

Compliance- дайджест



Сентябрь 2021

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

В Compliance-дайджесте отражены ключевые изменения требований регуляторов по информационной безопасности за сентябрь 2021 года. Для вашего удобства все новости в выпуске разбиты на 7 блоков: в этот раз – изменения в области персональных данных, биометрических персональных данных, требований к финансовым организациям, военной и военно-технической деятельности РФ, лицензирования деятельности по работе со СКЗИ, использования электронной подписи и новости в области стандартизации.

Изменения в области персональных данных

1. Минцифры опубликовало проект приказа [«Об утверждении порядка уничтожения персональных данных, полученных в результате обезличивания, субъектом экспериментального правового режима в сфере цифровых инноваций в случае прекращения статуса субъекта экспериментального правового режима»](#).

Субъект экспериментального правового режима должен не позднее 1 рабочего дня осуществить блокирование обезличенных данных и в срок, не превышающий 7 рабочих дней, уничтожить обезличенные данные.

Для уничтожения обезличенных данных применяются прошедшие процедуру оценки соответствия средства защиты информации, в составе которых реализована функция уничтожения информации. Факт уничтожения обезличенных данных фиксируется в акте об их уничтожении.

В акте должна быть отражена информация: о дате, времени и месте составления акта, о носителях обезличенных данных, о перечне и объеме уничтоженной информации, а также

о средствах защиты информации, посредством которых осуществлено уничтожение. К акту прилагаются копии документов, материалы и иная информация, подтверждающая факт уничтожения обезличенных данных.

В случае непредоставления необходимых документов, контролирующий орган может принять решение о проведении в отношении субъекта экспериментального правового режима контрольных мероприятий.

2. В Государственную Думу внесен законопроект [«О ратификации Соглашения о взаимной помощи по административным вопросам в сфере обмена персональными данными»](#), в том числе вводящий новую трактовку термина персональные данные, под которыми теперь подразумевается «любая информация, прямо или косвенно относящаяся к физическому лицу, либо идентифицированному, либо которое может быть идентифицировано».

3. Официально опубликован приказ Минцифры от 7 июля 2021 г. № 686 [«О признании утратившими силу приказа Министерства связи и массовых коммуникаций Российской Федерации от 14.11.2011 № 312 «Об утверждении Административного регламента исполнения Федеральной службой по надзору в сфере связи, информационных технологий и массовых коммуникаций государственной функции по осуществлению государственного контроля \(надзора\) за соответствием обработки персональных данных требованиям законодательства Российской Федерации в области персональных данных» и внесенных в него изменений»](#).

Госконтроль за обработкой персональных данных теперь осуществляется в соответствии с постановлением Правительства Российской Федерации от 29 июня 2021 г. № 1046 [«О федеральном государственном контроле \(надзоре\) за обработкой персональных данных»](#).

Изменения в области биометрических персональных данных

4. Официально опубликован приказ Минцифры от 7 июля 2021 г. № 685 [«Об определении форм подтверждения соответствия информационных технологий и технических средств, предназначенных для обработки биометрических персональных данных, требованиям, определенным в соответствии с пунктом 1 части 13 статьи 14.1 Федерального закона от 27 июля 2006 г. № 149-ФЗ «Об информации, информационных технологиях и о защите информации»](#), заменяющий приказ Минцифры от 25 июня 2018 г. № 323.

5. Официально опубликован приказ Минцифры от 6 августа 2021 г. № 816 [«Об утверждении методик проверки соответствия предоставленных биометрических персональных данных физического лица его биометрическим персональным данным, содержащимся в информационных системах, обеспечивающих идентификацию и \(или\) аутентификацию с использованием биометрических персональных данных, а также об определении степени взаимного соответствия указанных биометрических персональных данных, достаточной для проведения идентификации, предусмотренной Федеральным](#)

[законом от 27 июля 2006 г. № 149-ФЗ «Об информации, информационных технологиях и о защите информации».](#)

Настоящий приказ устанавливает, что степень взаимного соответствия предоставленных биометрических персональных данных данным, содержащимся в информационных системах (в том числе в Единой биометрической системе), достаточная для проведения идентификации физического лица, должна составлять не менее 99,99 %.

Приказ отменяет действующую ранее методику, определенную приказом Минцифры от 21 июня 2018 г. № 307.

6. Официально опубликован приказ Минцифры от 25 мая 2021 г. № 494 «[Об утверждении перечня угроз безопасности, актуальных при обработке биометрических персональных данных, их проверке и передаче информации о степени их соответствия предоставленным биометрическим персональным данным физического лица 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, а также актуальных при взаимодействии государственных органов, органов местного самоуправления, индивидуальных предпринимателей, нотариусов и организаций, за исключением организаций финансового рынка, с указанной системой, с учетом оценки возможного вреда, проведенной в соответствии с законодательством Российской Федерации о персональных данных](#)».

Обзор угроз биометрическим персональным данным (БПДн) при обработке в ЕБС за исключением организаций финансового рынка и требований приведен в таблице ниже:

пп. Перечня угроз	Уровень реализации угрозы	Последствия реализации угрозы	Способ реализации угрозы	Меры защиты по приказу ФСБ РФ № 378
1.1.	При обработке, включая сбор, БПДн и передаче собранных БПДн между структурными подразделениями	• угроза нарушения целостности (подмены, удаления) БПДн, • нарушения конфиденциальности (компрометации) БПДн, • нарушения достоверности БПДн (внесения фиктивных БПДн)	Целенаправленные действия с использованием возможностей, указанных в пункте 12 приложения к приказу ФСБ РФ № 378	Защита каналов связи внутри организации с использованием СКЗИ класса КС3
1.2.	При обработке и передаче БПДн между структурными подразделениями	• угроза нарушения целостности (подмены, удаления) БПДн, • нарушения конфиденциальности (компрометации) БПДн, • нарушения достоверности БПДн	Целенаправленные действия с использованием возможностей, указанных в пункте 11 приложения к приказу ФСБ РФ № 378 при использовании СЗИ от	Защита каналов связи внутри организации с использованием СКЗИ класса КС2 в случае применения средств (систем)

		(внесения фиктивных БПДн)	НСД, сертифицированных на 4 уровень доверия	защиты информации от НСД
1.3.	При передаче собранных БПДн организацией и ЕБС	- угроза нарушения целостности (подмены, удаления) БПДн, - нарушения достоверности БПДн (внесения фиктивных БПДн)	Целенаправленные действия с использованием возможностей, указанных в пункте 13 приложения к приказу ФСБ РФ № 378	Защита с использованием СКЗИ класса КВ
1.4.	При передаче собранных БПДн организацией и ЕБС	угроза нарушения конфиденциальности (компрометации) БПДн	Целенаправленные действия с использованием возможностей, указанных в пункте 12 приложения к приказу ФСБ РФ № 378	Защита с использованием СКЗИ класса КС3
2	При обработке БПДн, сведений о степени соответствия на устройстве физического лица и передаче БПДн с устройства физического лица в ЕБС	- угроза нарушения целостности (подмены, удаления) БПДн, - угроза нарушения конфиденциальности (компрометации) БПДн	Целенаправленные действия с использованием возможностей, указанных в пункте 10 приложения к приказу ФСБ РФ № 378	Защита устройства клиента с использованием СКЗИ класса КС1
3	При передаче информации о степени соответствия в процессе идентификации физического лица	угроза нарушения целостности (подмены, удаления) информации о степени соответствия	Целенаправленные действия с использованием возможностей, указанных в пункте 13 приложения к приказу ФСБ РФ № 378	Защита с использованием СКЗИ класса КВ
4	При передаче информации о степени соответствия в процессе идентификации физического лица	угроза нарушения конфиденциальности (компрометации) информации о степени соответствия	Целенаправленные действия с использованием возможностей, указанных в пункте 12 приложения к приказу ФСБ РФ № 378	Защита с использованием СКЗИ класса КС3
5	При обработке информации в процессе аутентификации, а также при предоставлении в ЕСИА сведений о физических лицах перед использованием	угроза нарушения целостности (подмены, удаления) информации о степени соответствия	Целенаправленные действия с использованием возможностей, указанных в пункте 12 приложения к приказу ФСБ РФ № 378	Защита с использованием СКЗИ класса КС3

	ЕБС для аутентификации			
6	При обработке информации в процессе аутентификации	угроза нарушения конфиденциальности (компрометации) информации о степени соответствия	Целенаправленные действия с использованием возможностей, указанных в пункте 12 приложения к приказу ФСБ РФ № 378	Защита с использованием СКЗИ класса КСЗ
7	При обработке, хранении, проверке БПДн, обработке и передаче информации о степени соответствия в ЕБС и при взаимодействии с ЕСИА	- угроза нарушения целостности (подмены, удаления) БПДн, - нарушения конфиденциальности (компрометации) БПДн, - нарушения достоверности БПДн (внесения фиктивных БПДн), - нарушения целостности (подмены, удаления) информации о степени соответствия, нарушения доступности (блокирования передачи) информации о степени соответствия - нарушения доступности (блокирования передачи) информации о степени соответствия	Целенаправленные действия с использованием возможностей, указанных в пункте 13 приложения к приказу ФСБ РФ № 378	Защита с использованием СКЗИ класса КВ

7. Официально опубликован приказ Минцифры от 27 августа 2021г. № 896 [«Об утверждении требований к деловой репутации единоличного исполнительного органа или членов коллегиального исполнительного органа организации, владеющей информационной системой, обеспечивающей идентификацию и \(или\) аутентификацию с использованием биометрических персональных данных физических лиц, и \(или\) оказывающей услуги по идентификации и \(или\) аутентификации с использованием биометрических персональных данных физических лиц»](#) для аккредитации организаций, владеющих ИС, обеспечивающими идентификацию и (или) аутентификацию с использованием БПДн, в соответствии с требованиями ранее размещенного проекта постановления Правительства [«О порядке 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, для осуществления аутентификации, идентификации либо идентификации и аутентификации»](#).

Изменения требований к финансовым организациям

8. Банк России выпустил методические рекомендации от 6 сентября 2021 г. № 16-МР «[О повышении внимания кредитных организаций к отдельным операциям клиентов – физических лиц](#)», с рекомендациями по выявлению операций по переводу денежных средств, соответствующих следующим признакам:

- необычно большое количество контрагентов – физических лиц (плательщиков и (или) получателей), например, более 10 в день, более 50 в месяц.
- необычно большое количество операций по зачислению и (или) списанию безналичных денежных средств, проводимых с физическими лицами, например, более 30 операций в день.
- значительные объемы операций по списанию и (или) зачислению безналичных денежных средств, совершаемых между физическими лицами, например, более 100 тысяч рублей в день, более 1 миллиона рублей в месяц.
- короткий промежуток времени (одна минута и менее) между зачислением денежных средств и списанием.
- зачисление и списание средств в течение 12 часов одних суток.
- в течение недели средний остаток денежных средств на банковском счете на конец дня не превышает 10% от среднесуточного объема операций по банковскому счету в течение недели.
- отсутствие платежей в пользу юридических лиц для обеспечения жизнедеятельности физического лица (например, оплата коммунальных услуг, услуг связи, иных услуг, товаров, работ).
- совпадение идентификационной информации об устройстве, используемом разными физлицами для удаленного доступа к услугам банка.

При выявлении двух и более перечисленных признаков банкам рекомендовано принятие мер в соответствии с Федеральным законом от 7 августа 2001 года № 115-ФЗ «О противодействии легализации (отмыванию) доходов, полученных преступным путем, и финансированию терроризма», предусматривающих как возможность отказа в выполнении распоряжения клиента о совершении операции, так и расторжение договора с клиентом при более двух блокировок операций в течение года.

9. ЦБ опубликовал проект указания «[О внесении изменений в Указание Банка России от 8 октября 2018 года № 4927-У «О перечне, формах и порядке составления и представления форм отчетности кредитных организаций в Центральный банк Российской Федерации](#)», устанавливающий требования по новой форме 0409071 «Сведения об оценке выполнения кредитными организациями требований к обеспечению защиты информации», включающей сведения:

- Сведения об оценке выполнения требований по направлению «Технологические меры»
- Сведения об оценке выполнения требований по направлению «Безопасность программного обеспечения»
- Сведения об оценке выполнения требований по направлению «Безопасность информационной инфраструктуры» (о результатах оценки выполнения требований 683-П, 719-П, 747-П и 757-П, ГОСТ Р 57580)

- Сведения о проверяющей организации, в том числе о стоимости работ по оценке соответствия

Также проект указания вводит еще одну новую форму отчетности О409106 «Отчет по управлению операционным риском в кредитной организации», в том числе включающую отчетность по рискам информационной безопасности, связанным с нарушением защиты информации.

ЦБ РФ также опубликовал проект указания [«О формах, сроках и методиках составления и представления операторами услуг платежной инфраструктуры, операторами по переводу денежных средств отчетности о защите информации при осуществлении переводов денежных средств»](#), который заменит Указания Банка России от 9 июня 2012 года № 2831-У «Об отчетности по обеспечению защиты информации при осуществлении переводов денежных средств операторов платежных систем, операторов услуг платежной инфраструктуры, операторов по переводу денежных средств» с обновлением форм отчетности О403202 и О403203, также включающими сведения об оценке выполнения требований по направлению «Безопасность информационной инфраструктуры» (о результатах оценки выполнения требований ГОСТ Р 57580) и технологических мер 719-П.

Изменения в области военной и военно-технической деятельности РФ

10. Официально опубликован приказ ФСБ от 28 сентября 2021 г. № 379 [«Об утверждении Перечня сведений в области военной, военно-технической деятельности Российской Федерации, которые при их получении иностранным государством, его государственными органами, международной или иностранной организацией, иностранными гражданами или лицами без гражданства могут быть использованы против безопасности Российской Федерации»](#). Приказ содержит 60 пунктов с перечнем сведений, не являющихся государственной тайной, которые могут быть использованы иностранцами против государственной безопасности иностранными государствами и организациями, включающим в том числе:

- сведения о персональных данных военнослужащих
- сведения о функционировании центров ГосСОПКА и инцидентах на предприятиях ОПК
- сведения о закупках в части программных и программно-аппаратных средств информатизации и защиты информации для нужд предприятий ОПК
- сведения о ГИС:
 - виде, количестве и наименованиях модулей ГИС
 - местах расположения хранилищ данных и каналов связи
 - исходных текстах и дистрибутивах ПО, применяемого в работе ГИС, технической документации (**техническом задании, моделях угроз и нарушителя**) на создание ГИС и систем безопасности, в том числе о настройках средств защиты информации.

Лицензирование деятельности по работе со СКЗИ

11. ФСБ России опубликовала проект постановления Правительства РФ [«О внесении изменений в некоторые акты Правительства Российской Федерации по вопросам лицензирования отдельных видов деятельности»](#), предлагающего изменения в **Постановление Правительства № 313 от 16 апреля 2012 г., устанавливающие запрет** осуществления иностранными юридическими лицами деятельности по разработке, производству, распространению СКЗИ.

Использование электронной подписи

12. Для общественного обсуждения опубликован проект федерального закона [«О внесении изменений в Федеральный закон от 27 декабря 2019 г. № 476-ФЗ «О внесении изменений в Федеральный закон «Об электронной подписи» и статью 1 Федерального закона «О защите прав юридических лиц и индивидуальных предпринимателей при осуществлении государственного контроля \(надзора\) и муниципального контроля»](#), направленный на приведение в соответствие норм Федерального закона «Об электронной подписи», устанавливающим требования к выдаче доверенностей, нормам действующего Гражданского кодекса Российской Федерации, в том числе в части возможности передоверия другому лицу совершения действий по выданной доверенности.

13. Минцифры опубликовало проект приказа [«Об утверждении Порядка формирования и ведения реестров выданных аккредитованными удостоверяющими центрами квалифицированных сертификатов ключей проверки электронной подписи, а также предоставления информации из таких реестров»](#).

14. Минцифры опубликовало проект приказа [«Об утверждении Порядка передачи реестров выданных аккредитованными удостоверяющими центрами квалифицированных сертификатов ключей проверки электронной подписи и иной информации в федеральный орган исполнительной власти, уполномоченный в сфере использования электронной подписи, в случае прекращения деятельности аккредитованного удостоверяющего центра»](#).

15. Минцифры опубликовало проект приказа [«Об утверждении перечня индикаторов риска нарушения обязательных требований при осуществлении федерального государственного контроля \(надзора\) в сфере электронной подписи»](#).

Новости в области стандартизации

16. На сайте Федерального агентства по техническому регулированию и метрологии в [сентябрьском номере размещен](#) ГОСТ ISO/IEC 24760-2-2021 «Информационные технологии. Методы и средства обеспечения безопасности. Основы управления идентичностью. Часть 2. Базовая архитектура и требования».