимостями, включающий мониторинг и выявление уязвимостей, их оценку и применимость к объектам

информационной инфраструктуры, определение методов и приоритетов устранения уязвимостей, устранение и контроль устранения выявленных уязвимостей.

6. Оператор единой системы учета платежных карт при использовании прикладного программного обеспечения автоматизированных систем и приложений, распространяемых оператором единой системы учета платежных карт среди пользователей единой системы учета платежных карт, являющихся кредитными организациями, филиалами иностранных банков (далее – пользователи единой системы учета платежных карт) для совершения действий в целях обмена защищаемой информацией, а также программного обеспечения, обрабатывающего защищаемую информацию при приеме электронных сообщений к исполнению в автоматизированных системах и приложениях в сети «Интернет», должен обеспечить проведение сертификации в системе сертификации федерального органа исполнительной власти, уполномоченного в области противодействия техническим разведкам и технической защиты информации при осуществлении регулирования в соответствии с подпунктом 13 пункта 8 Положения о Федеральной службе по техническому и экспортному контролю, утвержденного Указом Президента Российской Федерации от 16 августа 2004 года № 1085 (далее – сертификация), или оценки соответствия требованиям к оценочному уровню доверия (далее − ОУД) не ниже чем ОУД4[1] (далее − оценка соответствия прикладного программного обеспечения автоматизированных систем и приложений, а также отдельного программного обеспечения).

По решению оператора единой системы учета платежных карт оценка соответствия прикладного программного обеспечения автоматизированных систем и приложений, а также отдельного программного обеспечения проводится самостоятельно или с привлечением сторонних организаций,

[1] Подраздел 7.6 раздела 7 национального стандарта Российской Федерации ГОСТ Р ИСО/МЭК 15408-3-2013 «Информационная технология. Методы и средства обеспечения безопасности. Критерии оценки безопасности информационных технологий. Часть 3. Компоненты доверия к безопасности», утвержденного приказом Федерального агентства по техническому регулированию и метрологии от 8 ноября 2013 года № 1340-ст (М., ФГУП «Стандартинформ», 2014) и введенного в действие 1 сентября 2014 года.

имеющих лицензию на осуществление деятельности по технической защите конфиденциальной информации, на проведение работ и предоставление услуг, предусмотренных подпунктами «б», «д» или «е» пункта 4 Положения о лицензировании деятельности по технической защите конфиденциальной информации, утвержденного постановлением Правительства Российской Федерации от 3 февраля 2012 года № 79.

В отношении программного обеспечения и приложений, не указанных в абзаце первом настоящего пункта, оператор единой системы учета платежных карт должен самостоятельно определять необходимость сертификации или оценки соответствия прикладного программного обеспечения автоматизированных систем и приложений, а также отдельного программного обеспечения.

Оператор единой системы учета платежных карт в случае принятия решения о сертификации программного обеспечения автоматизированных систем и приложений, не указанных в абзаце первом настоящего пункта, должен обеспечить сертификацию программного обеспечения автоматизированных систем и приложений не ниже 4 уровня доверия в соответствии с приказом Федеральной службы по техническому и экспортному контролю от 2 июня 2020 года № 76[1].

Оператор единой системы учета платежных карт вправе не проводить сертификацию или оценку соответствия прикладного программного обеспечения автоматизированных систем и приложений, а также отдельного программного обеспечения (за исключением прикладного программного обеспечения, взаимодействующего с СКЗИ) в отношении разрабатываемого им программного обеспечения и приложений, если оператор единой системы учета платежных карт обеспечил сертификацию процессов безопасной разработки программного обеспечения ФСТЭК России на соответствие требованиям в части реализации безопасного жизненного цикла разработки программного

[1] Зарегистрирован Минюстом России 11 сентября 2020 года, регистрационный № 59772, с изменениями, внесенными приказом ФСТЭК России от 18 апреля 2022 года № 68 (зарегистрирован Минюстом России 20 июля 2022 года, регистрационный № 69318).

обеспечения и приложений, указанным в разделах 4 и 5 национального стандарта Российской Федерации ГОСТ Р 56939-2024 «Защита информации. Разработка безопасного программного обеспечения. Общие требования», утвержденного и введенного в действие с 20 декабря 2024 года приказом Федерального агентства по техническому регулированию и метрологии от 24 октября 2024 года № 1504-ст[1], при осуществлении полномочий в соответствии с подпунктами 13, 13(2) пункта 8, подпункта 9 пункта 9 Положения о Федеральной службе по техническому и экспортному контролю, утвержденного Указом Президента Российской Федерации от 16 августа 2004 года № 1085.

7. Оператор единой системы учета платежных карт должен обеспечивать защиту электронных сообщений при их передаче между пользователем единой системы учета платежных карт и оператором единой системы учета платежных карт посредством:

использования усиленной квалифицированной электронной подписи, сертификат ключа проверки которой выдан Банком России в соответствии с пунктом 3 части 2 статьи 17.2 Федерального закона от 6 апреля 2011 года № 63-ФЗ и реализуемой средствами электронной подписи не ниже класса КС1, предусмотренного пунктом 13 Требований к средствам электронной подписи, утвержденных приказом ФСБ России № 796 (далее - Требования к средствам электронной подписи), для контроля целостности и подтверждения подлинности электронных сообщений, в том числе применяемой для контроля целостности и подтверждения подлинности электронных сообщений пользователей единой системы учета платежных карт;

шифрования (расшифрования) электронных сообщений на сетевом уровне в соответствии с эталонной моделью взаимосвязи открытых систем, предусмотренной пунктом 1.7 раздела 1 государственного стандарта Российской Федерации ГОСТ Р ИСО/МЭК 7498-1-99 «Информационная

[1] М.: ФГБУ «Институт стандартизации», 2024.

технология. Взаимосвязь открытых систем. Базовая эталонная модель. Часть 1. Базовая модель»[1] (далее – ГОСТ Р ИСО/МЭК 7498-1-99), с использованием СКЗИ не ниже класса КС3, предусмотренного пунктом 12 Состава и содержания организационных и технических мер по обеспечению безопасности персональных данных при их обработке в информационных системах персональных данных с использованием средств криптографической защиты информации, необходимых для выполнения установленных Правительством Российской Федерации требований к защите персональных данных для каждого из уровней защищенности, утвержденных приказом ФСБ России № 378, прошедших процедуру оценки соответствия требованиям, установленным федеральным органом исполнительной власти, уполномоченным в области обеспечения безопасности;

отказа в приеме к исполнению электронных сообщений, не прошедших контроль и проверку, предусмотренные подпунктом 9.1 пункта 9 настоящего положения, контроль отсутствия вредоносного кода.

8. Оператор единой системы учета платежных карт должен хранить электронные сообщения, подписанные электронной подписью и признаваемые в соответствии со статьей 6 Федеральный закон от 6 апреля 2011 года № 63-ФЗ электронными документами, равнозначными документам на бумажном носителе, подписанным собственноручной подписью, и средства, обеспечивающие проверку электронной подписи, не менее пяти лет с даты подписания электронных сообщений.

9. Оператор единой системы учета платежных карт в части требований к защите информации, применяемых в отношении технологии обработки защищаемой информации, должен обеспечить конфиденциальность, целостность и достоверность защищаемой информации, регламентацию, реализацию, контроль (мониторинг) технологии обработки защищаемой информации, регистрацию результатов совершения действий, связанных с

[1] Принят постановлением Государственного комитета Российской Федерации по стандартизации и метрологии от 18 марта 1999 года N 78 (М., ИПК "Издательство стандартов", 1999) и введен в действие 1 января 2000 года.

осуществлением доступа к защищаемой информации, на следующих технологических участках:

идентификации, аутентификации и авторизации работников при осуществлении доступа к защищаемой информации, пользователей единой системы учета платежных карт при совершении действий в целях обработки, хранения и передачи защищаемой информации (далее − действия с защищаемой информацией);

формирования (подготовки), передачи и приема электронных сообщений;

удостоверения права пользователей единой системы учета платежных карт на совершение действий с защищаемой информацией;

осуществления действий с защищаемой информацией, учета результатов осуществления действий с защищаемой информацией, а также хранения электронных сообщений и информации об осуществленных действиях с защищаемой информацией.

9.1. Технология обработки защищаемой информации, применяемая при формировании (подготовке), передаче и приеме электронных сообщений, составляемых при взаимодействии оператора единой системы учета платежных карт и пользователя единой системы учета платежных карт, должна предусматривать:

структурный и логический контроль входящих электронных сообщений, в том числе проверку правильности заполнения полей электронного сообщения;

проверку правильности формирования (подготовки) исходящих электронных сообщений;

контроль дублирования электронного сообщения;

защиту информации, в том числе обеспечение ее целостности и конфиденциальности шифровальными (криптографическими) средствами, при ее передаче по каналам связи.

9.2. Технология обработки защищаемой информации, применяемая при удостоверении оператором единой системы учета платежных карт права пользователя единой системы учета платежных карт на совершение действий с защищаемой информацией, должна предусматривать:

подписание электронного сообщения пользователем единой системы учета платежных карт способом, указанным в абзаце втором пункта 7 настоящего Положения;

передачу сертификата ключа проверки электронной подписи с электронным сообщением.

9.3. Технология обработки защищаемой информации, применяемая при осуществлении действий с защищаемой информацией, учете результатов осуществления действий с защищаемой информацией, а также хранении электронных сообщений и информации об осуществленных действиях с защищаемой информацией, должна предусматривать:

регистрацию действий работников по доступу к защищаемой информации;

регистрацию исполненных запросов о предоставлении защищаемой информации пользователями единой системы учета платежных карт;

создание резервных копий баз данных, содержащих защищаемую информацию, в целях обеспечения доступности защищаемой информации;

хранение и целостность предоставленной в единой системе учета платежных карт информации.

10. В целях обеспечения защиты информации оператор единой системы учета платежных карт должен регистрировать результаты совершения следующих действий, связанных с осуществлением доступа к защищаемой информации:

идентификации, аутентификации и авторизации работников при осуществлении доступа к защищаемой информации, пользователей единой системы учета платежных карт при совершении действий с защищаемой информацией;

приема (передачи) электронных сообщений при взаимодействии оператора единой системы учета платежных карт с пользователями единой системы учета платежных карт, в том числе для удостоверения права пользователей единой системы учета платежных карт осуществлять действия с защищаемой информацией и для учета результатов осуществления действий с защищаемой информацией;

осуществления доступа работников к защищаемой информации и осуществления пользователями единой системы учета платежных карт действий с защищаемой информацией, выполняемых с использованием автоматизированных систем, программного обеспечения, в том числе подлежат регистрации следующие данные:

дата (день, месяц, год) и время (часы, минуты, секунды) совершения работником (пользователем единой системы учета платежных карт) действий с защищаемой информацией;

присвоенный работнику (пользователю единой системы учета платежных карт) идентификатор, позволяющий установить работника (пользователя единой системы учета платежных карт) в автоматизированной системе, программном обеспечении;

сведения, идентифицирующие технологический участок;

результат совершения пользователем единой системы учета платежных карт действия с защищаемой информацией («успешно» или «неуспешно»);

информация, используемая для идентификации устройств, при помощи которых осуществлен доступ к защищаемой информации, или устройств, к которым осуществлен доступ работниками (пользователями единой системы учета платежных карт) с использованием автоматизированных систем, программного обеспечения.

11. Оператор единой системы учета платежных карт должен осуществлять регистрацию инцидентов защиты информации, компьютерных инцидентов, указанных в пункте 5 статьи 2 Федерального закона от 26 июля 2017 года № 187-ФЗ «О безопасности критической информационной

инфраструктуры Российской Федерации» (далее - Федеральный закон от 26 июля 2017 года № 187-ФЗ), компьютерных атак, указанных в пункте 4 статьи 2 Федерального закона от 26 июля 2017 года № 187-ФЗ, случаев незаконного раскрытия защищаемой информации, указанной в пункте 1 настоящего Положения, а также представлять сведения о выявленных инцидентах защиты информации, компьютерных инцидентах, компьютерных атаках, случаях незаконного раскрытия защищаемой информации должностному лицу (отдельному структурному подразделению), ответственному за управление рисками, при соблюдении требований, предусмотренных абзацами вторым – пятым настоящего пункта.

По каждому инциденту защиты информации, компьютерному инциденту, компьютерной атаке, незаконному раскрытию защищаемой информации, оператор единой системы учета платежных карт должен осуществлять регистрацию:

сведений о защищаемой информации на технологических участках, на которых произошел несанкционированный доступ к защищаемой информации;

сведений, позволяющих выявить причину возникновения инцидента защиты информации, компьютерного инцидента;

результата реагирования на инцидент защиты информации, компьютерный инцидент, компьютерную атаку.

12. В целях реализации требований к обеспечению защиты информации оператор единой системы учета платежных карт должен информировать Банк России:

о выявленных оператором единой системы учета платежных карт инцидентах защиты информации, компьютерных инцидентах, компьютерных атаках, случаях незаконного раскрытия защищаемой информации, причинах их возникновения;

о результатах мероприятий по реагированию на инцидент защиты информации, компьютерный инцидент, и принятию мер по ликвидации последствий компьютерных атак;

о принадлежащих оператору единой системы учета платежных карт и (или) администрируемых в его интересах сайтах в сети «Интернет», которые используются оператором единой системы учета платежных карт для осуществления своей деятельности;

о планируемых мероприятиях, включая выпуск пресс-релизов и проведение пресс-конференций, размещение информации на официальном сайте оператора единой системы учета платежных карт в сети «Интернет», в отношении инцидентов защиты информации не позднее одного рабочего дня до дня проведения мероприятия.

Оператор единой системы учета платежных карт должен представлять в Банк России указанные в абзацах втором – пятом настоящего пункта сведения с использованием технической инфраструктуры (автоматизированной системы) Банка России или резервного способа взаимодействия (при технической невозможности использования технической инфраструктуры (автоматизированной системы) Банка России), информация о котором размещается на официальном сайте Банка России в сети «Интернет».

Предоставление оператором единой системы учета платежных карт в Банк России сведений, указанных в абзацах втором – третьем настоящего пункта, осуществляется в сроки, определенные приложением к настоящему Положению.

13. В целях обеспечения защиты информации оператор единой системы учета платежных карт должен осуществлять хранение информации об инцидентах защиты информации и данных, указанных в абзацах четвертом – девятом пункта 10 настоящего Положения, не менее пяти лет с даты их формирования оператором единой системы учета платежных карт (даты поступления в единую систему учета платежных карт).

14. При обеспечении безопасности объектов информационной

инфраструктуры, которые являются объектами критической информационной инфраструктуры Российской Федерации, применяются в том числе требования и порядок, установленные органами государственной власти Российской Федерации в области обеспечения безопасности критической информационной инфраструктуры в соответствии со статьей 6 Федерального закона от 26 июля 2017 года № 187-ФЗ.

15. Настоящее Положение подлежит официальному опубликованию и в соответствии с решением Совета директоров Банка России вступает в силу со дня официального опубликования, но не ранее 1 сентября 2026 года.

Председатель
Центрального банка
Российской Федерации Э.С. Набиуллина

Приложение
к Положению Банка России
от __ _____ 202__ года № _____-П
«О требованиях к обеспечению защиты информации, содержащейся в Единой системе учета платежных карт»

Сроки предоставления оператором единой системы учета платежных карт сведений о выявленных инцидентах защиты информации, о принятых мерах и проведенных мероприятиях по реагированию на выявленный инцидент защиты информации

№ п/п	Вид сведений	Срок предоставления
1	2	3
1	Сведения о выявлении инцидента защиты информации	В течение 3 часов с момента выявления инцидента защиты информации, и (или) незаконного раскрытия защищаемой информации, указанной в пункте 1 настоящего Положения
2	Сведения о выявлении незаконного раскрытия защищаемой информации, указанной в пункте 1 настоящего Положения	
3	Сведения о результатах расследования инцидента защиты информации или незаконного раскрытия защищаемой информации, указанной в пункте 1 настоящего Положения	В течение 30 дней со дня направления в Банк России сведений о выявлении инцидента защиты информации, или незаконного раскрытия защищаемой информации, указанной

1	2	3
		в пункте 1 настоящего Положения
4	Сведения о компьютерных инцидентах	В течение 3 часов с момента обнаружения компьютерного инцидента в случае его связи с функционированием значимого объекта критической информационной инфраструктуры. В течение 24 часов с момента обнаружения компьютерного инцидента во всех иных случаях
5	Сведения о компьютерных атаках	В течение 24 часов с момента обнаружения компьютерной атаки
6	Сведения о результатах мероприятий по реагированию на компьютерные инциденты и принятию мер по ликвидации последствий компьютерных атак	Не позднее 48 часов после завершения мероприятий по реагированию на компьютерные инциденты и принятию мер по ликвидации последствий компьютерных атак
7	Сведения о ликвидации последствий компьютерных атак и принятии мер по восстановлению функционирования и проверке работоспособности объектов информационной инфраструктуры	В течение 24 часов с момента завершения таких мер