COMPLIANCE-

ДАЙДЖЕСТ

Ноябрь 2022

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

В новом выпуске нашего ежемесячного Complicane-дайджеста вас ждет подборка основных изменений законодательства в области кибербезопасности, произошедших в ноябре. Какие сведения Роскомнадзор требует указывать в Акте об уничтожении персональных данных? Как нужно выбирать средства криптографической защиты для обеспечения безопасности ГИС по новым требованиям ФСБ России? Что должны знать и уметь руководители проектов, администраторы баз данных, системные аналитики и специалисты по информационным системам согласно проектам профстандартов? Об этом и многом другом – в нашем дайджесте.

Персональные данные

1. Официально опубликован приказ Роскомнадзора от 28.10.2022 № 179 «Об утверждении Требований к подтверждению уничтожения персональных данных».

Акт об уничтожении персональных данных может быть подготовлен как в бумажной, так и в электронной форме и должен содержать:

- наименование юрлица или ФИО физлица и адрес оператора;
- наименование юрлица или ФИО физлица, адрес лица, осуществлявшего обработку ПДн по поручению оператора (если обработка была поручена);
- ФИО субъекта или иную информацию, относящуюся к физлицу, чьи ПДн были уничтожены;
- ФИО и должность лица, уничтожившего ПДн субъекта;
- перечень категорий уничтоженных ПДн субъекта;
- наименование уничтоженного материального носителя, содержавшего ПДн субъекта;
- наименование ИСПДн, из которой были уничтожены ПДн субъекта;

- способ уничтожения ПДн;
- причина уничтожения ПДн;
- дата уничтожения ПДн субъекта.

Акт об уничтожении и выгрузка из журнала регистрации событий в ИСПДн должны храниться в течение трех лет с момента уничтожения ПДн. **Приказ вступит в действие 1 марта 2023 года.**

2. Официально опубликован приказ Роскомнадзора от 27.10.2022 № 178 «Об утверждении Требований к оценке вреда, который может быть причинен субъектам персональных данных в случае нарушения Федерального закона "О персональных данных"». В приказе определены три степени вреда: высокая, средняя и низкая. Акт оценки вреда может быть составлен в электронной или бумажной форме. **Документ вступит в силу с 1 марта 2023 года.**

Государственные информационные системы

3. Официально опубликован приказ ФСБ России от 24.10.2022 № 524 «Об утверждении Требований о защите информации, содержащейся в государственных информационных системах, с использованием шифровальных (криптографических) средств». **Настоящий приказ вступает в силу с 23 ноября 2023 года.**

Основные требования приказа:

- Необходимость использования СКЗИ для защиты информации, содержащейся в ГИС, подлежит обоснованию в модели угроз безопасности информации, техническом проекте и техническом задании на создание (развитие) ГИС.
- Класс СКЗИ должен быть обоснован в модели угроз и определен для каждого сегмента ГИС.
- Модель угроз безопасности информации и (или) техническое задание на создание (развитие) ГИС должны быть согласованы с ФСБ России в части криптографической защиты информации.
- Используемые СКЗИ должны быть сертифицированы ФСБ России.
- Класс СКЗИ определяется в зависимости от уровня значимости обрабатываемой в ГИС информации и масштаба ГИС.
- Класс СКЗИ, подлежащих использованию для защиты информации в ГИС, при ее взаимодействии с другими ГИС определяется по более высокому классу СКЗИ.
- Если иными НПА предусмотрена необходимость использовать СКЗИ более высокого класса, чем класс СКЗИ, определенный в соответствии с настоящими требованиями, то класс СКЗИ определяется в соответствии с такими НПА.

Таблица определения минимально допустимого класса СКЗИ:

Уровень значимости информации	Масштаб ГИС (сегмента ГИС)		
	Вся территория РФ или 2 и более субъектов РФ	1 субъект РФ	Объекты 1 госоргана, муниципального образования и (или) организации
	Минимально допустимые классы СКЗИ		
Высокий	КВ	КС3	КС2
Средний	КС3	КС3	КС1
Низкий	КС2	КС1	КС1

С подробным разбором документа можно ознакомиться в нашей статье.

Критическая информационная инфраструктура

4. Для общественного обсуждения представлен проект приказа ФСБ России, предусматривающий утверждение порядка осуществления мониторинга защищенности информационных ресурсов, принадлежащих:

- федеральным органам исполнительной власти;
- высшим исполнительным органам государственной власти субъектов РФ;
- государственным фондам;
- государственным корпорациям (компаниям);
- стратегическим предприятиям и стратегическим акционерным обществам;
- системообразующим организациям российской экономики;
- иным организациям, созданным на основании федеральных законов;
- субъектам критической информационной инфраструктуры РФ.

Согласно проекту, мониторинг защищенности будет выполнять Центр защиты информации и специальной связи ФСБ РФ в отношении информационных ресурсов (органов) организаций, имеющих непосредственное подключение к сети «Интернет».

Предполагается, что для целей мониторинга органы (организации) должны будут направлять в Центр защиты информации и специальной связи ФСБ РФ информацию:

- о доменных именах и внешних сетевых адресах принадлежащих им информационных ресурсов однократно в срок до 1 марта 2023 года;
- об изменениях доменных имен и внешних сетевых адресов принадлежащих им информационных ресурсов, а также о приобретении доменных имен и внешних сетевых адресов новых информационных ресурсов в срок до 7 календарных дней со дня приобретения (начала использования).

Проектом предусматривается, что представители регулятора должны будут уведомлять органы (организации) о проведении оценки защищенности информационных ресурсов не позднее чем за 14 календарных дней.

Лицензирование деятельности

5. ФСБ России представила для общественного обсуждения проект приказа, которым предполагается отменить приказ регулятора от 29 декабря 2020 г. № 641. Также проект определяет сроки и последовательность административных процедур (действий), в том числе в электронной форме, при предоставлении Центром по лицензированию, сертификации и защите государственной тайны ФСБ России и территориальными органами безопасности государственной услуги по лицензированию деятельности, связанной с шифровальными (криптографическими) средствами, а также порядок взаимодействия лицензирующих органов с заявителями при предоставлении госуслуги.

Удостоверяющий центр

6. В Госдуму внесен законопроект № 244043-8 «О внесении изменений в Федеральный закон "Об информации, информационных технологиях о защите информации", направленный на создание информационной системы национального удостоверяющего центра.

Новости в области стандартизации

7. Минтруд России представил для общественного обсуждения проекты профессиональных стандартов:

- Руководитель проектов в области информационных технологий – должен знать основы информационной безопасности;
- Администратор баз данных – должен уметь выявлять инциденты информационной безопасности в базах данных и знать основы информационной безопасности;
- Системный аналитик – должен определять и описывать требования и возможные решения в области защиты информации совместно со специалистами по информационной безопасности;
- Специалист по информационным системам – должен взаимодействовать со службой информационной безопасности при обнаружении инцидентов ИБ и понимать модели угроз информационной безопасности.

8. Опубликован стандарт ПНСТ 799-2022 Информационные технологии. Криптографическая защита информации. Термины и определения. Документ начнет действовать с 1 января 2023 года.

9. ФСТЭК России опубликовала отчет о результатах деятельности технического комитета по стандартизации «Защита информации» (ТК 362) по состоянию на 29 ноября 2022 года.

Отраслевые изменения

10. К прикладному и системному ПО, включенному в единый реестр российских программ для электронных вычислительных машин и баз данных, могут ввести дополнительные требования. Соответствующий проект постановления Правительства РФ

опубликован на федеральном портале проектов нормативных правовых актов. Документ предусматривает следующие новшества:

- обновления ПО должны выполняться только после подтверждения со стороны пользователя ПО;
- ПО должно соответствовать требованиям законодательства РФ о защите информации и о защите персональных данных в случаях, установленных законодательством РФ;
- передача данных по каналам связи, в том числе текстовых сообщений и (или) электронных документов, голосовой, звуковой, визуальной и иной информации, с использованием ПО должна осуществляться с учетом требований законодательства РФ о защите информации и о связи.

11. Опубликован приказ ФСБ России от 04.11.2022 № 547 «Об утверждении Перечня сведений в области военной, военно-технической деятельности Российской Федерации, которые при их получении иностранными источниками могут быть использованы против безопасности Российской Федерации».

В части ИБ внесены следующие сведения:

- персональные данные военнослужащих (сотрудников, работников) войск, воинских формирований и органов, членов их семей;
- сведения об использовании технологий криптографической защиты информации, квантовых технологий и технологий искусственного интеллекта при разработке и производстве образцов вооружения, военной и специальной техники;
- сведения о функционировании центров ГосСОПКА;
- сведения о проведении закупок в части программных и программно-аппаратных средств информатизации и защиты информации для нужд предприятий оборонно-промышленного комплекса;
- сведения о составе и организации работы ГИС и объектов КИИ, местах расположения хранилищ данных и каналов связей, дистрибутивах ПО, применяемого в работе ГИС и на объектах КИИ, технической документации (техническом задании, моделях угроз и нарушителя), действующих паролях, настройках средств защиты информации и результатах анализа защищенности и реагирования на компьютерные инциденты.

12. В Госдуму внесен законопроект № 238005-8, предлагающий применять конфискацию имущества, полученного в результате совершения преступлений в сфере компьютерной информации.

13. Опубликовано постановление Правительства РФ от 14.11.2022 № 2051 «Об утверждении Правил обращения со сведениями о результатах проведенной оценки уязвимости объектов транспортной инфраструктуры, судов ледокольного флота, используемых для проводки по морским путям, судов, в отношении которых применяются правила торгового мореплавания и требования в области охраны судов и портовых средств, установленные международными договорами Российской Федерации, а также со сведениями, содержащимися в планах и паспортах обеспечения транспортной безопасности объектов транспортной инфраструктуры и (или) транспортных средств, которые являются информацией ограниченного доступа, и признании утратившими силу некоторых актов Правительства Российской Федерации».

14. Опубликовано постановление Правительства РФ от 03.11.2022 № 1979 «Об утверждении Правил направления в систему обеспечения соблюдения операторами связи требований при оказании услуг связи и услуг по пропуску трафика в сети связи общего пользования и получения из указанной системы сведений».

15. Опубликовано распоряжение Правительства РФ от 15.11.2022 № 3461-р, которым утверждается перечень сведений, включенных в реестр линий связи, пересекающих государственную границу РФ, и средств связи, к которым подключаются указанные линии связи, содержащий информацию, которая является общедоступной.

16. Официально опубликован приказ Минцифры России от 12.09.2022 № 659 «Об утверждении требований к линиям связи, пересекающим Государственную границу Российской Федерации, и к средствам связи, к которым подключаются указанные линии связи».

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