ЦЕНТРАЛЬНЫЙ БАНК РОССИЙСКОЙ ФЕДЕРАЦИИ
(БАНК РОССИИ)

Методические рекомендации Банка России по нейтрализации организациями финансового рынка угроз безопасности, актуальных при обработке биометрических персональных данных, векторов единой биометрической системы, проверке и передаче информации о степени соответствия векторов единой биометрической системы предоставленным биометрическим персональным данным физического лица в информационных системах организаций финансового рынка, осуществляющих аутентификацию на основе биометрических персональных данных физических лиц, за исключением единой биометрической системы, а также актуальных при взаимодействии информационных систем организаций финансового рынка, иных организаций, индивидуальных предпринимателей с указанными информационными системами

09.10.2024 № 19-МР

Глава 1. Общие положения

1.1. Настоящие Методические рекомендации разработаны в целях обеспечения единства подходов организаций финансового рынка, указанных в части 1 статьи 3 Федерального закона от 29 декабря 2022 года № 572-ФЗ «Об осуществлении идентификации и (или) аутентификации физических лиц с использованием биометрических персональных данных, о внесении изменений в отдельные законодательные акты Российской Федерации и признании утратившими силу отдельных положений законодательных актов Российской Федерации» (далее соответственно – организации финансового рынка, Федеральный закон от 29 декабря 2022 года № 572-ФЗ), к нейтрализации угроз безопасности, актуальных при обработке биометрических персональных данных, векторов единой биометрической системы, проверке и передаче информации о степени соответствия векторов единой биометрической системы предоставленным биометрическим персональным данным физического лица в информационных системах

организаций финансового рынка, осуществляющих аутентификацию на основе биометрических персональных данных физических лиц, за исключением единой биометрической системы, а также актуальных при взаимодействии информационных систем организаций финансового рынка, иных организаций, индивидуальных предпринимателей с указанными информационными системами, определенных Указанием Банка России от 25 сентября 2023 года № 6541-У «О перечне угроз безопасности, актуальных при обработке биометрических персональных данных, векторов единой биометрической системы, проверке и передаче информации о степени соответствия векторов единой биометрической системы предоставленным биометрическим персональным данным физического лица в информационных системах организаций финансового рынка, осуществляющих аутентификацию на основе биометрических персональных данных физических лиц, за исключением единой биометрической системы, а также актуальных при взаимодействии информационных систем организаций финансового рынка, иных организаций, индивидуальных предпринимателей с указанными информационными системами»[1] (далее – угрозы безопасности биометрических персональных данных).

1.2. Организациям финансового рынка рекомендуется принимать меры, направленные на нейтрализацию угроз безопасности биометрических персональных данных, векторов единой биометрической системы, информации о степени соответствия векторов единой биометрической системы предоставленным биометрическим персональным данным физического лица в информационных системах организаций финансового рынка, осуществляющих аутентификацию на основе биометрических персональных данных физических лиц, за исключением единой биометрической системы (далее – информация о степени соответствия), при использовании информационных систем, осуществляющих аутентификацию на основе биометрических персональных данных физических лиц, за

[1] Зарегистрировано Минюстом России 26 октября 2023 года, регистрационный № 75743.

исключением единой биометрической системы, а также при взаимодействии информационных систем организаций финансового рынка, иных организаций, индивидуальных предпринимателей с указанными информационными системам на следующих технологических участках:

1.2.1. Обработки биометрических персональных данных и информации о степени соответствия с использованием стационарных средств вычислительной техники и банкоматов, принадлежащих организациям финансового рынка, а также обработки биометрических персональных данных с использованием мобильных (переносных) устройств вычислительной техники (в том числе планшетов и электронных терминалов), принадлежащих организациям финансового рынка, устройств физического лица, оконечных устройств информационных систем, обеспечивающих функционирование контрольно-пропускных пунктов, в целях аутентификации физического лица с использованием биометрических персональных данных (далее – удаленная (дистанционная) аутентификация).

1.2.2. Обработки биометрических персональных данных, обработки, в том числе при получении и хранении, информации о степени соответствия, векторов единой биометрической системы в информационных системах организаций финансового рынка, осуществляющих аутентификацию на основе биометрических персональных данных физических лиц, в целях аутентификации физического лица, а также для рассмотрения обращений субъектов персональных данных, предполагающих неправомерную обработку их биометрических персональных данных при проведении аутентификации и (или) оспаривающих результаты проведения аутентификации.

1.2.3. Взаимодействия информационных систем организаций финансового рынка, иных организаций, индивидуальных предпринимателей с информационными системами организаций финансового рынка, осуществляющими аутентификацию на основе биометрических персональных данных физических лиц, в целях аутентификации физического лица.

1.2.4. Предоставления организациями финансового рынка в единую систему идентификации и аутентификации[1] сведений о физических лицах, содержащихся в информационных системах организаций финансового рынка, включая идентификаторы таких сведений, перед использованием информационных систем организаций финансового рынка, осуществляющих аутентификацию на основе биометрических персональных данных физических лиц, для аутентификации физических лиц.

1.3. Организациям финансового рынка рекомендуется обеспечить регистрацию действий, связанных с:

выполнением процедур идентификации, аутентификации, авторизации уполномоченных работников при доступе к объектам информационной инфраструктуры организаций финансового рынка, используемым на указанных в пункте 1.2 настоящих Методических рекомендаций технологических участках;

контролем обработки биометрических персональных данных в соответствии с целями, указанными в согласии физического лица на обработку его персональных данных и биометрических персональных данных;

назначением и изменением прав доступа уполномоченных работников к объектам информационной инфраструктуры организаций финансового рынка, используемым на указанных в пункте 1.2 настоящих Методических рекомендаций технологических участках;

уничтожением (удалением) биометрических персональных данных физических лиц на объектах информационной инфраструктуры организаций финансового рынка, используемых на указанных в пункте 1.2 настоящих Методических рекомендаций технологических участках;

формированием электронного сообщения, содержащего биометрические персональные данные физических лиц, для его передачи;

---

[1] Федеральная государственная информационная система «Единая система идентификации и аутентификации в инфраструктуре, обеспечивающей информационно-технологическое взаимодействие информационных систем, используемых для предоставления государственных и муниципальных услуг в электронной форме», обеспечивающая санкционированный доступ к информации, содержащейся в информационных системах (пункт 5 статьи 2 Федерального закона от 29 декабря 2022 года № 572-ФЗ).

подписанием электронных сообщений, содержащих биометрические персональные данные физических лиц, а также информацию о степени соответствия.

1.4. Организациям финансового рынка рекомендуется обеспечить хранение информации о регистрируемых действиях, указанных в пункте 1.3 настоящих Методических рекомендаций, не менее 5 лет.

1.5. Организациям финансового рынка рекомендуется обеспечивать обработку и хранение вместе с векторами единой биометрической системы и биометрическими персональными данными следующей информации:

об идентификаторе учетной записи в единой системе идентификации и аутентификации физического лица, чьи биометрические данные хранятся в информационной системе организации финансового рынка;

о метках даты и времени размещения биометрических персональных данных в информационной системе организации финансового рынка;

о способе размещения биометрических персональных данных в единой биометрической системе, в результате преобразования которых были созданы передаваемые векторы единой биометрической системы;

о параметрах технических средств, с использованием которых осуществлялся процесс аутентификации физического лица и обработки параметров биометрических персональных данных.

1.6. Организациям финансового рынка рекомендуется связывать векторы единой биометрической системы и биометрические персональные данные с идентификатором учетной записи физического лица в информационных системах организаций финансового рынка и идентификатором в единой системе идентификации и аутентификации.

1.7. Организациям финансового рынка рекомендуется использовать средства, реализующие методы обнаружения атак на биометрическое предъявление, в соответствии с национальным стандартом Российской Федерации ГОСТ Р 58624.1-2019 (ИСО/МЭК 30107-1:2016) «Информационные технологии. Биометрия. Обнаружение атаки на

биометрическое предъявление. Часть 1. Структура», утвержденным приказом Федерального агентства по техническому регулированию и метрологии от 31 октября 2019 года № 850-ст[1], национальным стандартом Российской Федерации ГОСТ Р 58624.2-2019 (ИСО/МЭК 30107-2:2017) «Информационные технологии. Биометрия. Обнаружение атаки на биометрическое предъявление. Часть 2. Форматы данных», утвержденным приказом Федерального агентства по техническому регулированию и метрологии от 31 октября 2019 года № 851-ст[2], и национальным стандартом Российской Федерации ГОСТ Р 58624.3-2019 (ИСО/МЭК 30107-3:2017) «Информационные технологии. Биометрия. Обнаружение атаки на биометрическое предъявление. Часть 3. Испытания и протоколы испытаний», утвержденным приказом Федерального агентства по техническому регулированию и метрологии от 20 ноября 2019 года № 1197-ст[3].

1.8. Организациям финансового рынка рекомендуется на периодической основе не реже 1 раза в год осуществлять контроль состояния объектов информационной инфраструктуры, используемых на указанных в пункте 1.2 настоящих Методических рекомендаций технологических участках.

Организациям финансового рынка рекомендуется определить работников, ответственных за контроль состояния объектов информационной инфраструктуры, используемых на указанных в пункте 1.2 настоящих Методических рекомендаций технологических участках.

1.9. Организациям финансового рынка рекомендуется разработать отдельную политику обработки, хранения и использования биометрических персональных данных.

---

[1] М., ФГУП «Стандартинформ», 2019.
[2] М., ФГУП «Стандартинформ», 2019.
[3] М., ФГУП «Стандартинформ», 2019.

Глава 2. Меры, направленные на нейтрализацию угроз безопасности биометрических персональных данных на технологическом участке обработки биометрических персональных данных и информации о степени соответствия с использованием стационарных средств вычислительной техники и банкоматов, принадлежащих организациям финансового рынка, а также обработки биометрических персональных данных с использованием мобильных (переносных) устройств вычислительной техники (в том числе планшетов и электронных терминалов), принадлежащих организациям финансового рынка, устройств физического лица, оконечных устройств информационных систем, обеспечивающих функционирование контрольно-пропускных пунктов, в целях удаленной (дистанционной) аутентификации

2.1. Организациям финансового рынка рекомендуется обеспечивать целостность и конфиденциальность электронных сообщений, содержащих биометрические персональные данные физических лиц, при обработке биометрических персональных данных с использованием мобильных (переносных) устройств вычислительной техники (в том числе планшетов и электронных терминалов), принадлежащих организациям финансового рынка, путем применения средств криптографической защиты информации (далее – СКЗИ) класса не ниже КС1, предусмотренных пунктом 10 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 Федеральной службы безопасности Российской Федерации от 10 июля 2014 года № 378[1] (далее – Состав и содержание организационных и технических мер), в случае применения средств (систем) защиты информации от несанкционированного доступа, прошедших оценку соответствия в форме обязательной сертификации не ниже 4-го уровня

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

доверия в соответствии с Требованиями по безопасности информации, устанавливающими уровни доверия к средствам технической защиты информации и средствам обеспечения безопасности информационных технологий, утвержденными приказом Федеральной службы по техническому и экспортному контролю от 2 июня 2020 года № 76[1], или применения СКЗИ класса не ниже КС2, предусмотренных пунктом 11 Состава и содержания организационных и технических мер, в иных случаях.

2.2. Организациям финансового рынка рекомендуется обеспечивать целостность и конфиденциальность электронных сообщений, содержащих биометрические персональные данные физических лиц и информацию о степени соответствия, при обработке биометрических персональных данных и информации о степени соответствия с использованием стационарных средств вычислительной техники и банкоматов, принадлежащих организациям финансового рынка, путем применения СКЗИ класса не ниже КС2, предусмотренных пунктом 11 Состава и содержания организационных и технических мер, а также пунктом 14 Требований к средствам электронной подписи, утвержденных приказом Федеральной службы безопасности Российской Федерации от 27 декабря 2011 года № 796[2] (далее – Требования к средствам электронной подписи).

2.3. Организациям финансового рынка рекомендуется обеспечивать целостность и конфиденциальность электронных сообщений, содержащих биометрические персональные данные физических лиц, при обработке биометрических персональных данных с использованием устройств физического лица, оконечных устройств информационных систем, обеспечивающих функционирование контрольно-пропускных пунктов,

---

[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).

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

в целях аутентификации физического лица путем применения СКЗИ класса не ниже КС1, предусмотренных пунктом 10 Состава и содержания организационных и технических мер.

2.4. Организациям финансового рынка рекомендуется обеспечить использование прикладного программного обеспечения автоматизированных систем и приложений, распространяемых организациями финансового рынка клиентам – физическим лицам для совершения действий в целях осуществления удаленной (дистанционной) аутентификации с использованием биометрических персональных данных физических лиц, прошедших сертификацию в системе сертификации Федеральной службы по техническому и экспортному контролю в соответствии с порядком, установленным постановлением Правительства Российской Федерации от 26 июня 1995 года № 608 «О сертификации средств защиты информации», или оценку соответствия по требованиям к оценочному уровню доверия (далее – ОУД) не ниже чем ОУД 4, предусмотренного пунктом 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[1] (далее – ГОСТ Р ИСО/МЭК 15408-3-2013).

2.5. Организациям финансового рынка рекомендуется разработать памятку, описывающую особенности работы программного обеспечения для аутентификации физического лица с использованием биометрических персональных данных на устройстве физического лица и возможные действия физического лица в случае реализации событий, связанных с компрометацией. Памятка также должна содержать основные положения эксплуатационной

[1] М., ФГУП «Стандартинформ», 2014.

документации используемых программных и (или) программно-аппаратных средств на устройстве клиента.

2.6. Организациям финансового рынка рекомендуется осуществлять контроль среды исполнения на устройствах физического лица, а также осуществлять сбор и хранение цифровых отпечатков таких устройств в соответствии со стандартом Банка России СТО БР БФБО-1.7-2023 «Безопасность финансовых (банковских) операций. Обеспечение безопасности финансовых сервисов с использованием технологии цифровых отпечатков устройств», который принят и введен в действие приказом Банка России от 1 марта 2023 года № ОД-335 и размещен на официальном сайте Банка России в информационно-телекоммуникационной сети «Интернет» в разделе «Информационная безопасность» / «Стандарты Банка России».

Глава 3. Меры, направленные на нейтрализацию угроз безопасности биометрических персональных данных на технологическом участке обработки биометрических персональных данных, обработки, в том числе при получении и хранении, информации о степени соответствия, векторов единой биометрической системы в информационных системах организаций финансового рынка, осуществляющих аутентификацию на основе биометрических персональных данных физических лиц, в целях аутентификации физического лица, а также для рассмотрения обращений субъектов персональных данных, предполагающих неправомерную обработку их биометрических персональных данных при проведении аутентификации и (или) оспаривающих результаты проведения аутентификации

3.1. Организациям финансового рынка рекомендуется при обработке электронных сообщений, содержащих биометрические персональные данные физического лица, а также при обработке, в том числе при получении и хранении, информации о степени соответствия, векторов единой биометрической системы в информационных системах организаций финансового рынка, осуществляющих аутентификацию на основе

биометрических персональных данных физических лиц, в целях аутентификации физического лица:

обеспечивать целостность биометрических персональных данных, информации о степени соответствия, векторов единой биометрической системы путем использования усиленной квалифицированной 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 биометрических персональных данных, информации о степени соответствия, векторов единой биометрической системы (при их получении из единой биометрической системы) путем применения СКЗИ класса не ниже КС3, предусмотренных пунктом 12 Состава и содержания организационных и технических мер.

3.2. Организациям финансового рынка рекомендуется обеспечивать целостность и конфиденциальность электронных сообщений, содержащих биометрические персональные данные физического лица, в том числе при хранении используемых в целях аутентификации биометрических персональных данных для рассмотрения обращений субъектов персональных данных, предполагающих неправомерную обработку их биометрических персональных данных при проведении аутентификации и (или) оспаривающих результаты проведения аутентификации, путем применения СКЗИ класса не ниже КС3, предусмотренных пунктом 12 Состава и содержания организационных и технических мер, а также пунктом 15 Требований к средствам электронной подписи.

3.3. Организациям финансового рынка рекомендуется обеспечить регистрацию действий работников, связанных с процессом удаленной (дистанционной) аутентификации, получения векторов единой биометрической системы, а также получения информации о степени соответствия векторов единой биометрической системы.

3.4. Организациям финансового рынка рекомендуется усилить внутренний контроль за обработкой биометрических персональных данных в соответствии с полученным согласием субъекта персональных данных, в том числе в соответствии с заявленной целью обработки биометрических персональных данных.

3.5. Организациям финансового рынка рекомендуется блокировать, удалять, уничтожать векторы единой биометрической системы гарантированным способом с использованием прошедших в установленном порядке процедуру оценки соответствия средств защиты информации при получении:

мотивированного запроса оператора единой биометрической системы о блокировании, об удалении, уничтожении векторов единой биометрической системы в случае отзыва субъектом персональных данных у оператора единой биометрической системы согласия на обработку биометрических персональных данных или получения оператором единой биометрической системы от субъекта персональных данных требования о блокировании, об удалении, уничтожении биометрических персональных данных и (или) векторов единой биометрической системы;

отзыва субъектом персональных данных согласия на обработку биометрических персональных данных или требования субъекта персональных данных о блокировании, об удалении, уничтожении биометрических персональных данных и (или) векторов единой биометрической системы.

3.6. Организациям финансового рынка рекомендуется проверять в своих информационных системах, осуществляющих аутентификацию на основе биометрических персональных данных, наличие обновленных векторов единой биометрической системы для целей аутентификации, а также проверять факт истечения срока их использования.

При этом рекомендуется удалять векторы единой биометрической системы после истечения срока их использования или при получении обновленных векторов единой биометрической системы.

Глава 4. Меры, направленные на нейтрализацию угроз безопасности биометрических персональных данных на технологическом участке взаимодействия информационных систем организаций финансового рынка, иных организаций, индивидуальных предпринимателей с информационными системами организаций финансового рынка, осуществляющими аутентификацию на основе биометрических персональных данных физических лиц, в целях аутентификации физического лица

4.1. Для обеспечения целостности и конфиденциальности электронных сообщений, содержащих биометрические персональные данные и информацию о степени соответствия, при взаимодействии информационных систем организаций финансового рынка, иных организаций, индивидуальных предпринимателей в целях аутентификации физического лица с информационными системами организаций финансового рынка, осуществляющими аутентификацию на основе биометрических персональных данных физических лиц, организациям финансового рынка рекомендуется применять СКЗИ класса не ниже КС3, предусмотренных пунктом 12 Состава и содержания организационных и технических мер, а также пунктом 15 Требований к средствам электронной подписи.

4.2. Организациям финансового рынка рекомендуется обеспечивать функционирование объектов информационной инфраструктуры для выполнения действий, указанных в пункте 4.1 настоящих Методических рекомендаций с применением протокола на базе OpenID Connect, предусмотренного Методическими рекомендациями по использованию единой системы идентификации и аутентификации, размещенными в информационно-телекоммуникационной сети «Интернет» по адресу https://digital.gov.ru/ru/documents/ (далее – протокол на базе OpenID Connect), безопасная реализация которого в составе подсистемы обработки

биометрических персональных данных подтверждена заключением ФСБ России о соответствии требованиям по безопасности информации.

4.3. Организациям финансового рынка в отношении процесса проведения работниками организаций финансового рынка аутентификации физического лица рекомендуется определить:

порядок информирования субъекта персональных данных в случае совершения непреднамеренных ошибок работниками организации финансового рынка;

порядок информирования субъекта персональных данных при возникновении инцидентов защиты информации.

Глава 5. Меры, направленные на нейтрализацию угроз безопасности биометрических персональных данных на технологическом участке предоставления организациями финансового рынка в единую систему идентификации и аутентификации сведений о физических лицах, содержащихся в информационных системах организаций финансового рынка, включая идентификаторы таких сведений, перед использованием информационных систем организаций финансового рынка, осуществляющих аутентификацию на основе биометрических персональных данных физических лиц, для аутентификации физических лиц

5.1. В целях обеспечения целостности и конфиденциальности электронных сообщений, содержащих персональные данные, при предоставлении организациями финансового рынка в единую систему идентификации и аутентификации сведений о физических лицах, содержащихся в информационных системах организаций финансового рынка, включая идентификаторы таких сведений, перед использованием информационных систем организаций финансового рынка, осуществляющих аутентификацию на основе биометрических персональных данных физических лиц, организациям финансового рынка рекомендуется применять СКЗИ класса не ниже КС3, предусмотренных пунктом 12 Состава и

содержания организационных и технических мер, а также пунктом 15 Требований к средствам электронной подписи.

5.2. Организациям финансового рынка рекомендуется руководствоваться Методическими рекомендациями по работе с единой системой идентификации и аутентификации, размещенными в информационно-телекоммуникационной сети «Интернет» по адресу https://digital.gov.ru/ru/documents/.

5.3. Организациям финансового рынка рекомендуется обеспечить регистрацию действий, связанных с:

процессом взаимодействия информационных систем организаций финансового рынка с единой системой идентификации и аутентификации, реализуемым в том числе с применением протокола на базе OpenID Connect, предусмотренного Методическими рекомендациями по использованию единой системы идентификации и аутентификации, размещенными в информационно-телекоммуникационной сети «Интернет» по адресу https://digital.gov.ru/ru/documents/;

процессом предоставления организациями финансового рынка в единую систему идентификации и аутентификации сведений о физических лицах, содержащихся в информационных системах организаций финансового рынка, включая идентификаторы таких сведений, перед использованием информационных систем организаций финансового рынка, осуществляющих аутентификацию на основе биометрических персональных данных физических лиц, для их аутентификации.

Глава 6. **Информирование Банка России об инцидентах при использовании информационных систем организаций финансового рынка, осуществляющих аутентификацию на основе биометрических персональных данных физических лиц, за исключением единой биометрической системы**

6.1. Организациям финансового рынка рекомендуется осуществлять регистрацию инцидентов защиты информации и инцидентов операционной

надежности при обработке, включая сбор и передачу, биометрических персональных данных в целях удаленной (дистанционной) аутентификации.

6.2. Организациям финансового рынка рекомендуется информировать Банк России о выявленных инцидентах защиты информации и инцидентах операционной надежности, включенных в перечень типов инцидентов, определенный стандартом Банка России СТО БР БФБО-1.5-2023 «Безопасность финансовых (банковских) операций. Управление инцидентами, связанными с реализацией информационных угроз, и инцидентами операционной надежности. О формах и сроках взаимодействия Банка России с кредитными организациями, некредитными финансовыми организациями и субъектами национальной платежной системы при выявлении инцидентов, связанных с реализацией информационных угроз, и инцидентов операционной надежности», который принят и введен в действие приказом Банка России от 8 февраля 2023 года № ОД-215 и размещен на официальном сайте Банка России в информационно-телекоммуникационной сети «Интернет» по адресу http://www.cbr.ru/information_security/ (далее – стандарт Банка России СТО БР БФБО-1.5-2023), а также о причинах возникновения инцидента защиты информации или операционной надежности, о принятых мерах и проведенных мероприятиях по реагированию на инцидент защиты информации или инцидент операционной надежности.

6.3. Организациям финансового рынка в целях информирования Банка России о выявленных инцидентах защиты информации и инцидентах операционной надежности рекомендуется руководствоваться порядком, а также сроками и формами взаимодействия организаций финансового рынка с Банком России, которые определены стандартом Банка России СТО БР БФБО-1.5-2023.

Глава 7. **Заключительные положения**

7.1. Настоящие Методические рекомендации 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