Compliance-дайджест

Август 2021

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

В Compliance Дайджесте собраны ключевые изменения требований регуляторов по информационной безопасности за август 2021 года. Для вашего удобства мы разделили все новости на 7 блоков: изменения в области защиты ГИС, изменения в области защиты ПДн, изменения в области биометрических персональных данных, использование СКЗИ, взаимодействие с НКЦКИ, новости в области стандартизации, отраслевые изменения.

Изменения в области защиты ГИС

1. Официально опубликован «Порядок организации и проведения работ по аттестации объектов информатизации на соответствие требованиям о защите информации ограниченного доступа, не составляющей государственную тайну», утвержденный приказом ФСТЭК России от 29 апреля 2021 г. № 77.

Подробный обзор данного порядка опубликован в статье Андрея Семенова, заместителя руководителя отдела комплаенс и аттестации дирекции по интеграции компании «Ростелеком-Солар».

2. ФСТЭК России опубликовала проект федерального закона «О внесении изменений в статью 16 Федерального закона «Об информации, информационных технологиях и о защите информации», направленного на установление единых для государственных органов и коммерческих организаций требований по защите информации, обладателями которой являются государственные органы, вне зависимости

от места ее хранения или обработки, а также требований к организации и управлению системой защиты информации.

Проектом изменений в федеральный закон предлагается расширить область действия требований ФСБ и ФСТЭК России по защите государственных информационных систем (в том числе требований приказа ФСТЭК России от 11 февраля 2013 г. № 17) на коммерческие организации при создании и эксплуатации информационных систем, в которых обрабатывается информация, обладателями которой являются государственные органы.

Изменения в области защиты ПДн

3. Официально опубликован приказ Роскомнадзора от 21 июня 2021 г. № 106 «Об утверждении Правил использования информационной системы Федеральной службы по надзору в сфере связи, информационных технологий и массовых коммуникаций, в том числе порядка взаимодействия субъекта персональных данных с оператором».

С использованием указанной информационной системы Роскомнадзора оператором ПДн может обеспечиваться получение от субъекта ПДн согласия на обработку ПДн, разрешенных для распространения. Получение и отзыв согласия будет организован на информационном ресурсе оператора с использованием ЕСИА и путем его подписания простой электронной подписью.

Приказ вступает в силу 1 марта 2022 г.

4. Роскомнадзор представил для общественного обсуждения проект приказа «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 перечня предлагается исключить: Аргентинскую Республику, Королевство Марокко, Республику Чили, Тунисскую Республику.

И предлагается включить: Народную Республику Бангладеш, Республику Беларусь, Республику Замбию, Республику Нигер, Новую Зеландию, Республику Таджикистан, Республику Узбекистан, Республику Чад, Социалистическую Республику Вьетнам, Тоголезскую Республику, Федеративную Республику Бразилию, Федеративную Республику Нигерию.

Изменения в области биометрических персональных данных

5. Минцифры опубликовало для публичного обсуждения проект федерального закона «О внесении изменений в статью 5 Федерального закона «О внесении изменений в отдельные законодательные акты Российской Федерации», предусматривающего перенос сроков вступления в силу отдельных норм Федерального закона от 29 декабря 2020 г. № 479-ФЗ «О внесении изменений в отдельные законодательные акты Российской Федерации» (далее – Закон № 479-ФЗ), касающихся сбора, размещения, обработки биометрических персональных данных, контроля (надзора) в сфере идентификации и (или) аутентификации, на 1 сентября 2022 г., в том числе в части использования СКЗИ на стороне клиента.

6. Минцифры опубликовало доработанный проект 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», накладывающий серьезные ограничения на организации, осуществляющие идентификацию и аутентификацию граждан по биометрическим данным, а именно требования:

- по минимальному размеру собственных средств (капитала) в 500 млн руб. для организаций, осуществляющих идентификацию и аутентификацию на основе биометрических данных;
- по наличию финансового обеспечения ответственности за убытки, причиненные третьим лицам, в сумме не менее чем 100 миллионов руб.;
- по наличию лицензии ФСБ на деятельность в области криптографии и использования сертифицированных СКЗИ;
- к составу персонала, имеющего высшее образование в области информационных технологий или информационной безопасности;
- по размещению оборудования только на территории РФ;
- запрет на аккредитацию иностранных юридических лиц из стран, входящих в перечень иностранных государств, совершающих недружественные действия в отношении РФ.

7. Минцифры опубликовало проект постановления Правительства Российской Федерации «О проведении эксперимента по размещению гражданами Российской Федерации своих 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 применением мобильного телефона, смартфона, планшетного компьютера, а

также использованию указанной системы государственными органами, банками и иными организациями с применением указанных биометрических персональных данных при предоставлении отдельных услуг» в период с 1 октября 2021 г. по 1 октября 2022 г.

Участниками эксперимента являются:

- Минцифры, ФСБ, Минобрнауки, Департамент транспорта и развития дорожно-транспортной инфраструктуры города Москвы, Банк России;
- Ростелеком, Московский метрополитен, высшие учебные заведения, банки, операторы связи и иные юридические лица, согласившиеся на участие в эксперименте на добровольной основе.

Использование СКЗИ

8. Минцифры уведомляет о начале разработки нормативного правового акта, направленного на установление требований к технологиям взаимодействия средств криптографической защиты информации с иными средствами информатизации, необходимых для применения государственными органами, органами местного самоуправления, государственными и муниципальными унитарными предприятиями, государственными и муниципальными учреждениями при осуществлении взаимодействия в электронной форме с гражданами (физическими лицами) и организациями.

Планируемый срок вступления нормативного правового акта в силу – декабрь 2021 г.

Взаимодействие с НКЦКИ

9. ФСБ России опубликовала для общественного обсуждения проект приказа «О внесении изменений в Порядок информирования ФСБ России о компьютерных инцидентах, реагирования на них, принятия мер по ликвидации последствий компьютерных атак, проведенных в отношении значимых объектов критической информационной инфраструктуры Российской Федерации, утвержденный приказом ФСБ России от 19 июня 2019 г. № 282», устанавливающим, что:

- разработанный План подлежит утверждению руководством субъекта КИИ;
- копия утвержденного Плана должна быть направлена в НКЦКИ в течение 7 календарных дней;
- проект Плана должен разрабатываться при методическом обеспечении НКЦКИ (вместо «совместно с НКЦКИ»).

Новости в области стандартизации

10. Росстандарт опубликовал следующие документы, имеющие отношение к информационной безопасности:

- ГОСТ ISO/IEC 19896-1-2021. Информационные технологии. Методы и средства обеспечения безопасности. Требования к компетенции специалистов по тестированию и оценке безопасности информационных технологий. Часть 1. Введение, основные понятия и общие требования.
- ГОСТ ISO/IEC 24760-2-2021. Информационные технологии. Методы и средства обеспечения безопасности. Основы управления идентичностью. Часть 2. Базовая архитектура и требования.
- ГОСТ ISO/IEC 27014-2021. Информационные технологии. Информационная безопасность, кибербезопасность и защита конфиденциальности. Руководство деятельностью по обеспечению информационной безопасности.
- ГОСТ ISO/IEC 29100-2021. Информационные технологии. Методы и средства обеспечения безопасности. Основы защиты персональных данных.
- ГОСТ ISO/IEC TS 19249-2021. Информационные технологии. Методы и средства обеспечения безопасности. Каталог принципов построения архитектуры и проектирования безопасных продуктов, систем и приложений.
- ПНСТ 543-2021. Информационные технологии. Биометрия. Руководство по биометрической регистрации.
- ГОСТ Р 59547-2021. Защита информации. Мониторинг информационной безопасности. Общие положения.

11. Банк России официально опубликовал информацию о введении нового рекомендуемого стандарта по безопасности финансовых операций СТО БР ФАПИ.ПАОК-1.0-2021 «Безопасность финансовых (банковских) операций. Прикладные программные интерфейсы. Обеспечение безопасности финансовых сервисов при инициации OpenID Connect клиентом потока аутентификации по отдельному каналу. Требования», который совершенствует механизм сохранности данных при проведении финансовых операций. Защиту информации обеспечат установленные в документе требования к финансовым API.

Отраслевые изменения

12. Банк России опубликовал проект нового нормативного акта «Об обязательных для кредитных организаций требованиях к операционной надежности при осуществлении банковской деятельности в целях обеспечения непрерывности оказания банковских услуг», ограничивающего не более двумя часами время недоступности процессов, связанных со вкладами, переводами, открытием и ведением банковских счетов, операциями на финансовом рынке, кассовыми операциями и онлайн-сервисами дистанционного обслуживания, а также с идентификацией по биометрическим данным. Для крупных банков с активами более 500 млрд руб. время восстановления процессов, обеспечивающих размещение и обновление биометрических персональных данных в Единой биометрической системе, планируется ограничить в полчаса.

13. Министерство науки и высшего образования Российской Федерации подготовило проект ведомственного нормативного правового акта «Об определении угроз безопасности персональных данных, актуальных при обработке персональных данных в информационных системах персональных данных, эксплуатируемых в сферах деятельности, нормативно-правовое регулирование которых осуществляется Министерством науки и высшего образования Российской Федерации».

14. Минюстом России 9 августа 2021 г. под № 64574 зарегистрирован приказ Федерального казначейства от 15 июня 2021 г. № 21н «Об утверждении Порядка реализации Федеральным казначейством функций аккредитованного удостоверяющего центра и исполнения его обязанностей».