

Compliance-дайджест



Октябрь 2021

Compliance-дайджест: изменения законодательства в области ИБ за октябрь 2021 года

В нашем ежемесячном compliance-дайджесте собраны ключевые изменения требований регуляторов по информационной безопасности за октябрь 2021 года. Для вашего удобства все новости разбиты на 6 блоков: персональные данные, использование электронной подписи, биометрические персональные данные (на этот раз получился обширный блок), служебная тайна, функционирование ГосСОПКА, сертификация ФСТЭК России.

Персональные данные

1. Официально опубликован приказ Роскомнадзора от 14 сентября 2021 г. № 183 «[О внесении изменений в перечень иностранных государств, не являющихся сторонами Конвенции Совета Европы о защите физических лиц при автоматизированной обработке персональных данных и обеспечивающих адекватную защиту прав субъектов персональных данных, утвержденный приказом Федеральной службы по надзору в сфере связи, информационных технологий и массовых коммуникаций от 15 марта 2013 г. № 274](#)».

Из списка исключены следующие страны:

- Аргентинская Республика;
- Королевство Марокко;
- Республика Чили;
- Тунисская Республика.

Включены в обновленный перечень 11 стран:

- Республика Беларусь;
- Республика Узбекистан;
- Республика Таджикистан;
- Федеративная Республика Бразилия;
- Народная Республика Бангладеш;
- Социалистическая Республика Вьетнам
- Республика Замбия;
- Республика Нигер;
- Республика Чад;
- Тоголезская Республика;
- Федеративная Республика Нигерия.

2. Минцифры подготовило и представило для общественного обсуждения [проект ведомственного приказа «Об утверждении индикативных показателей для федерального государственного контроля \(надзора\) за обработкой персональных данных»](#).

3. Минцифры подготовило проект ведомственного приказа [«Об утверждении перечня индикаторов риска нарушения обязательных требований по федеральному государственному контролю \(надзору\) за обработкой персональных данных»](#).

Устанавливаются следующие индикаторы риска, используемые в качестве основания для проведения внеплановых контрольных (надзорных) мероприятий:

- выявление в течение шести месяцев более десяти фактов невыполнения однотипных требований об уточнении, блокировании или уничтожении недостоверных или полученных незаконным путем персональных данных, направленных различными лицами и (или) контролирующим органом (территориальным органом);
- поступление в течение шести месяцев более десяти информационных сообщений от различных лиц о доступе, распространении, предоставлении в информационно-телекоммуникационной сети «интернет» баз персональных данных, принадлежащих контролируемому лицу.

Использование электронной подписи

4. ФСБ России [представила для общественного обсуждения проект ведомственного приказа «О внесении изменений в Требования к средствам удостоверявшего центра, утвержденные приказом ФСБ России от 27 декабря 2011 г. № 796»](#).

Совместно со средствами, реализующими механизм меток доверенного времени, проектом предполагается применение некриптографических средств защиты информации, сертифицированных ФСТЭК или ФСБ России:

- защиту от атак, направленных на веб-серверы, в том числе путем контроля и фильтрации информационных потоков по протоколу передачи гипертекста проходящих к веб-серверу и от веб-сервера (WAF);
- защиту от вредоносного ПО;
- обнаружение (предотвращение) вторжений;
- доверенную загрузку средств вычислительной техники в том числе путем контроля локального доступа и целостности ПО средств вычислительной техники.

5. Официально опубликованы приказ Минцифры от 18 августа 2021 г.:

- № 856 [«О порядке формирования, актуализации классификатора полномочий и обеспечения доступа к нему».](#)
- № 857 [«Об утверждении единых требований к формам доверенностей, необходимых для использования квалифицированной электронной подписи».](#)
- № 858 [«Об утверждении единых требований к машиночитаемым формам документов о полномочиях».](#)

Биометрические персональные данные

Изменение порядка обработки биометрических персональных данных в ЕБС

6. Официально опубликован приказ Минцифры России от 10 сентября 2021 г. № 930 [«Об утверждении порядка обработки, включая сбор и хранение, параметров биометрических персональных данных, порядка размещения и обновления биометрических персональных данных в единой биометрической системе и в иных информационных системах, обеспечивающих идентификацию и \(или\) аутентификацию с использованием биометрических персональных данных физических лиц, а также требований к информационным технологиям и техническим средствам, предназначенным для обработки биометрических персональных данных в целях проведения идентификации».](#)

Определено, что хранение параметров биометрических персональных данных в иных информационных системах, обеспечивающих идентификацию и (или) аутентификацию с использованием биометрических персональных данных физлиц, собранных для проведения идентификации, не допускается.

Кроме этого, уточнены порядок размещения и обновления биометрических персональных данных в ЕБС и в иных информационных системах, обеспечивающих идентификацию и аутентификацию с использованием биометрических персональных данных физлиц, а также требования к информационным технологиям и техническим средствам, предназначенным для обработки биометрических персональных данных в целях проведения идентификации.

Приказ вступает в силу с 1 марта 2022 г., отменяя аналогичный приказ Минцифры России от 25 июня 2018 г. № 321.

Контроль и надзор в единой биометрической системе

7. Опубликовано указание Банка России от 21 сентября 2021 г. № 5936-У «[О порядке осуществления Банком России надзора за соблюдением банками и операторами финансовых платформ порядка размещения и обновления сведений, указанных в пункте 5.6 статьи 7 Федерального закона от 7 августа 2001 года № 115-ФЗ «О противодействии легализации \(отмыванию\) доходов, полученных преступным путем, и финансированию терроризма»](#)».

Обновлен порядок надзора Банком России за соблюдением требований к размещению сведений в ЕСИА, а также в ЕБС, документ заменяет собой указание Банка России от 17 октября 2018 г. № 4933-У.

Действие указания распространяется на кредитные организации и некредитные финансовые организации, являющиеся операторами финансовых платформ.

В рамках надзора Банк России проводит проверки полноты внесения сведений в ЕСИА и ЕБС, а также запрашивает документы и информацию, подтверждающие соблюдение порядка размещения и обновления сведений и биометрических персональных данных.

8. Официально опубликовано Постановление Правительства РФ от 30 сентября 2021 г. № 1657 «[Об утверждении Правил осуществления федеральным органом исполнительной власти, уполномоченным в области обеспечения безопасности, и федеральным органом исполнительной власти, уполномоченным в области противодействия техническим разведкам и технической защиты информации, контроля и надзора за выполнением органами, организациями, индивидуальными предпринимателями и нотариусами, указанными в части 18.2 статьи 14.1 Федерального закона «Об информации, информационных технологиях и о защите информации», организационных и технических мер по обеспечению безопасности персональных данных и использованием средств защиты информации, указанных в части 18.3 статьи 14.1 Федерального закона «Об информации, информационных технологиях и о защите информации»](#)».

Постановлением правительства установлен порядок осуществления ФСТЭК и ФСБ России мероприятий по контролю и надзору за выполнением организационных и технических мер по обеспечению безопасности персональных данных при использовании ЕБС.

Контроль осуществляется посредством проведения плановых и внеплановых проверок. Срок проведения плановой проверки не может превышать 20 рабочих дней. Срок проведения внеплановой проверки не может превышать 10 рабочих дней.

Срок проведения каждой из проверок в отношении оператора персональных данных, который осуществляет свою деятельность на территориях нескольких субъектов РФ, устанавливается отдельно по каждому филиалу, представительству и обособленному

структурному подразделению оператора персональных данных, при этом общий срок проведения проверки не может превышать 60 рабочих дней.

9. Официально опубликовано Постановление Правительства Российской Федерации от 20 октября 2021 г. № 1798 [«Об утверждении Правил осуществления Федеральной службой по надзору в сфере связи, информационных технологий и массовых коммуникаций и Федеральной службой безопасности Российской Федерации контроля и надзора за соблюдением многофункциональными центрами предоставления государственных и муниципальных услуг порядка размещения и обновления биометрических персональных данных в единой информационной системе персональных данных, обеспечивающей обработку, включая сбор и хранение, биометрических персональных данных, их проверку и передачу информации о степени их соответствия предоставленным биометрическим персональным данным физического лица»](#).

Установлен порядок осуществления Роскомнадзором и ФСБ России контроля и надзора за соблюдением МФЦ порядка размещения и обновления биометрических персональных данных в единой биометрической системе. Контроль осуществляется путем проведения совместных плановых и внеплановых выездных проверок. Срок проведения плановой проверки не должен превышать 20 рабочих дней, внеплановой проверки – 10 рабочих дней.

В случае выявления при проведении проверки нарушения установленных требований выдается предписание об устранении нарушения с указанием срока его устранения, принимаются меры по контролю за устранением выявленного нарушения.

10. Официально опубликовано Постановление Правительства Российской Федерации от 11 октября 2021 г. № 1729 [«Об утверждении Положения о федеральном государственном контроле \(надзоре\) в сфере идентификации и \(или\) аутентификации»](#).

Документ регулирует порядок осуществления государственного контроля в отношении аккредитованных организаций, осуществляющих идентификацию и (или) аутентификацию с использованием биометрических персональных данных, полномочия по его осуществлению контроля возложены на Минцифры России.

Установлены следующие виды плановых контрольных мероприятий: инспекционный визит, документарная проверка и выездная проверка в зависимости от категории риска причинения вреда (определены высокая, средняя и низкая категории).

Постановлением также определены особенности организации проведения профилактических мероприятий, к которым относятся информирование, обобщение правоприменительной практики, объявление предостережения, консультирование и профилактический визит.

Документ вступает в силу с 1 января 2022 г.

Требования к проверке простой электронной подписи для электронной формы согласия

11. Официально опубликовано Постановление Правительства Российской Федерации от 15 октября 2021 г. № 1754 «[Об утверждении требований к проверке простой электронной подписи, которой в соответствии с частями 5 и 23 статьи 14.1 Федерального закона «Об информации, информационных технологиях и о защите информации» подписаны согласия на обработку персональных данных и биометрических персональных данных, при хранении указанных согласий](#)».

Минцифры, согласно постановлению правительства, должно до 1 апреля 2022 г. обеспечить доработку ЕСИА для предоставления сервиса по проверке простой электронной подписи, которой подписаны согласия на обработку персональных и биометрических персональных данных при идентификации с использованием биометрических данных субъекта.

Проверка подлинности простой электронной подписи осуществляется оператором, которому предоставлено согласие на обработку персональных данных, посредством сервиса единой системы идентификации и аутентификации.

С использованием данного сервиса обеспечивается проверка подлинности простой электронной подписи, ключ которой хранится в системе не менее 5 лет, а также в случае замены лицом, подписавшим согласие на обработку персональных данных, ключа простой электронной подписи.

Результат проверки, содержащий в том числе сведения о дате и времени проверки, предоставляется оператору в электронной форме.

Единая биометрическая система и многофункциональные центры

12. Официально опубликовано Постановление Правительства Российской Федерации от 15 октября 2021 г. № 1753 «[Об утверждении требований к организационным и техническим условиям осуществления многофункциональными центрами предоставления государственных и муниципальных услуг размещения или обновления в единой системе идентификации и аутентификации сведений, необходимых для регистрации физических лиц в данной системе, размещения биометрических персональных данных в единой информационной системе персональных данных, обеспечивающей обработку, включая сбор и хранение, биометрических персональных данных, их проверку и передачу информации о степени их соответствия предоставленным биометрическим персональным данным физического лица, с использованием программно-технических комплексов](#)».

МФЦ обязаны использовать средства криптографической защиты информации. Они осуществляют мониторинг и контроль за техническим состоянием программно-технических комплексов, необходимых для приема документов, обработки, включая сбор

и хранение, передачи и проверки персональных данных, а также реализуют защиту от несанкционированного доступа. Кроме этого, постановлением закреплены требования к условиям размещения биометрических персональных данных в ЕБС. Определено, что возможность хранения биометрических персональных данных физлиц в МФЦ, а также в программно-технических комплексах при размещении или обновлении сведений должна быть исключена.

МФЦ должны будут обеспечить уполномоченных работников квалифицированными сертификатами ключей проверки электронной подписи.

Аккредитация организаций для обработки биометрических персональных данных

13. Официально опубликовано Постановление Правительства Российской Федерации от 20 октября 2021 г. № 1799 [«Об аккредитации организаций, владеющих информационными системами, обеспечивающими идентификацию и \(или\) аутентификацию с использованием биометрических персональных данных физических лиц, и \(или\) оказывающих услуги по идентификации и \(или\) аутентификации с использованием биометрических персональных данных физических лиц»](#).

С 1 января 2022 г. вступает в силу порядок аккредитации организаций, оказывающих услуги по идентификации и/или аутентификации с использованием биометрических персональных данных физических лиц, накладывающий существенные ограничения на организации, осуществляющие идентификацию и аутентификацию граждан по биометрическим данным, а именно требования к:

- минимальному размеру собственных средств (капитала) в 500 млн руб. для организаций, осуществляющих идентификацию и аутентификацию на основе биометрических данных (50 млн руб. для организаций, осуществляющих только аутентификацию на основе биометрических данных);
- наличию финансового обеспечения ответственности за убытки, причиненные третьим лицам, в сумме не менее чем 100 млн руб. (50 млн руб. для организаций, осуществляющих только аутентификацию на основе биометрических данных);
- документам, подтверждающим наличие права собственности на аппаратные шифровальные (криптографические) средства, используемые для оказания услуг по идентификации и (или) аутентификации с использованием биометрических персональных данных;
- составу персонала, имеющего высшее образование в области информационных технологий или информационной безопасности;
- наличию лицензии ФСБ на деятельность в области криптографии и использования сертифицированных СКЗИ;
- наличию подключения к ГосСОПКА;
- размещению оборудования только на территории РФ;
- запрету на аккредитацию иностранных юридических лиц из стран, входящих в перечень иностранных государств, совершающих недружественные действия в отношении РФ.

Аккредитация проводится Минцифры России и действует без ограничения срока. Постановление Правительства устанавливает: порядок приостановления и прекращения действия аккредитации; порядок внесения изменений в перечень аккредитованных организаций и изменения области аккредитации; дополнительные требования к аккредитации организаций, являющихся иностранными юридическими лицами.

14. Официально опубликовано Постановление Правительства Российской Федерации от 23 октября 2021 г. № 1815 [«Об утверждении перечня случаев осуществления сбора и обработки используемых для идентификации либо идентификации и аутентификации биометрических персональных данных в информационных системах организаций, осуществляющих идентификацию и \(или\) аутентификацию с использованием биометрических персональных данных физических лиц, а также случаев использования организациями, за исключением кредитных организаций, некредитных финансовых организаций, которые осуществляют указанные в части первой статьи 761 Федерального закона «О Центральном банке Российской Федерации \(Банке России\)» виды деятельности, субъектами национальной платежной системы, индивидуальными предпринимателями указанных информационных систем для идентификации либо идентификации и аутентификации физического лица, выразившего согласие на их проведение»](#).

С 1 марта 2022 г. устанавливаются случаи осуществления сбора и обработки используемых для идентификации либо идентификации и аутентификации биометрических персональных данных в информационных системах организаций, для которых в том числе требуется аккредитация:

- идентификация и (или) аутентификация водителей легкового такси;
- идентификация и (или) аутентификация пользователей краткосрочной аренды транспортных средств (каршеринга);
- идентификация и (или) аккредитация участников гражданско-правовых сообществ (есть исключения);
- идентификация и (или) аутентификация при проходе на территорию организаций посредством СКУД, за исключением следующих владельцев СКУД:
 - организаций ОПК,
 - организаций атомного энергопромышленного комплекса,
 - организаций ядерного оружейного комплекса,
 - организаций химического комплекса,
 - организаций ТЭК,
 - организаций – субъектов КИИ,
 - организаций – объектов транспортной инфраструктуры,
 - организаций, совершение террористического акта на территории которых может привести к возникновению чрезвычайной ситуации с опасными социально-экономическими последствиями согласно установленному категорированию,
 - режимных объектов,
 - дошкольных образовательных организаций и общеобразовательных организаций.

Служебная тайна

15. Министерство обороны России представило для общественного обсуждения [проект «Правил обращения со сведениями, составляющими служебную тайну в области обороны»](#), которые будут предназначаться для органов государственной власти Российской Федерации, органов государственной власти субъектов Российской Федерации, органов местного самоуправления и организаций, участвующих в организации и выполнении мероприятий в области обороны.

Функционирование ГосСОПКА

16. ФСБ России представила для общественного обсуждения [проект ведомственного приказа «О внесении изменений в приказ ФСБ России от 11 декабря 2013 г. № 747 «Об утверждении Перечня должностных лиц органов федеральной службы безопасности, уполномоченных составлять протоколы об административных правонарушениях, и о реализации отдельных положений Кодекса Российской Федерации об административных правонарушениях в органах федеральной службы безопасности» и утвержденный этим приказом Перечень»](#).

Данный перечень расширяет список должностных лиц, уполномоченных составлять протоколы об административных правонарушениях по нарушениям, связанным с обеспечением функционирования ГосСОПКА, в том числе на рассмотрение дел об административных правонарушениях, предусмотренных частями 2 и 3 статьи 13.12.1 и частью 2 статьи 19.7.15 КОАП.

Сертификация ФСТЭК России

17. Официально опубликован приказ ФСТЭК от 05 августа 2021 г. № 121 [«О внесении изменений в Положение о системе сертификации средств защиты информации, утвержденное приказом Федеральной службы по техническому и экспортному контролю от 3 апреля 2018 г. № 55»](#), который вносит в положение следующие изменения:

- Установлен запрет на сертификацию средств защиты информации иностранного производства, в отношении которых нормативными правовыми актами Российской Федерации установлены ограничения или запреты на их использование в Российской Федерации.
- Отменен срок действия сертификата соответствия для единичного образца или партии средства защиты информации. Определены условия, при которых серийно производимые средства защиты считаются сертифицированными в том числе после окончания срока действия сертификата соответствия.
- Уточнен порядок отбора образцов (образца) средства защиты информации для сертификационных испытаний.
- Упразднена процедура предварительного рассмотрения образца средства защиты информации и документации на него.

- Изменен порядок маркирования сертифицированных средств защиты информации.
- Сокращен объем испытаний сертифицированных средств защиты информации при продлении срока действия сертификата соответствия.