COMPLIANCE-

ДАЙДЖЕСТ

Июль 2022

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

В нашем ежемесячном compliance-дайджесте собраны ключевые изменения требований регуляторов по информационной безопасности за июль 2022 года. Главная тема дайджеста — новации в части защиты персональных данных, появившиеся с принятием Федерального закона № 266. Также расскажу о развитии нормативно-правовой базы в рамках Указа Президента РФ № 250, новых законопроектах, направленных на защиту критической информационной инфраструктуры, инициативе ФСТЭК России сократить сроки проведения отдельных процедур по сертификации средств защиты и других новостях из мира ИБ-комплаенса.

Персональные данные

1. Официально опубликован Федеральный закон от 14.07.2022 № 266-ФЗ, который внес большое количество поправок в нормативные правовые акты, регулирующие защиту персональных данных. Пройдусь коротко по основным новшествам документа. Впервые в законе появилось требование для госорганов, Банка России и органов местного самоуправления согласовывать с Роскомнадзором разрабатываемые нормативные правовые акты, которые регулируют:

- трансграничную передачу ПДн;
- обработку специальных категорий ПДн;
- обработку биометрических ПДн;
- обработку ПДн несовершеннолетних;
- предоставление и распространение ПДн, полученных в результате обезличивания.

Кроме того, законодатели сократили сроки рассмотрения обращений граждан, желающих узнать, какие именно сведения о них обрабатывает оператор персональных данных, с 30 до 10 рабочих дней. При этом организация может продлить время подготовки ответа в случае предоставления мотивированного уведомления о причинах задержки, но не более чем на 5 рабочих дней.

Также закон закрепил обязанность операторов предоставлять услуги даже в тех случаях, когда человек не согласен сообщить свои персональные данные, в том числе биометрические.

Отдельный блок изменений связан с трансграничной передачей персональных данных. В частности, операторов обязали отправлять уведомление в Роскомнадзор о такой деятельности еще до начала её осуществления. Сделать это можно на бумажном носителе или в форме электронного документа. При этом до подачи уведомления регулятору оператор должен собрать ряд определенных в законе сведений, запросив их у органов власти иностранного государства, иностранных физических и юридических лиц, которым планирует передавать персональные данные. Обязанность такого взаимодействия в законе появилась впервые. По результатам рассмотрения уведомления, согласно поправкам, Роскомнадзор вправе ограничить или запретить трансграничную передачу ПДн.

Еще одно новшество касается оценки вреда, который может быть причинен гражданам в случае нарушения 152-ФЗ. Ранее операторы должны были проводить её самостоятельно в качестве одной из мер по обеспечению безопасности персональных данных. Согласно закону, Роскомнадзор должен установить единые требования по оценке потенциального вреда, а также по подтверждению уничтожения ПДн.

Ряд изменений в законе направлен на борьбу с компьютерными инцидентами в области обработки персональных данных. Операторов ПДн обязали сообщать о компьютерных инцидентах, повлекших неправомерную передачу персональных данных, ФСБ России путем взаимодействия с Государственной системой обнаружения, предупреждения и ликвидации последствий компьютерных атак. Полученные данные служба будет передавать в Роскомнадзор. При этом операторы также должны будут уведомлять Роскомнадзор обо всех инцидентах напрямую:

- в течение 24 часов предоставлять сведения о причинах, повлекших нарушение прав субъектов ПДн, о предполагаемом вреде, нанесенном правам субъектов ПДн, о принятых мерах по устранению соответствующих последствий;
- в течение 72 часов о результатах внутреннего расследования выявленного инцидента, а также сведения о лицах, действия которых стали причиной выявленного инцидента.

Роскомнадзор будет вести реестр учета инцидентов в области ПДн, а также определит порядок взаимодействия с операторами ПДн в рамках его ведения.
Еще один блок изменений связан с требованиями к операторам по информированию Роскомнадзора. Так, по новым правилам, при отправке уведомления регулятору о начале

обработки персональных данных операторы будут обязаны для каждой цели обработки таких сведений указывать:

- категории ПДн;
- категории субъектов, чьи персональные данные обрабатываются;
- правовое основание обработки ПДн;
- перечень действий с ПДн;
- способы обработки ПДн.

Кроме того, в законе прописаны сроки информирования Роскомнадзора в случае изменения сведений и в случае прекращения обработки персональных данных оператором.

Федеральный закон заработает с 1 сентября 2022 года за исключением отдельных положений, вступающих в силу в иные сроки.

2. Роскомнадзор опубликовал проект приказа «Об утверждении перечня иностранных государств, обеспечивающих адекватную защиту прав субъектов персональных данных». Перечень содержит 55 государств, относящихся к Конвенции Совета Европы о защите физлиц при автоматизированной обработке персональных данных, и 34 государства, не являющихся её сторонами. Впервые в список предлагается добавить Кот-Д'Ивуар, КНР, Киргизию, Таиланд и Индию.

Биометрические персональные данные

3. Официально опубликован Федеральный закон от 14.07.2022 № 325-ФЗ «О внесении изменений в статьи 14 и 14-1 Федерального закона "Об информации, информационных технологиях и о защите информации" и статью 5 Федерального закона "О внесении изменений в отдельные законодательные акты РФ».
Закон разрешает организациям и госорганам, в чьих информационных системах персональных данных и государственных информационных системах обрабатываются биометрические ПДн, соответствующие видам сведений, размещаемых в единой биометрической системе (ЕБС), размещать такие биометрические ПДн в ЕБС без согласия субъекта ПДн. При этом государственные органы и организации должны уведомить субъект ПДн о возможности обратиться к оператору ЕБС с требованием о блокировании или об уничтожении его биометрических ПДн.

4. Опубликовано Постановление Правительства РФ от 12.07.2022 № 1237, согласно которому у россиян появилась возможность самостоятельно размещать свои биометрические данные в ЕБС с помощью специализированного программного обеспечения.

Подзаконные акты Указа Президента РФ №250

5. Официально опубликовано постановление Правительства РФ от 15.07.2022 № 1272, разработанное в рамках Указа Президента РФ от 01.05.2022 № 250. Документ утвердил типовое положение о заместителе руководителя органа (организации), ответственном за обеспечение информационной безопасности. В положении, в частности, определены квалификационные требования к ответственному лицу, трудовые (должностные) обязанности, права и ответственность.

Также постановлением утверждено типовое положение о структурном подразделении, обеспечивающем информационную безопасность органа (организации). Согласно документу, оно должно подчиняться заместителю руководителя органа (организации), ответственному за обеспечение ИБ, либо иным лицам из состава руководства при условии курирования со стороны руководителя органа (организации). Деятельность подразделения обязан контролировать руководитель органа (организации). Также в положении описаны цели и задачи структурного ИБ-подразделения, функции, права, взаимоотношения и связи, показатели эффективности и результативности.

Критическая информационная инфраструктура

6. ФСТЭК России информирует о порядке представления субъектами КИИ, осуществляющими деятельность в сферах энергетики и топливно-энергетического комплекса, сведений о результатах присвоения объектам КИИ одной из категорий значимости либо об отсутствии необходимости присвоения им одной из таких категорий.

7. В Госдуму внесен законопроект № 154496-8 «О внесении изменений в Федеральный закон «О безопасности критической информационной инфраструктуры РФ», согласно которому к субъектам КИИ предлагается относить информационные системы, информационно-телекоммуникационные сети и автоматизированные системы управления, функционирующие в сфере государственной регистрации недвижимости.б

8. В Госдуму внесен законопроект №164428-8 «О внесении изменений в Федеральный закон «О Центральном банке РФ (Банке России)», который позволит определить полномочия Банка России по контролю выполнения планов мероприятий по переходу на преимущественное применение финансовыми организациями российского ПО на значимых объектах КИИ, включая контроль выполнения финансовыми организациями закупок иностранного ПО и связанных с ними услуг.

Сертификация СЗИ

9. Для общественного обсуждения опубликован проект приказа ФСТЭК России, которым предлагается сократить сроки проведения отдельных процедур по сертификации средств защиты информации (СЗИ) в части:

- рассмотрения заявки на сертификацию СЗИ;

- разработки и утверждения программы и методик сертификационных испытаний СЗИ;
- устранения недостатков, выявленных ФСТЭК России при рассмотрении материалов по сертификации СЗИ;
- внесения изменений в сертифицированное СЗИ.

Также в проекте определены случаи, при которых разработчик СЗИ, имеющий сертификат соответствия процедур безопасной разработки программного обеспечения требованиям национальных стандартов в области защиты информации, вправе самостоятельно провести сертификационные испытания разрабатываемых им СЗИ.

Информационные сообщения ФСТЭК России

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

- Справка-доклад по состоянию на 29.06.2022 г.
- Справка-доклад по состоянию на 28.07.2022 г.

11. ФСТЭК России по результатам деятельности технического комитета по стандартизации «Защита информации» (ТК 362) опубликовала:

- проект национального стандарта ГОСТ Р «Защита информация. Идентификация и аутентификация. Уровни доверия аутентификации»;
- проект национального стандарта ГОСТ Р «Защита информации. Разработка безопасного программного обеспечения. Руководство по проведению статического анализа программного обеспечения»;
- Сведения о принятых национальных и международных стандартах за второй квартал 2022 года.

12. ФСТЭК России опубликовала результаты анализа работы технического комитета по стандартизации «Защита информации» (ТК 362) и активности организаций-членов ТК 362 во втором квартале 2022 года. В документе рассматривается состояние работ по разработке, согласованию и подготовке к утверждению ряда национальных и межгосударственных стандартов.

13. ФСТЭК России в рамках деятельности технического комитета по стандартизации «Связь» (ТК 480) представила первую редакцию проекта национального стандарта ГОСТ Р «Эксплуатация и управление сетями связи общего пользования в целях обеспечения целостности и устойчивого функционирования. Общие требования».

14. ФСТЭК России информирует о внесении изменений в программы переподготовки и повышения квалификации специалистов по защите информации.