ЦЕНТРАЛЬНЫЙ БАНК РОССИЙСКОЙ ФЕДЕРАЦИИ
(БАНК РОССИИ)

Методические рекомендации Банка России по организации взаимодействия информационных систем организаций финансового рынка с инфраструктурой, обеспечивающей информационно-технологическое взаимодействие информационных систем, используемых для предоставления государственных и муниципальных услуг и исполнения государственных и муниципальных функций в электронной форме

30.09.2024 № 16-МР

Глава 1. Общие положения

1.1. Настоящие Методические рекомендации Банка России разработаны в целях обеспечения единства подходов кредитных организаций, некредитных финансовых организаций, которые осуществляют указанные в части первой статьи 76.1 Федерального закона от 10 июля 2002 года № 86-ФЗ «О Центральном банке Российской Федерации (Банке России)» виды деятельности, субъектов национальной платежной системы, лиц, оказывающих профессиональные услуги на финансовом рынке (далее при совместном упоминании – организации финансового рынка), к организации взаимодействия их информационных систем с инфраструктурой, обеспечивающей информационно-технологическое взаимодействие информационных систем, используемых для предоставления государственных и муниципальных услуг и исполнения государственных и муниципальных функций в электронной форме (далее – инфраструктура электронного правительства).

1.2. Организациям финансового рынка рекомендуется руководствоваться настоящими Методическими рекомендациями Банка

России при взаимодействии их информационных систем с инфраструктурой электронного правительства в целях:

обеспечения санкционированного доступа к информации, содержащейся в информационных системах, с использованием федеральной государственной информационной системы «Единая система идентификации и аутентификации в инфраструктуре, обеспечивающей информационно-технологическое взаимодействие информационных систем, используемых для предоставления государственных и муниципальных услуг в электронной форме» (далее – ЕСИА), включая инфраструктуру, обеспечивающую доступ физических лиц (граждан Российской Федерации, иностранных граждан, лиц без гражданства), юридических лиц, индивидуальных предпринимателей к имеющимся в распоряжении государственных органов и органов местного самоуправления сведениям и документам, используемым для предоставления государственных и муниципальных услуг, исполнения государственных и муниципальных функций, и к сведениям, сформированным в результате их оказания и исполнения и содержащимся в государственных и муниципальных информационных системах (далее − необходимые сведения), а также доступ организаций к необходимым сведениям о физическом лице (гражданине Российской Федерации, иностранном гражданине, лице без гражданства), юридическом лице, индивидуальном предпринимателе, в том числе по инициативе или с согласия физического лица (гражданина Российской Федерации, иностранного гражданина, лица без гражданства), юридического лица, индивидуального предпринимателя (далее − инфраструктура Цифрового профиля);

использования сертификата ключа проверки усиленной неквалифицированной электронной подписи, созданного в инфраструктуре электронного правительства.

1.3. Организациям финансового рынка рекомендуется обеспечивать защиту информации при взаимодействии их информационных систем с инфраструктурой электронного правительства с применением средств

криптографической защиты информации, имеющих подтверждение соответствия требованиям, установленным федеральным органом исполнительной власти, уполномоченным в области обеспечения безопасности (далее – СКЗИ), разработанных и эксплуатируемых в соответствии с Положением о разработке, производстве, реализации и эксплуатации шифровальных (криптографических) средств защиты информации (далее – Положение ПКЗ-2005), утвержденным приказом ФСБ России от 9 февраля 2005 года № 66[1] и технической документацией на СКЗИ.

1.4. Организациям финансового рынка при взаимодействии их информационных систем с инфраструктурой электронного правительства рекомендуется применять средства защиты информации, прошедшие сертификацию в системе сертификации ФСТЭК России на соответствие требованиям по безопасности информации.

Глава 2. Рекомендации по организации взаимодействия информационных систем организаций финансового рынка с инфраструктурой электронного правительства в целях обеспечения санкционированного доступа к информации, содержащейся в информационных системах

2.1. Организациям финансового рынка рекомендуется при организации взаимодействия их информационных систем с ЕСИА руководствоваться Регламентом информационного взаимодействия участников с оператором ЕСИА и оператором эксплуатации инфраструктуры электронного правительства и иными документами об организации взаимодействия с ЕСИА, размещенными по адресу https://digital.gov.ru/ru/documents/.

2.2. Организациям финансового рынка рекомендуется организовать взаимодействие их информационных систем с ЕСИА с применением протокола на базе OpenID Connect, безопасная реализация которого

[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).

подтверждена положительным заключением ФСБ России о соответствии требованиям по безопасности информации, руководствуясь Методическими рекомендациями по использованию ЕСИА, размещенными по адресу https://digital.gov.ru/ru/documents/6186/, а также посредством единой системы межведомственного электронного взаимодействия (далее – СМЭВ), руководствуясь рекомендациями по работе со СМЭВ, размещенными по адресу https://info.gosuslugi.ru/new/smev, а также материалами по использованию личного кабинета участника взаимодействия, размещенными по адресу https://lkuv.gosuslugi.ru/paip-portal/#/main/.

2.3. Организациям финансового рынка рекомендуется использовать форматы сообщений, соответствующие видам сведений СМЭВ, размещенным по адресу https://lkuv.gosuslugi.ru/paip-portal/#/main/.

2.4. Организациям финансового рынка рекомендуется при взаимодействии их информационных систем с инфраструктурой Цифрового профиля руководствоваться Методическими рекомендациями по интеграции с REST API Цифрового профиля и Сценариями использования инфраструктуры Цифрового профиля и Цифрового профиля организации, размещенными по адресу https://digital.gov.ru/ru/documents/, а также видами сведений СМЭВ, размещенными по адресу https://lkuv.gosuslugi.ru/paip-portal/#/main/.

2.5. При осуществлении обмена электронными сообщениями, содержащими конфиденциальную информацию (не содержащей сведения, составляющие государственную тайну, но защищаемую в соответствии с законодательством Российской Федерации) и (или) персональные данные, организациям финансового рынка рекомендуется:

обеспечивать целостность электронных сообщений с использованием усиленной электронной подписи, реализуемой средствами электронной подписи класса не ниже КС3, предусмотренными 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 от 10 июля 2014 года № 378[1] (далее – Состав и содержание организационных и технических мер), а также пунктом 15 Требований к средствам электронной подписи, утвержденных приказом ФСБ России от 27 декабря 2011 года № 796[2] (далее – Требования к средствам электронной подписи);

обеспечивать конфиденциальность электронных сообщений с использованием СКЗИ класса не ниже КС3, предусмотренных пунктом 12 Состава и содержания организационных и технических мер.

2.6. Организациям финансового рынка рекомендуется при организации взаимодействия их информационных систем с ЕСИА руководствоваться Рекомендациями по обеспечению информационной безопасности при взаимодействии информационных систем организаций финансового рынка с инфраструктурой электронного правительства, приведенными в приложении к настоящим Методическим рекомендациям Банка России.

2.7. Организациям финансового рынка рекомендуется размещать объекты информационной инфраструктуры, используемые при взаимодействии с инфраструктурой электронного правительства, в выделенных (отдельных) сегментах (группах сегментов) вычислительных сетей.

2.8. Для объектов информационной инфраструктуры в пределах выделенных (отдельных) сегментов (группы сегментов) вычислительных

---

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

[2] Зарегистрирован Минюстом России 9 февраля 2012 года, регистрационный № 23191, с изменениями, внесенными приказами ФСБ России от 4 декабря 2020 года № 555 (зарегистрирован Минюстом России 30 декабря 2020 года, регистрационный № 61972), от 13 апреля 2021 года № 142 (зарегистрирован Минюстом России 20 мая 2021 года, регистрационный № 63528), от 13 апреля 2022 года № 179 (зарегистрирован Минюстом России 11 мая 2022 года, регистрационный № 68446).

сетей, в отношении которых применяются меры защиты информации, реализующие стандартный уровень защиты информации (уровень 2), определенный национальным стандартом Российской Федерации ГОСТ Р 57580.1-2017 «Безопасность финансовых (банковских) операций. Защита информации финансовых организаций. Базовый состав организационных и технических мер», утвержденным приказом Росстандарта от 8 августа 2017 года № 822-ст «Об утверждении национального стандарта Российской Федерации»[1], организациям финансового рынка рекомендуется обеспечивать уровень соответствия защиты информации не ниже четвертого в соответствии с ГОСТ Р 57580.2-2018 «Безопасность финансовых (банковских) операций. Защита информации финансовых организаций. Методика оценки соответствия», утвержденным приказом Росстандарта от 28 марта 2018 года № 156-ст «Об утверждении национального стандарта Российской Федерации»[2].

2.9. Обращаем внимание на необходимость обеспечить при организации взаимодействия и присоединения информационных систем организаций финансового рынка к ЕСИА, СМЭВ и инфраструктуре Цифрового профиля реализацию мер, указанных в пункте 11 Положения об инфраструктуре, обеспечивающей информационно-технологическое взаимодействие информационных систем, используемых для предоставления государственных и муниципальных услуг и исполнения государственных и муниципальных функций в электронной форме, утвержденного постановлением Правительства Российской Федерации от 8 июня 2011 года № 451, и пункте 5 Правил присоединения информационных систем организаций к инфраструктуре, обеспечивающей информационно-технологическое взаимодействие информационных систем, используемых для предоставления государственных и муниципальных услуг и исполнения государственных и муниципальных функций в электронной

[1] М., ФГУП «Стандартинформ», 2017.
[2] М., ФГУП «Стандартинформ», 2018.

форме, утвержденных постановлением Правительства Российской Федерации от 22 декабря 2012 года № 1382 «О присоединении информационных систем организаций к инфраструктуре, обеспечивающей информационно-технологическое взаимодействие информационных систем, используемых для предоставления государственных и муниципальных услуг и исполнения государственных и муниципальных функций в электронной форме».

Глава 3. **Рекомендации по организации взаимодействия информационных систем организаций финансового рынка с инфраструктурой электронного правительства в целях использования в ней сертификата ключа проверки усиленной неквалифицированной электронной подписи**

3.1. Организациям финансового рынка при организации взаимодействия своих информационных систем с инфраструктурой электронного правительства с целью использования в ней сертификата ключа проверки усиленной неквалифицированной электронной подписи согласно Правилам создания и использования сертификата ключа проверки усиленной неквалифицированной электронной подписи в инфраструктуре, обеспечивающей информационно-технологическое взаимодействие информационных систем, используемых для предоставления государственных и муниципальных услуг в электронной форме, утвержденным постановлением Правительства Российской Федерации от 1 декабря 2021 года № 2152 «Об утверждении Правил создания и использования сертификата ключа проверки усиленной неквалифицированной электронной подписи в инфраструктуре, обеспечивающей информационно-технологическое взаимодействие информационных систем, используемых для предоставления государственных и муниципальных услуг в электронной форме», рекомендуется руководствоваться материалами об интеграции с соответствующей инфраструктурой, размещенными по адресу https://partners.gosuslugi.ru/catalog/goskey/.

3.2. Организациям финансового рынка рекомендуется осуществлять взаимодействие, указанное в пункте 3.1 настоящих Методических рекомендаций

Банка России, посредством СМЭВ, руководствуясь рекомендациями по работе со СМЭВ, размещенными по адресу https://info.gosuslugi.ru/new/smev, а также материалами по использованию личного кабинета участника взаимодействия, размещенными по адресу https://lkuv.gosuslugi.ru/paip-portal/#/main/.

3.3. Организациям финансового рынка рекомендуется использовать форматы сообщений, соответствующие видам сведений СМЭВ, размещенным по адресу https://partners.gosuslugi.ru/catalog/goskey/, а также по адресу https://lkuv.gosuslugi.ru/paip-portal/#/main/.

3.4. Организациям финансового рынка рекомендуется обеспечивать проверку соответствия (сверку) подписи документов, поступивших из инфраструктуры электронного правительства после их подписания клиентами организаций финансового рынка, на неизменность (соответствие) первичным документам, сформированным клиентами организаций финансового рынка и направленным в инфраструктуру электронного правительства.

Глава 4. **Заключительные положения**

4.1. Настоящие Методические рекомендации Банка России подлежат опубликованию в «Вестнике Банка России» и размещению на официальном сайте Банка России в информационно-телекоммуникационной сети «Интернет».

Заместитель
Председателя Банка России Г.А. Зубарев

Приложение
к Методическим рекомендациям
Банка России по организации
взаимодействия информационных
систем организаций финансового
рынка с инфраструктурой,
обеспечивающей информационно-
технологическое взаимодействие
информационных систем,
используемых для предоставления
государственных и муниципальных
услуг и исполнения
государственных и муниципальных
функций в электронной форме

Рекомендации по обеспечению информационной безопасности при взаимодействии информационных систем организаций финансового рынка с инфраструктурой электронного правительства

1. Организациям финансового рынка в целях обеспечения безопасности реализации протокола на базе OpenID Connect рекомендуется:

обеспечивать целостность электронных сообщений с использованием усиленной электронной подписи, реализуемой средствами электронной подписи класса не ниже КС3, предусмотренными пунктом 12 Состава и содержания организационных и технических мер, а также пунктом 15 Требований к средствам электронной подписи;

обеспечивать конфиденциальность электронных сообщений с использованием СКЗИ класса не ниже КС3, предусмотренных пунктом 12 Состава и содержания организационных и технических мер;

обеспечивать проведение тематических исследований по оценке влияния среды функционирования СКЗИ, включая используемое прикладное программное обеспечение и реализацию OpenID Connect, в соответствии с требованиями ФСБ России по информационной безопасности в порядке, а также в соответствии с пунктом 35 Положения ПКЗ-2005;

применять средства межсетевого экранирования, сертифицированные ФСТЭК России на соответствие требованиям к устройствам типа межсетевой экран не ниже 4-го класса защиты, с применением средств защиты информации от воздействий вредоносного кода, предназначенных для применения на серверах информационных систем (тип «А»), согласно Требованиям к межсетевым экранам, утвержденным приказом ФСТЭК России от 9 февраля 2016 года № 9[1], средств защиты от компьютерных атак, сертифицированных ФСТЭК России на соответствие требованиям к программным, программно-аппаратным или аппаратным средствам типа «системы обнаружения вторжений» не ниже 4-го класса защиты согласно Требованиям к системам обнаружения вторжений, утвержденным приказом ФСТЭК России от 6 декабря 2011 года № 638[2], либо средств, совмещающих в себе межсетевой экран и систему обнаружения вторжения (NGFW) не ниже 4-го класса защиты, сертифицированных согласно Требованиям по безопасности информации к многофункциональным межсетевым экранам уровня сети, утвержденным приказом ФСТЭК России от 7 марта 2023 года № 44[3];

применять антивирусные средства, сертифицированные ФСТЭК России на соответствие требованиям к антивирусным средствам не ниже 4-го класса защиты согласно Требованиям к средствам антивирусной защиты, утвержденным приказом ФСТЭК России от 20 марта 2013 года № 28[4];

применять квалифицированный сертификат ключа проверки электронной подписи, созданного в соответствии с Федеральным законом от 6 апреля 2011 года № 63-ФЗ «Об электронной подписи» удостоверяющим центром Банка России.

2. Организациям финансового рынка в целях обеспечения защиты каналов связи при подключении пользователей к ЕСИА рекомендуется

---

[1] Зарегистрирован Минюстом России 25 марта 2016 года, регистрационный № 41564.
[2] Зарегистрирован Минюстом России 1 февраля 2012 года, регистрационный № 23088.
[3] Зарегистрирован Минюстом России 14 июня 2023 года, регистрационный № 73832.
[4] Зарегистрирован Минюстом России 3 мая 2012 года, регистрационный № 24045.

обеспечивать защиту всех каналов связи, находящихся вне пространства, в пределах которого организацией финансового рынка осуществляется контроль за пребыванием и действиями лиц и (или) транспортных средств (контролируемая зона), с помощью СКЗИ класса не ниже КС3, предусмотренных пунктом 12 Состава и содержания организационных и технических мер, находящихся в контролируемой зоне организации финансового рынка и обеспечивающих криптографическую аутентификацию канала связи.

При взаимодействии с использованием протокола защиты транспортного уровня (протокол TLS), за исключением случая, указанного в абзаце третьем настоящего пункта, организациям финансового рынка рекомендуется осуществлять аутентификацию с использованием сертификата безопасности, а также применять СКЗИ класса не ниже КС3, предусмотренные пунктом 12 Состава и содержания организационных и технических мер, на стороне организации финансового рынка, а также обеспечить применение СКЗИ класса не ниже КС1, предусмотренных пунктом 10 Состава и содержания организационных и технических мер, на стороне пользователя.

При взаимодействии организации финансового рынка с пользователем с использованием мобильного приложения, предоставленного организацией финансового рынка, при подключении пользователей к ЕСИА организациям финансового рынка рекомендуется использовать протокол защиты транспортного уровня (протокол TLS), обеспечивающий одностороннюю аутентификацию, а также обеспечить применение СКЗИ класса не ниже КС1, предусмотренных пунктом 10 Состава и содержания организационных и технических мер.