COMPLIANCE-

ДАЙДЖЕСТ

Апрель 2023

Compliance-дайджест: что изменилось в ИБ-законодательстве в апреле

В свежем выпуске нашего дайджеста расскажу о новостях из мира ИБ-комплаенса. Что меняется в области контроля за обработкой персональных данных? Как будут обеспечивать безопасность финансовых сервисов с помощью технологии цифровых отпечатков устройств согласно новому стандарту ЦБ РФ? Какие изменения готовит Минцифры в порядке обращения с документами для служебного пользования? Об этом и многом другом читайте в апрельском дайджесте.

Персональные данные

1. Опубликован приказ Роскомнадзора от 10.01.2023 № 1, который вносит изменения в форму проверочного листа, используемого ведомством при осуществлении государственного контроля за обработкой персональных данных.

Нововведения направлены на то, чтобы привести список контрольных вопросов в соответствие измененным нормам 152-ФЗ. Правки коснулись вопросов в части выполнения требований по трансграничной передаче ПДн, уведомлению Роскомнадзора об инцидентах с ПДн, прекращению обработки ПДн, осуществлению блокирования и уничтожения ПДн.

Биометрические персональные данные

2. Опубликовано постановление Правительства Российской Федерации от 11.04.2023 № 585, утверждающее Положение о федеральном государственном контроле (надзоре) в сфере идентификации и (или) аутентификации, которое приводит порядок осуществления данного вида государственного контроля (надзора) в

соответствие с регламентирующим его Федеральным законом от 29.12.2022 № 572-ФЗ.

Минцифры России осуществляет государственный контроль с применением риск-ориентированного подхода, т. е. относит объекты контроля к категориям высокого, среднего или низкого риска.

Плановые контрольные мероприятия в виде инспекционного визита, выездной или документарной проверки проводят один раз в два года в отношении объектов контроля высокой категории риска и один раз в два с половиной года – в отношении объектов, отнесенных к категории среднего риска.

Положение установило виды профилактических мероприятий, которые могут проводиться при осуществлении государственного контроля: информирование, обобщение правоприменительной практики, объявление предостережения, консультирование и профилактический визит.

Лицензионный контроль

3. Для общественного обсуждения представлены проекты приказов ФСТЭК России, которые утверждают сроки и последовательность административных процедур при осуществлении ведомством лицензионного контроля за деятельностью:

– по технической защите конфиденциальной информации;
– по разработке и производству средств защиты конфиденциальной информации (в пределах компетенции ФСТЭК России).

К проведению выездной проверки будут привлекать экспертов, экспертные организации, не состоящие в гражданско-правовых и трудовых отношениях с лицензиатом, в отношении которого проводится проверка. Срок ее проведения не может превышать 20 рабочих дней.

Государственный контроль включает в себя следующие административные процедуры:

- организация плановой (внеплановой) проверки;
- проведение документарной проверки;
- проведение выездной проверки;
- оформление результатов проверки;
- принятие предусмотренных законодательством РФ мер при выявлении нарушений лицензионных требований к деятельности лицензиата;
- принятие мер по контролю за устранением лицензиатом выявленных нарушений лицензионных требований.

4. ФСТЭК России планирует отменить свои приказы от 20.07.2012 № 89 и № 90, которыми утверждены административные регламенты ведомства в сфере лицензионного контроля видов деятельности, отнесенных к компетенции ФСТЭК России.

Финансовый сектор

5. Банк России опубликовал стандарт обеспечения безопасности финансовых сервисов с использованием технологии цифровых отпечатков устройств. Он устанавливает рекомендации по обеспечению организациями банковской системы и иных сфер финансового рынка контроля идентификаторов доступа пользовательских устройств методом формирования и обработки цифровых отпечатков устройств при дистанционном предоставлении банковских и финансовых услуг.

Цифровой отпечаток формируется с учетом таких параметров устройств, как идентификаторы аппаратной части, версия ОС, версия установленного на устройстве браузера и других системных и аппаратных параметров устройства.

Цифровой отпечаток устройства формируется в целях:

- выполнения мероприятий по противодействию осуществлению переводов денежных средств без согласия клиента;
- выявления цепочек связанных операций по переводу денежных средств, совершенных без согласия клиента;
- выявления устройств, неоднократно задействованных при реализации компьютерных атак/инцидентов;
- использования в качестве фактора аутентификации.

Документ закрепляет рекомендации по хранению цифрового отпечатка, а также рекомендации по его применению.

Порядок обращения с документами для служебного пользования

6. Минцифры разработало проект Положения о порядке обращения с документами для служебного пользования в федеральных органах исполнительной власти, государственных корпорациях, а также подведомственных им организациях.

Проект постановления предусматривает переход от регулирования порядка обращения со служебной информацией ограниченного распространения к утверждению Положения о порядке обращения с документами для служебного пользования (далее – документы ДСП).

В положении закрепляются следующие понятия: служебная информация ограниченного доступа, документ для служебного пользования, пометка «Для служебного пользования», тиражирование документа для служебного пользования, учетная информация, руководитель, уполномоченное лицо, внутренний порядок обращения с документами для служебного пользования.

Положение также устанавливает:

- требования к порядку создания документов ДСП и составу учетной информации таких документов;
- требования к внутреннему порядку обращения с документами ДСП;
- порядок и условия снятия пометки «Для служебного пользования»;
- требования к обеспечению защиты информации при работе с документами ДСП и ответственность за нарушение положения.

Отраслевые изменения

7. Для общественного обсуждения представлен проект Указа Президента, который приравнивает предъявление гражданином документов, удостоверяющих личность, с использованием мобильного приложения портала Госуслуг к предъявлению оригиналов таких документов.

Случаи, в которых это возможно, а также перечень документов будет должно определить Правительство РФ. В проекте указа подчеркивается, что использование мобильного приложения для предъявления сведений будет осуществляться гражданами добровольно.

Предусматривается, что юридические лица до начала использования мобильного приложения для проверки или получения сведений при принятии соответствующего решения будут предоставлять в Минцифры России информацию об условиях его использования в порядке, установленном Правительством РФ.

8. Для общественного обсуждения представлен проект приказа Минэнерго России, утверждающий требования по обеспечению безопасности значимых объектов критической информационной инфраструктуры при организации и осуществлении дистанционного управления технологическими режимами работы и эксплуатационным состоянием объектов электроэнергетики из диспетчерских центров субъекта оперативно-диспетчерского управления в электроэнергетике.

Дополнительные требования предусматривают:

- обеспечение защиты трафика команд дистанционного управления между диспетчерским центром и объектами электроэнергетики, в том числе с использованием средств криптографической защиты информации;
- организацию взаимодействия технологических сетей связи, используемых для дистанционного управления, с внешними выделенными сетями связи через межсетевой экран;
- требования поддержки безопасности программного обеспечения и программно-аппаратных средств, используемых для реализации дистанционного управления;
- требования к наличию и согласованию схем организации каналов связи, используемых для дистанционного управления.

Проект приказа содержит требования, которые связаны с осуществлением предпринимательской и иной экономической деятельностью, и оценка соблюдения которых осуществляется в рамках государственного контроля (надзора) и привлечения к административной ответственности.

Автор дайджеста: Екатерина Борисенкова, консультант по информационной безопасности отдела комплаенс и аттестации центра «Solar Интеграция» компании «РТК-Солар»