COMPLIANCE-

# ДАЙДЖЕСТ

Январь 2023

## Compliance-дайджест: что изменилось в ИБ-законодательстве в январе

В свежем выпуске дайджеста делимся новостями из мира комплаенса за прошедший январь. Как операторам персональных данных взаимодействовать с ГосСОПКА в случае инцидента? В каких случаях может быть запрещена трансграничная передача персональных данных? Что нужно для обеспечения безопасной настройки Linux согласно рекомендациям ФСТЭК России? О свежей нормативке, которая отвечает на эти и другие вопросы, читайте в посте.

## Персональные данные

1. ФСБ России представила проект приказа, в котором описан порядок взаимодействия операторов информационных систем персональных данных (далее – ИСПДн) с Государственной системой обнаружения, предупреждения и ликвидации последствий компьютерных атак (далее – ГосСОПКА).

   Согласно документу операторы ИСПДн в течение 24 часов с момента обнаружения компьютерного инцидента направляют информацию о нем в ГосСОПКА в соответствии с определенными НКЦКИ форматами или заполняют форму уведомления, которая есть на сайте Роскомнадзора.

   В течение 72 часов оператор заполняет форму уведомления о результатах внутреннего расследования, которая также размещена на сайте Роскомнадзора.

2. Опубликовано Постановление Правительства Российской Федерации от 29.12.2022 № 2526, утверждающее случаи, при которых к операторам, осуществляющим трансграничную передачу персональных данных в целях реализации полномочий и обязанностей, возложенных на государственные и муниципальные органы международным договором Российской Федерации, законодательством Российской

Федерации, не применяются требования частей 3–6, 8–11 статьи 12 Федерального закона «О персональных данных».

3. Опубликовано Постановление Правительства Российской Федерации от 10.01.2023 № 6, в котором утверждаются правила принятия решения о запрещении или об ограничении трансграничной передачи персональных данных Роскомнадзором. Решение принимается на основании поступивших представлений от федеральных органов исполнительной власти.
   **Постановление вступит в силу с 1 марта 2023 года.**

4. Опубликовано Постановление Правительства Российской Федерации от 16.01.2023 № 24, утверждающее правила, согласно которым Роскомнадзор принимает решение о запрещении трансграничной передачи персональных данных в целях защиты нравственности, здоровья, прав и законных интересов граждан.
   **Постановление вступит в силу с 1 марта 2023 года.**

## Биометрические персональные данные

5. В России будет создан Координационный совет по развитию цифровых технологий идентификации и аутентификации на основе биометрических персональных данных. Соответствующее постановление Правительства РФ размещено на официальном интернет-портале правовой информации.

   Согласно постановлению Координационный совет определяет стратегические направления развития биометрических технологий в России и развития единой биометрической системы, а также готовит предложения по внедрению в различные сферы правоотношений.

   Также Координационный совет рассматривает вопросы и разрабатывает предложения по совершенствованию биометрических технологий, по унификации требований к инфраструктуре обработки данных с применением биометрических технологий в целях предоставления государственных и муниципальных услуг, а также иных услуг, в том числе в дистанционном формате.

   В состав совета, утверждаемый правительством, войдут представители Администрации Президента РФ, Минцифры России, ФСБ России, Роскомнадзора, ПАО «Ростелеком», ПАО «Центр биометрических технологий» и Банка России.

   Все члены Координационного совета будут работать бесплатно, на общественных началах.

6. Опубликован проект постановления Правительства РФ, которое приводит Положение о федеральном государственном контроле (надзоре) в сфере идентификации и (или) аутентификации в соответствие с Федеральным законом от 29 декабря 2022 г. № 572-ФЗ «Об осуществлении идентификации и (или) аутентификации физических лиц с использованием биометрических персональных данных, о внесении изменений в отдельные законодательные акты Российской Федерации и признании утратившими силу отдельных положений законодательных актов Российской Федерации».
   В частности, согласно Федеральному закону № 572-ФЗ Минцифры России осуществляет контроль и надзор в сфере идентификации и (или) аутентификации не

только в отношении аккредитованных организаций, осуществляющих аутентификацию на основе биометрических ПДн физических лиц, и аккредитованных государственных органов, но и в отношении Банка России в случае прохождения им аккредитации.

Кроме того, Федеральный закон № 572-ФЗ запрещает идентификацию с использованием любых иных информационных систем, помимо единой биометрической системы.

Также этот закон предусматривает, что плановые контрольные (надзорные) мероприятия в отношении аккредитованных организаций и аккредитованных государственных органов проводятся не реже чем раз в три года (кроме объектов контроля, отнесенных к категории низкого риска).

7. Для общественного обсуждения представлен проект постановления Правительства Российской Федерации.
   Он предусматривает утверждение правил представления физическим лицом в многофункциональном центре предоставления государственных и муниципальных услуг (далее – МФЦ) отказа от сбора и размещения биометрических персональных данных в целях проведения идентификации и (или) аутентификации, отзыва отказа, а также письменного подтверждения МФЦ представления физическим лицом указанных отказа и отзыва отказа.

## Государственная система защиты информации в РФ

8. Для общественного обсуждения представлен проект Указа Президента Российской Федерации «Об утверждении Положения о государственной системе защиты информации в Российской Федерации».

   Проект положения определяет состав, направления деятельности государственной системы защиты информации в России, а также требования к организации защиты информации ограниченного доступа и общедоступной информации, обладателями которой являются государство, субъект РФ и муниципальное образование.

## НПА, опубликованные ФСТЭК России

9. ФСТЭК России опубликовала методический документ «Рекомендации по обеспечению безопасной настройки операционных систем Linux».
   Рекомендации предназначены для ГИС и объектов КИИ, построенных с использованием операционных систем Linux, не сертифицированных по требованиям безопасности информации, до их замены на сертифицированные отечественные операционные системы.

10. ФСТЭК России сообщила об утверждении Требований по безопасности информации к средствам виртуализации и опубликовала выписку из них.
    Документ предназначен для организаций, осуществляющих разработку средств виртуализации, заявителей на осуществление сертификации, а также для испытательных лабораторий и органов по сертификации, выполняющих работы по сертификации средств защиты информации на соответствие обязательным требованиям по безопасности информации.

Документ включает минимально необходимые требования по безопасности информации, предъявляемые к уровню доверия средства виртуализации, хостовой операционной системе, в среде которой функционирует средство виртуализации, составу функций безопасности средства виртуализации.
Чтобы дифференцировать требования по безопасности информации к средствам виртуализации, устанавливается 6 классов защиты. Самый низкий класс – шестой, самый высокий – первый.

11. ФСТЭК России опубликовала справку-доклад о ходе работ по плану ТК 362 на 2023 год по состоянию на 31.01.2023.

12. В рамках деятельности технического комитета по стандартизации «Защита информации» (ТК 362) планируется разработка следующих национальных стандартов, связанных с информационной безопасностью:
    - Информационная технология. Методология разработки доверенных систем. Конструктивная информационная безопасность. Общие положения.
    - Информационная технология. Методология разработки доверенных систем. Конструктивная информационная безопасность. Шаблоны проектирования.
    - Информационная технология. Методология разработки доверенных систем. Конструктивная информационная безопасность. Методология разработки.
    - Защита информации. Система организации и управления защитой информации. Общие положения.
    - Информационная технология. Методы и средства обеспечения безопасности. Критерии оценки безопасности информационных технологий. Часть 2. Функциональные компоненты безопасности.
    - Информационная технология. Методы и средства обеспечения безопасности. Критерии оценки безопасности информационных технологий. Часть 1. Введение и общая модель.
    - Защита информации. Формальная модель управления доступом. Рекомендации по разработке.
    - Защита информации. Идентификация и аутентификация. Типовые угрозы и уязвимости процессов идентификации и аутентификации.
    - Защита информации. Формальная модель управления доступом. Рекомендации по верификации формальных описаний модулей средства защиты, реализующих политики управления доступом.
    - Защита информации. Идентификация и аутентификация. Рекомендации по управлению идентификацией и аутентификацией.
    - Защита информации. Техника защиты информации. Номенклатура показателей качества.
    - Защита информации. Система автоматизированного управления учетными записями и правами доступа. Общие требования.
    - Защита информации. Основные термины и определения.

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