

COMPLIANCE-

ДАЙДЖЕСТ



Февраль 2023

Compliance-дайджест: что изменилось в ИБ-законодательстве в феврале 2023 года

В свежем выпуске дайджеста делимся новостями из мира ИБ-комплаенса за прошедший февраль. Какие внеплановые проверки сможет проводить Роскомнадзор в отношении операторов персональных данных? В каких случаях нарушения при обращении с биометрическими персональными данными могут привести к штрафу, а в каких – к уголовному делу? Что разрешат делать специалистам со средним профессиональным образованием при обеспечении безопасности значимых объектов КИИ? Ответы на эти и другие вопросы – в нашем дайджесте.

Персональные данные

1. Опубликован [приказ ФСБ России от 13.02.2023 № 77](#), утверждающий порядок взаимодействия операторов информационных систем персональных данных (далее – ИСПДн) с государственной системой обнаружения, предупреждения и ликвидации последствий компьютерных атак (далее – ГосСОПКА).

Субъекты КИИ и ФСТЭК России обязаны направлять данные об инцидентах в ГосСОПКУ в течение суток с момента обнаружения инцидента. Остальные операторы ИСПДн направляют данные об инциденте в течение 24 часов с момента его обнаружения через сайт Роскомнадзора, а в течение трех суток – уведомление о результатах внутреннего расследования инцидента. Роскомнадзор передает эти данные в НКЦКИ.

Документ вступил в силу 1 марта 2023 года.

2. Утверждено постановление Правительства РФ [от 04.02.2023 № 161](#). Согласно ему Роскомнадзор получил возможность при согласовании с органами прокуратуры проводить внеплановые контрольные (надзорные) мероприятия и внеплановые

проверки по фактам утечки ПДн в интернет. Изменения также касаются аккредитованных организаций в ИТ-сфере.

Биометрические персональные данные

3. В связи с принятием Федерального закона от 29.12.2022 № 572-ФЗ Правительство РФ должно внести в Госдуму проекты изменений:
 - в КОАП в части установления оборотных административных штрафов за нарушения с сфере обработки ПДн (включая нарушения, связанные с особенностями обработки биометрических ПДн);
 - в Уголовный кодекс в части введения уголовной ответственности за незаконную обработку биометрических ПДн, повлекшую общественно опасные последствия.
4. Опубликован Федеральный закон от 06.02.2023 № 8-ФЗ, который прямо определяет геномную информацию биометрическими персональными данными.

Критическая информационная инфраструктура

5. Для общественного обсуждения представлен проект приказа Минпромторга России. Он должен утвердить порядок проведения оценки актуальности и достоверности сведений, указанных в пункте 17 Правил категорирования объектов КИИ, в отношении субъектов КИИ, которые работают в области оборонной, металлургической и химической промышленности.

К проведению оценки привлекут ФГУП «НПП «Гамма», на базе которого будет создан отраслевой центр компетенций по информационной безопасности в промышленности.

Приказ предполагает, что для проверки актуальности и достоверности сведений о категорировании будут запрашивать и проводить оценку информации о результатах присвоения субъектами КИИ одной из категорий значимости либо об отсутствии необходимости присвоения им одной из таких категорий.

Также сведения о категорировании можно будет подтвердить с помощью выездной оценки по месту нахождения объекта КИИ.

6. Для общественного обсуждения представлен проект приказа ФСТЭК России, который позволяет привлекать специалистов со средним профессиональным образованием к обеспечению безопасности значимых объектов КИИ (далее – ЗОКИИ). На специалистов могут возлагаться следующие функции:
 - установка и настройка средств защиты информации ЗОКИИ;
 - информирование работников о нарушениях требований по безопасности информации и правил эксплуатации средств защиты информации;
 - ведение протоколов и журналов учета при осуществлении мониторинга средств защиты информации ЗОКИИ.

Лицензирования деятельности

7. Опубликованы приказы ФСТЭК России:
- [от 12.01.2023 № 3](#) «Об утверждении форм документов, используемых ФСТЭК России в процессе лицензирования деятельности по технической защите конфиденциальной информации, и признании утратившими силу приказа ФСТЭК России от 17 июля 2017 г. № 134 и внесенных в него изменений»;
 - [от 12.01.2023 № 4](#) «Об утверждении форм документов, используемых ФСТЭК России в процессе лицензирования деятельности по разработке и производству средств защиты конфиденциальной информации, и признании утратившими силу приказа ФСТЭК России от 17 июля 2017 г. № 133 и внесенных в него изменений».

Новости в области стандартизации

8. Минпросвещения России представило проекты приказов федеральных государственных образовательных стандартов среднего профессионального образования по специальностям [«Обеспечение информационной безопасности информационных систем»](#) и [«Обеспечение информационной безопасности автоматизированных систем»](#).

Первая образовательная программа предполагает освоение следующих видов деятельности:

- эксплуатация информационно-телекоммуникационных систем и сетей;
- защита информации в информационно-телекоммуникационных системах и сетях с использованием программных и программно-аппаратных, в том числе криптографических средств защиты;
- эксплуатация и защита безопасности объектов сетевой инфраструктуры;
- приемка, подготовка и монтаж телекоммуникационного оборудования;
- информационно-справочная поддержка и инструктирование клиентов по вопросам эксплуатации технологических составляющих инфокоммуникационных систем.

Вторая программа предполагает изучение следующих видов деятельности:

- обеспечение функционирования средств и систем обеспечения защиты средств связи сетей электросвязи от несанкционированного доступа к ним;
- обеспечение функционирования средств защиты информации в компьютерных системах и сетях;
- эксплуатация автоматизированных (информационных) систем в защищенном исполнении;
- защита информации техническими средствами;
- написание технической документации в области информационной безопасности.

Информационные сообщения регуляторов

9. ФСТЭК России сообщила об отмене госпошлины в рамках предоставления лицензии на деятельность по технической защите конфиденциальной информации и лицензии на деятельность по разработке и производству средств защиты конфиденциальной информации в 2023 году.

10. ФСБ России [признала утратившими силу следующие административные регламенты](#), которые имеют отношение к информационной безопасности:

- Административный регламент ФСБ России по предоставлению государственной услуги по лицензированию деятельности предприятий, учреждений и организаций по проведению работ, связанных с использованием сведений, составляющих государственную тайну, созданием средств защиты информации, а также с осуществлением мероприятий и (или) оказанием услуг по защите государственной тайны.
- Административный регламент ФСБ России по предоставлению государственной услуги по лицензированию деятельности по разработке и производству средств защиты конфиденциальной информации.
- Административный регламент ФСБ России по предоставлению государственной услуги по лицензированию деятельности по разработке, производству, распространению шифровальных (криптографических) средств, информационных систем и телекоммуникационных систем, защищенных с использованием шифровальных (криптографических) средств, выполнению работ, оказанию услуг в области шифрования информации, техническому обслуживанию шифровальных (криптографических) средств, информационных систем и телекоммуникационных систем, защищенных с использованием шифровальных (криптографических) средств (за исключением случая, если техническое обслуживание шифровальных (криптографических) средств, информационных систем и телекоммуникационных систем, защищенных с использованием шифровальных (криптографических) средств, осуществляется для обеспечения собственных нужд юридического лица или индивидуального предпринимателя).

Отраслевые изменения

11. Для общественного обсуждения представлен [проект постановления Правительства Российской Федерации](#) «Об утверждении Положения о федеральной государственной информационной системе «Управление государственной единой облачной платформой».

Положение определяет цели и задачи системы, ее структуру и основные функции, перечень участников, оператора (Минцифры), порядок обеспечения доступа к системе, а также требования к защите информации, в ней содержащейся.

ГосОблако — это совокупность унифицированных облачных услуг, оказываемых независимыми поставщиками. Оно предназначено для размещения и функционирования информационных систем и ресурсов госорганов.

12. Представлен [проект постановления Правительства Российской Федерации](#), согласно которому срок реализации эксперимента по повышению уровня защищенности государственных информационных систем федеральных органов исполнительной власти и подведомственных им учреждений будет продлен до 30 марта 2024 года.

13. Для общественного обсуждения представлен [проект постановления Правительства Российской Федерации](#) «Об утверждении Правил осуществления федерального государственного контроля за обеспечением защиты государственной тайны, об изменении

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