

COMPLIANCE-

ДАЙДЖЕСТ



Июнь 2022

Compliance-дайджест: что изменилось в ИБ-законодательстве в июне 2022 года

В нашем ежемесячном compliance-дайджесте собраны ключевые изменения требований регуляторов по информационной безопасности за июнь 2022 года. Вы узнаете о новых штрафах, которые предлагается ввести за нарушения в области биометрических персональных данных, об информационных сообщениях ФСТЭК России, о нормативных правовых актах, принятых в развитие майского Указа Президента России, а также об отраслевых новшествах. Все новости по традиции разбиты на тематические блоки.

Биометрические персональные данные

1. Опубликован [законопроект](#), предусматривающий введение административных штрафов за нарушения, связанные с обработкой биометрических персональных данных граждан.

Согласно документу, за нарушение порядка обработки, размещения и обновления таких сведений в единой биометрической системе (ЕБС) и в других системах, обеспечивающих с их помощью идентификацию и (или) аутентификацию, а также в иных ГИС, владельцами и (или) операторами которых являются госорганы, для должностных лиц предполагаются штрафы от 100 до 300 тысяч рублей, для юридических лиц – от 300 до 500 тысяч рублей. Аналогичная ответственность предусматривается за нарушение требований к информационным технологиям и техническим средствам, предназначенным для обработки биометрических ПДн в целях проведения идентификации.

Кроме того, законопроектом предлагается ввести административную ответственность за обработку биометрических ПДн для идентификации и (или) аутентификации физических

лиц в информационных системах организаций, в государственных информационных системах, за исключением ЕБС, владельцами и (или) операторами которых являются государственные органы, без аккредитации (в том числе если аккредитация приостановлена или прекращена). Согласно документу, штрафы за такие нарушения для должностных лиц могут составить от 300 до 600 тысяч рублей, для юрлиц – от 500 тысяч до 1 000 000 рублей.

2. Опубликован [законопроект](#), предполагающий введение уголовной ответственности за внесение в ЕСИА и в ЕБС заведомо недостоверных сведений.

3. Официально опубликовано [Постановление Правительства РФ от 15.06.2022 № 1066](#), утвердившее правила, по которым россияне могут размещать свои биометрические персональные данные в ЕБС.

4. Официально опубликовано [Постановление Правительства РФ от 15.06.2022 № 1067](#), определившее случаи и сроки использования биометрических персональных данных, размещенных физическими лицами в ЕБС.

5. Официально опубликовано [Постановление Правительства РФ от 16.06.2022 № 1089](#), утвердившее положение о ЕБС.

Информационные сообщения ФСТЭК России

6. ФСТЭК России опубликовала отчеты о результатах деятельности технического комитета по стандартизации «Защита информации» (ТК 362):

- [Справка-доклад по состоянию на 31.05.2022 г.](#)
- [Справка-доклад по состоянию на 29.06.2022 г.](#)

7. ФСТЭК России опубликовала [письмо](#) с предложением отменить ГОСТ Р 58189-2018 «Защита информации. Требования к органам по аттестации объектов информатизации».

8. ФСТЭК России [сообщила](#) о внесении изменений в программы переподготовки и повышения квалификации специалистов по защите информации.

Подзаконные акты Указа Президента РФ №250

9. Опубликовано [распоряжение Правительства РФ от 22.06.2022 № 1661-р](#), утвердившее перечень ключевых органов (организаций), которым требовалось оценить уровень защищенности своих информационных систем с привлечением организаций, имеющих соответствующие лицензии ФСБ России и ФСТЭК России, до 1 июля 2022 года. Мероприятия проводятся в рамках [Указа Президента РФ от 01.05.2022 № 250](#).

10. Минцифры России [опубликовало](#) типовое техническое задание на выполнение работ по оценке уровня защищенности информационной инфраструктуры, указанной в [Указе Президента РФ от 01.05.2022 № 250](#).

Отраслевые изменения

11. Опубликован [приказ Минцифры России от 02.03.2022 № 156](#) «Об утверждении Порядка защиты сетей связи и информационных систем операторов связи от несанкционированного доступа к ним и передаваемой по ним информации при функционировании системы обеспечения вызова экстренных оперативных служб по единому номеру "112"».

12. Минздрав России разработал [Концепцию информационной безопасности в сфере здравоохранения](#). Документ направлен на повышение эффективности защиты информации, обрабатываемой медицинскими информационными системами, и на обеспечение безопасности объектов КИИ РФ в сфере здравоохранения. Также в концепции содержатся эскизные решения по реализации мер защиты информации, архитектура и эскизные решения по построению системы реагирования на компьютерные атаки в информационных системах в сфере здравоохранения. Для координации взаимодействия по обеспечению информационной безопасности планируется создать «Отраслевой Центр информационной безопасности и импортозамещения программного обеспечения Министерства здравоохранения РФ».