Compliance-дайджест

Ноябрь 2021

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

В нашем ежемесячном compliance-дайджесте собраны ключевые изменения требований регуляторов по информационной безопасности за ноябрь 2021 года. Для вашего удобства все новости разбиты на 9 блоков: персональные данные, защита информации, биометрические персональные данные, сертификация средств защиты информации, государственная тайна, оборонный комплекс, лицензирование деятельности по защите информации, стандартизация и отраслевые изменения.

Персональные данные

1. Банк России подготовил проект нового указания «О внесении изменений в Указание Банка России от 10 декабря 2015 года № 3889-У «Об определении угроз безопасности персональных данных, актуальных при обработке персональных данных в информационных системах персональных данных».

Проект указания учитывает изменения в ФЗ-152 в части появления нового типа ПДн – разрешенных субъектом ПДн для их распространения, то есть предоставления доступа неограниченному кругу лиц.

2. Официально опубликован приказ Минцифры от 29 сентября 2021 г. № 1015 «Об утверждении порядка уничтожения персональных данных, полученных в результате обезличивания, субъектом экспериментального правового режима в сфере цифровых инноваций в случае прекращения статуса субъекта экспериментального правового режима».

- Для уничтожения обезличенных данных применяются прошедшие в установленном порядке процедуру оценки соответствия СрЗИ, в составе которых реализована функция уничтожения информации.
- Факт уничтожения обезличенных данных фиксируется в акте об уничтожении. Акт составляется в четырех экземплярах.
- В акте должна содержаться информация:
  - о носителях обезличенных данных;
  - о перечне и объеме уничтоженной информации;
  - о СрЗИ, посредством которых осуществлено уничтожение.
- В течение трех рабочих дней со дня подписания акта субъект экспериментального правового режима предоставляет акт с копиями документов, подтверждающих факт уничтожения, в Роскомнадзор, ФСБ России и Минэкономразвития России.

Защита информации

3. Минцифры представило для общественного обсуждения законопроект, предусматривающий внесение изменений в Федеральный закон от 27 июля 2006 г. № 149-ФЗ «Об информации, информационных технологиях и о защите информации».

В законопроекте вводятся следующие понятия:

- Государственная единая облачная платформа (ГосОблако);
- облачные услуги;
- облачные вычисления;
- пользователи облачных услуг.

Также в законопроекте регламентируется дальнейшая разработка требований к обеспечению безопасности информации в ГосОблаке. Правительством будут определены требования к:

- инфраструктуре ГосОблака;
- центрам обработки данных, при использовании которых поставщиками облачных услуг будет обеспечиваться функционирование ГосОблака;
- услугам ГосОблака и их основным параметрам;
- поставщикам услуг ГосОблака, а также порядок и правила подключения поставщиков услуг к ГосОблаку;
- архитектуре информационных систем при переводе в ГосОблако.

Также будет определен порядок подключения информационно-телекоммуникационных инфраструктур к инфраструктуре ГосОблака.

Биометрические персональные данные

4. Официально опубликован приказ Минцифры от 1 сентября 2021 г. № 902 «Об утверждении перечня угроз безопасности, актуальных при обработке биометрических персональных данных, их проверке и передаче информации о степени их соответствия предоставленным биометрическим персональным данным физического лица в информационных системах организаций, осуществляющих идентификацию и (или)

аутентификацию с использованием биометрических персональных данных физических лиц, за исключением единой информационной системы 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, а также актуальных при взаимодействии государственных органов, органов местного самоуправления, индивидуальных предпринимателей, нотариусов и организаций, за исключением организаций финансового рынка, с указанными информационными системами, с учетом оценки возможного вреда, проведенной в соответствии с законодательством Российской Федерации о персональных данных, и учетом вида аккредитации организации из числа организаций, указанных в частях 18.28 и 18.31 статьи 14.1 Федерального закона от 27 июля 2006 года № 149-ФЗ «Об информации, информационных технологиях и о защите информации».

Приказ определяет следующие угрозы БПДн при их обработке в информационных системах, за исключением ЕБС, аккредитованными на проведение идентификации и аутентификации с использованием БПДн организациями (за исключением финансовых):

Пункт проекта	Уровень реализации угрозы	Последствия реализации угрозы	Способ реализации угрозы	Меры защиты П-378
п. 1	При автоматизированной обработке БПДн на пользовательском оборудовании (оконечном оборудовании) клиента – физического лица	• Нарушения целостности (подмены, удаления) БПДн • Нарушения конфиденциальности (компрометации) БПДн	Целенаправленные действия с использованием возможностей, указанных в пункте 10 приложения к приказу ФСБ РФ № 378	Защита устройства клиента с использованием СКЗИ класса КС1
п. 2.1	При сборе БПДн в центральном (головном) офисе, филиалах или внутренних структурных подразделениях организаций с использованием стационарных СВТ и при передаче собранных БПДн между филиалами или внутренними структурными подразделениями организаций и центральным (головным) офисом для обработки БПДн	• Нарушения целостности (подмены, удаления) БПДн • Нарушения достоверности БПДн (внесения фиктивных БПДн) • Нарушения конфиденциальности (компрометации) БПДн	Целенаправленные действия с использованием возможностей, указанных в пункте 11 (при использовании СЗИ от НСД, сертифицированных на 4 уровень доверия) или указанных в пункте 12 приложения к приказу ФСБ РФ № 378	Защита каналов связи внутри организации с использованием СКЗИ класса КС2 (в случае применения средств (систем) защиты информации от НСД) или с использованием СКЗИ класса КС3 (в противном случае)
п. 2.2		• Нарушения конфиденциальности (компрометации) БПДн	Целенаправленные действия с использованием возможностей, указанных в пункте 11	Защита каналов связи внутри организации с использованием СКЗИ класса КС2
п. 2.3		• Несанкционированный доступ к компонентам,	Использования уязвимостей (уязвимостей кода (ПО),	-

		защищаемой информации, системным, конфигурационным, иным служебным данным	уязвимостей архитектуры и конфигурации систем и сетей, а также организационных и многофакторных уязвимостей), внедрения вредоносного ПО, использования недекларированных возможностей ПО и (или) программно-аппаратных средств, ошибочных действий в ходе создания и эксплуатации систем и сетей, в том числе при установке, настройке программных и программно-аппаратных средств	
п. 2.4		• Нарушения доступности, в том числе отказ в обслуживании компонентов, нарушения функционирования (работоспособности) программно-аппаратных средств обработки, передачи и хранения информации		-
п. 3.1	При сборе БПДн работниками организаций с использованием мобильных (переносных) устройств (планшетов) и при передаче собранных БПДн между мобильными (переносными) средствами и информационной инфраструктурой структурных подразделений организаций в целях идентификации либо идентификации и аутентификации физического лица	• Нарушения целостности (подмены, удаления) БПДн • Нарушения конфиденциальности (компрометации) БПДн • Нарушения достоверности БПДн (внесения фиктивных БПДн)	Целенаправленные действия с использованием возможностей, указанных в пункте 10 (при использовании программных средств, реализующих доверенную загрузку, прошедших оценку соответствия в форме обязательной сертификации) или указанных в пункте 11 приложения к приказу ФСБ РФ № 378 (в случае неприменения средств доверенной загрузки)	Защита каналов связи внутри организации между мобильным устройством и инфраструктурой организации с использованием СКЗИ класса КС1 (в случае применения программных средств, реализующих доверенную загрузку, прошедших оценку соответствия в форме обязательной сертификации) или с использованием СКЗИ класса КС2 (в противном случае)
п. 3.2		• Несанкционированный доступ к компонентам, защищаемой информации, системным, конфигурационным, иным служебным данным	Использования уязвимостей (уязвимостей кода (ПО), уязвимостей архитектуры и конфигурации систем и сетей, а также организационных и многофакторных уязвимостей), внедрения вредоносного ПО, использования недекларированных	-
п. 3.3		• Нарушения доступности, в том числе отказ в		-

		обслуживании компонентов • Нарушения функционирования (работоспособности) программно-аппаратных средств обработки, передачи и хранения информации	возможностей ПО и (или) программно-аппаратных средств, ошибочных действий в ходе создания и эксплуатации систем и сетей, в том числе при установке, настройке программных и программно-аппаратных средств	
п. 4.1	При обработке (за исключением сбора), в том числе хранении, БПДн и информации о степени их соответствия предоставленным БПДн в ИС организаций в целях аутентификации физического лица	• Нарушения целостности (подмены, удаления) БПДн и информации о степени соответствия	Целенаправленные действия с использованием возможностей, указанных в пункте 13 приложения к приказу ФСБ РФ № 378	Защита с использованием СКЗИ класса КВ
п. 4.2		• Нарушения конфиденциальности (компрометации) БПДн	Целенаправленные действия с использованием возможностей, указанных в пункте 12 приложения к приказу ФСБ РФ № 378	Защита с использованием СКЗИ класса КС3
п. 5.1	При обработке (за исключением сбора) БПДн и информации о степени их соответствия при взаимодействии с собственными ИС организаций с использованием стационарных СВТ в целях аутентификации физического лица	• нарушения целостности (подмены, удаления) БПДн, нарушения достоверности БПДн (внесения фиктивных БПДн)	Целенаправленные действия с использованием возможностей, указанных в пункте 11 (при использовании СЗИ от НСД, сертифицированных на 4 уровень доверия) или указанных в пункте 12 приложения к приказу ФСБ РФ № 378 (в противном случае)	Защита с использованием СКЗИ класса КС2 (в случае применения средств (систем) защиты информации от НСД) или с использованием СКЗИ класса КС3 (в противном случае)
		• Нарушения конфиденциальности (компрометации) БПДн	Целенаправленные действия с использованием возможностей, указанных в пункте 11	Защита с использованием СКЗИ класса КС2
п. 5.2	При обработке (за исключением сбора) БПДн и информации о степени их соответствия при взаимодействии с собственными ИС организаций с использованием мобильных (переносных) устройств (планшетов) в целях аутентификации физического лица	• Нарушения целостности (подмены, удаления) БПДн и информации о степени соответствия • Нарушения конфиденциальности (компрометации) БПДн • Нарушения достоверности БПДн (внесения фиктивных БПДн)	Целенаправленные действия с использованием возможностей, указанных в пункте 10 (при использовании программных средств, реализующих доверенную загрузку, прошедших оценку соответствия в форме обязательной сертификации) или указанных в пункте 11 приложения к приказу ФСБ РФ № 378 (в случае неприменения средств доверенной загрузки)	Защита с использованием СКЗИ класса КС1 (в случае применения программных средств, реализующих доверенную загрузку, прошедших оценку соответствия в форме обязательной сертификации) или с использованием

				СКЗИ класса КС2 (в противном случае)
п. 6	При обработке (за исключением сбора) БПДн и информации о степени соответствия в осуществляющих обработку БПДн ИС организаций и при взаимодействии с собственными ИС в целях аутентификации физического лица	• Несанкционированный доступ к компонентам, защищаемой информации, системным, конфигурационным, иным служебным данным	Использования уязвимостей (уязвимостей кода (ПО), уязвимостей архитектуры и конфигурации систем и сетей, а также организационных и многофакторных уязвимостей), внедрения вредоносного ПО, использования недекларированных возможностей ПО и (или) программно-аппаратных средств, ошибочных действий в ходе создания и эксплуатации систем и сетей, в том числе при установке, настройке программных и программно-аппаратных средств	-
п. 7		• Нарушения доступности, в том числе отказ в обслуживании компонентов • Нарушения функционирования (работоспособности) программно-аппаратных средств обработки, передачи и хранения информации		-
п. 8	При хранении БПДн и информации о степени соответствия в осуществляющих обработку БПДн ИС организаций в целях идентификации либо идентификации и аутентификации физического лица	• Нарушения целостности (подмены, удаления) БПДн и информации о степени соответствия • Нарушения конфиденциальности (компрометации) БПДн при обработке (за исключением сбора)	Целенаправленные действия с использованием возможностей, указанных в пункте 13 приложения к приказу ФСБ РФ № 378	Защита с использованием СКЗИ класса КВ
п. 9.1	При обработке (за исключением сбора) БПДн и информации о степени их соответствия при взаимодействии с собственными ИС организаций с использованием стационарных СВТ в целях идентификации либо идентификации и аутентификации физического лица	• Нарушения целостности (подмены, удаления) БПДн, нарушения достоверности БПДн (внесения фиктивных БПДн)	Целенаправленные действия с использованием возможностей, указанных в пункте 11 (при использовании СЗИ от НСД, сертифицированных на 4 уровень доверия) или указанных в пункте 12 приложения к приказу ФСБ РФ № 378 (в противном случае)	Защита с использованием СКЗИ класса КС2 (в случае применения средств (систем) защиты информации от НСД) или с использованием СКЗИ класса КС3 (в противном случае)
		• Нарушения конфиденциальности (компрометации) БПДн	Целенаправленные действия с использованием возможностей, указанных в пункте 11	Защита с использованием СКЗИ класса КС2
п. 9.2	При обработке (за исключением сбора) БПДн и информации	• Нарушения целостности (подмены, удаления) БПДн и	Целенаправленные действия с использованием	Защита с использованием СКЗИ класса КС1

	о степени их соответствия при взаимодействии с собственными ИС организаций с использованием мобильных (переносных) устройств (планшетов) в целях идентификации либо идентификации и аутентификации физического лица	информации о степени соответствия • Нарушения конфиденциальности (компрометации) БПДн, нарушения достоверности БПДн (внесения фиктивных БПДн)	возможностей, указанных в пункте 10 (при использовании программных средств, реализующих доверенную загрузку, прошедших оценку соответствия в форме обязательной сертификации) или указанных в пункте 11 приложения к приказу ФСБ РФ № 378 (в случае неприменения средств доверенной загрузки)	(в случае применения программных средств, реализующих доверенную загрузку, прошедших оценку соответствия в форме обязательной сертификации) или с использованием СКЗИ класса КС2 (в противном случае)
п. 10	При обработке (за исключением сбора) БПДн и информации о степени соответствия в осуществляющих обработку БПДн информационных системах организаций и при взаимодействии с собственными информационными системами в целях идентификации либо идентификации и аутентификации физического лица	• Несанкционированный доступ к компонентам, защищаемой информации, системным, конфигурационным, иным служебным данным	Использования уязвимостей (уязвимостей кода (ПО), уязвимостей архитектуры и конфигурации систем и сетей, а также организационных и многофакторных уязвимостей), внедрения вредоносного ПО, использования недекларированных возможностей ПО и (или) программно-аппаратных средств, ошибочных действий в ходе создания и эксплуатации систем и сетей, в том числе при установке, настройке программных и программно-аппаратных средств	-
п. 11		• Нарушения доступности, в том числе отказ в обслуживании компонентов, нарушения функционирования (работоспособности) программно-аппаратных средств обработки, передачи и хранения информации		-
п. 12	При взаимодействии государственных органов, органов местного самоуправления, индивидуальных предпринимателей, нотариусов и организаций с ИС организаций, осуществляющих идентификацию и (или) аутентификацию с использованием БПДн, в целях аутентификации физического лица	• Нарушения целостности (подмены, удаления) информации о степени соответствия, нарушения конфиденциальности (компрометации) информации о степени соответствия	Целенаправленные действия с использованием возможностей, указанных в пункте 12	Защита с использованием СКЗИ класса КС3

п. 13.1	При взаимодействии государственных органов, органов местного самоуправления, индивидуальных предпринимателей, нотариусов и организаций с ИС организаций, осуществляющих идентификацию и (или) аутентификацию с использованием БПДн, в целях идентификации либо идентификации и аутентификации физического лица	• Нарушения целостности (подмены, удаления) БПДн и информации о степени соответствия	Целенаправленные действия с использованием возможностей, указанных в пункте 13 приложения к приказу ФСБ РФ № 378	Защита с использованием СКЗИ класса КВ
п. 13.2		• Нарушения конфиденциальности (компрометации) БПДн	Целенаправленные действия с использованием возможностей, указанных в пункте 12	Защита с использованием СКЗИ класса КС3

5. Минцифры подготовило и представило для общественного обсуждения проект ведомственного приказа «Об утверждении перечня индикаторов риска нарушения обязательных требований по федеральному государственному контролю (надзору) в сфере идентификации и (или) аутентификации».

Устанавливаются следующие индикаторы риска нарушения обязательных требований для аккредитованной организации, осуществляющей идентификацию и (или) аутентификацию с использованием БПДн физических лиц:

- неисполнение предписания об устранении выявленного нарушения обязательных требований;
- наличие задолженности по уплате налогов;
- возбуждение производства по делу о банкротстве;
- возбуждение дела об административном правонарушении в области предпринимательской деятельности, персональных данных, защиты информации или возбуждение уголовного дела в связи с совершением преступления;
- поступление в течение 12 месяцев двух и более сообщений от различных лиц о нарушении конфиденциальности, неправомерного доступа, распространения, предоставления в сеть «интернет» БПДн физических лиц.

6. Минцифры представило для общественного обсуждения проект приказа «Об утверждении типового порядка действий уполномоченного работника многофункционального центра предоставления государственных и муниципальных услуг при размещении или обновлении в единой системе идентификации и аутентификации сведений, необходимых для регистрации физических лиц в данной системе, размещении

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 использованием программно-технических комплексов».

Проект разработан в соответствии с требованиями постановления Правительства РФ от 15 октября 2021 г. № 1753.

Для сбора БПДн в ЕБС предлагается использовать уже существующие криптобиокабины, развернутые в МФЦ в рамках оказания услуг по выдаче биометрических загранпаспортов.

В МФЦ должно быть предусмотрено рабочее место уполномоченного работника МФЦ в непосредственной близости к криптобиокабине с целью контроля данным работником действий заявителя в процессе сбора БПДн, необходимых для размещения в ЕБС. При этом не допускается самостоятельное размещение или обновление уполномоченным работником МФЦ принадлежащих ему сведений в ЕСИА и БПД в ЕБС.

Уполномоченный работник МФЦ при предоставлении услуги по размещению сведений осуществляет следующий порядок действий:

- устанавливает личность заявителя;
- проводит процедуры по регистрации или обновлению сведений в ЕСИА при отсутствии у заявителя подтвержденной учетной записи в ЕСИА;
- получает согласие заявителя на обработку ПДн и БПДн;
- формирует и распечатывает заявление, которое подписывается заявителем;
- распечатывает и выдает заявителю штриховой код доступа заявителя к криптобиокабине;
- контролирует факт прохождения заявителя в криптобиокабину, а также контролирует процесс сбора БПДн в криптобиокабине;
- после размещения сведений заявителя подписывает электронное заявление своей квалифицированной электронной подписью.

Сертификация средств защиты информации

7. ФСТЭК России опубликовал информационное сообщение ФСТЭК России от 10 ноября 2021 г. № 240/24/5444 «О внесении изменений в Положение о системе сертификации средств защиты информации, утвержденное приказом Федеральной службы по техническому и экспортному контролю от 3 апреля 2018 г. № 55».

Регулятор приводит консолидированный список внесенных изменений:

- Установлен запрет на сертификацию средств защиты информации иностранного производства, в отношении которых нормативными правовыми актами Российской Федерации установлены ограничения или запреты на их использование в Российской Федерации.
- Отменен срок действия сертификата соответствия для единичного образца или партии средства защиты информации. Определены условия, при которых

серийно производимые средства защиты считаются сертифицированными, в том числе после окончания срока действия сертификата соответствия.
- Уточнен порядок отбора образцов (образца) средства защиты информации для сертификационных испытаний.
- Упразднена процедура предварительного рассмотрения образца средства защиты информации и документации на него.
- Изменен порядок маркирования сертифицированных средств защиты информации.
- Сокращен объем испытаний сертифицированных средств защиты информации при продлении срока действия сертификата соответствия.

Государственная тайна

8. Официально опубликовано постановление Правительства Российской Федерации от 30 октября 2021 г. № 1868 «О внесении изменений в Правила отнесения сведений, составляющих государственную тайну, к различным степеням секретности». Документ вступает в силу с 1 января 2022 г.

Оборонный комплекс

9. Для общественного обсуждения представлен проект приказа министра обороны Российской Федерации «Об утверждении Перечня сведений Вооруженных Сил Российской Федерации, подлежащих отнесению к служебной тайне в области обороны».

Перечень включает 813 пунктов сведений. Вот некоторые из них:

- Сведения, раскрывающие организацию или состояние защиты информации на объектах информатизации, предназначенных для обработки служебной информации ограниченного распространения.
- Сведения, раскрывающие требования по защите информации, предъявляемые к создаваемым (модернизируемым) объектам информатизации, средствам защиты информации, предназначенным для обработки служебной информации ограниченного распространения.
- Сведения, раскрывающие перечни защищаемых ресурсов или параметры разграничения доступа к защищаемым ресурсам на объектах информатизации, а также состояние защищенности автоматизированных (информационных) систем, предназначенных для обработки служебной информации ограниченного распространения.
- Сведения, раскрывающие меры по защите информационной инфраструктуры Вооруженных Сил, меры по обеспечению защиты информации при организации сетевого взаимодействия автоматизированных (информационных) систем военного назначения, в том числе схемы информационно-технического взаимодействия.
- Сведения, раскрывающие порядок устранения уязвимостей информационной безопасности и выпуска обновлений безопасности программного обеспечения автоматизированных (информационных) систем военного назначения.

- Сведения, раскрывающие результаты анализа угроз информационной безопасности в сети «интернет».
- Сведения, раскрывающие вопросы организации, обеспечения функционирования средств защиты информации от несанкционированного доступа на объектах информатизации, обрабатывающих информацию ограниченного распространения.
- Сведения, раскрывающие применение общего программного обеспечения, порядок настройки средств защиты информации и средств антивирусной защиты объектов информатизации и другие.

10. Официально опубликовано постановление Правительства Российской Федерации от 26 ноября 2021 г. № 2052 «Об утверждении Правил обращения со сведениями, составляющими служебную тайну в области обороны».

В постановлении описан порядок обращения с документами, содержащими сведения, составляющие служебную тайну в области обороны, в том числе:

- проставление и снятие пометки «Для служебного пользования»;
- прием и учет (регистрация) документов;
- уничтожение документов;
- передача информации на машинном носителе;
- действия при утрате документов.

Правила не распространяются на обращение с документами, содержащими сведения, составляющие государственную тайну.

В ФСБ России и Росгвардии, а также в подведомственных им организациях при обращении с документами и машинными носителями информации, содержащими сведения, составляющие служебную тайну в области обороны, должны руководствоваться Положением о порядке обращения со служебной информацией ограниченного распространения в федеральных органах исполнительной власти, уполномоченном органе управления использованием атомной энергии и уполномоченном органе по космической деятельности, утвержденным постановлением Правительства Российской Федерации от 3 ноября 1994 г. № 1233.

Лицензирование деятельности по защите информации

11. Официально опубликовано Постановление Правительства Российской Федерации от 26 ноября 2021 г. № 2054 «О внесении изменений в Положение о лицензировании деятельности по разработке и производству средств защиты конфиденциальной информации».

12. Официально опубликовано Постановление Правительства Российской Федерации от 26 ноября 2021 г. № 2055 «О внесении изменений в Положение о лицензировании деятельности по технической защите конфиденциальной информации».

Постановления Правительства вступят в силу с 1 марта 2022 года. Изменения в первую очередь связаны с переходом на реестровую модель.

Местом осуществления лицензируемого вида деятельности не могут являться помещения, здания, сооружения жилого назначения. Некоторые эксперты оценивают данное требование как возможное ограничение на осуществление лицензированного вида деятельности при удаленном режиме работы.

По сравнению с проектами документов в итоговых версиях убрали возможность выездной оценки соответствия соискателя лицензии (лицензиата) лицензионным требованиям с использованием средств дистанционного взаимодействия.

Стандартизация

13. Официально опубликован приказ Министерства труда и социальной защиты Российской Федерации от 12 октября 2021 г. № 723н «Об утверждении профессионального стандарта «Специалист по проектированию автоматизированных систем управления технологическими процессами».

14. На сайте Федерального агентства по техническому регулированию и метрологии в ноябрьском номере размещены:

- 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 Р 59381-2021 «Информационные технологии. Методы и средства обеспечения безопасности. Основы управления идентичностью. Часть 1. Терминология и концепции».
- ГОСТ ISO/IEC 24760-2-2021 «Информационные технологии. Методы и средства обеспечения безопасности. Основы управления идентичностью. Часть 2. Базовая архитектура и требования».
- ГОСТ Р 59382-2021 «Информационные технологии. Методы и средства обеспечения безопасности. Основы управления идентичностью. Часть 3. Практические приемы».
- ГОСТ Р 59383-2021 «Информационные технологии. Методы и средства обеспечения безопасности. Основы управления доступом».
- 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 Р 59407-2021 «Информационные технологии. Методы и средства обеспечения безопасности. Базовая архитектура 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».
- ГОСТ Р 59494-2021 «Информационные технологии. Методы и средства обеспечения безопасности. Безопасность приложений. Часть 5-1. Структуры данных протоколов и мер обеспечения безопасности приложений. XML-схемы».
- ГОСТ Р 59503-2021 «Информационные технологии. Методы и средства обеспечения безопасности. Менеджмент информационной безопасности. Экономика информационной безопасности организации».
- ГОСТ Р 59506-2021 «Безопасность машин. Вопросы защиты информации в системах управления, связанных с обеспечением функциональной безопасности».
- ГОСТ Р 59515-2021 «Информационные технологии. Методы и средства обеспечения безопасности. Подтверждение идентичности».
- ГОСТ Р 59516-2021 «Информационные технологии. Менеджмент информационной безопасности. Правила страхования рисков информационной безопасности».
- ГОСТ Р ИСО/МЭК 27000-2021 «Информационные технологии. Методы и средства обеспечения безопасности. Системы менеджмента информационной безопасности. Общий обзор и терминология».
- ГОСТ Р ИСО/МЭК 27002-2021 «Информационные технологии. Методы и средства обеспечения безопасности. Свод норм и правил применения мер обеспечения информационной безопасности».
- ГОСТ Р ИСО/МЭК 27003-2021 «Информационные технологии. Методы и средства обеспечения безопасности. Системы менеджмента информационной безопасности. Руководство по реализации».
- ГОСТ Р ИСО/МЭК 27004-2021 «Информационные технологии. Методы и средства обеспечения безопасности. Менеджмент информационной безопасности. Мониторинг, оценка защищенности, анализ и оценивание».
- ГОСТ Р ИСО/МЭК 27017-2021 «Информационные технологии. Методы и средства обеспечения безопасности. Правила применения мер обеспечения информационной безопасности на основе ИСО/МЭК 27002 при использовании облачных служб».
- ГОСТ Р ИСО/МЭК 27019-2021 «Информационные технологии. Методы и средства обеспечения безопасности. Меры обеспечения информационной безопасности в энергетике (неатомной)».
- ГОСТ Р ИСО/МЭК 27021-2021 «Информационные технологии. Методы и средства обеспечения безопасности. Требования к компетентности специалистов по системам менеджмента информационной безопасности».
- ГОСТ Р ИСО/МЭК 27033-2-2021 «Информационные технологии. Методы и средства обеспечения безопасности. Безопасность сетей. Часть 2. Рекомендации по проектированию и реализации безопасности сетей».
- ГОСТ Р ИСО/МЭК 27034-2-2021 «Информационные технологии. Методы и средства обеспечения безопасности. Безопасность приложений. Часть 2. Нормативная структура организации».

- ГОСТ Р ИСО/МЭК 27034-3-2021 «Информационные технологии. Методы и средства обеспечения безопасности. Безопасность приложений. Часть 3. Процесс менеджмента безопасности приложений».
- ГОСТ Р ИСО/МЭК 27034-6-2021 «Информационные технологии. Методы и средства обеспечения безопасности. Безопасность приложений. Часть 6. Практические примеры».
- ГОСТ Р ИСО/МЭК 27036-1-2021 «Информационные технологии. Методы и средства обеспечения безопасности. Информационная безопасность во взаимоотношениях с поставщиками. Часть 1. Обзор и основные понятия».
- ГОСТ Р 59329-2021 «Системная инженерия. Защита информации в процессах приобретения и поставки продукции и услуг для системы».
- ГОСТ Р 59330-2021 «Системная инженерия. Защита информации в процессе управления моделью жизненного цикла системы».
- ГОСТ Р 59331-2021 «Системная инженерия. Защита информации в процессе управления инфраструктурой системы».
- ГОСТ Р 59332-2021 «Системная инженерия. Защита информации в процессе управления портфелем проектов».
- ГОСТ Р 59333-2021 «Системная инженерия. Защита информации в процессе управления человеческими ресурсами системы».
- ГОСТ Р 59334-2021 «Системная инженерия. Защита информации в процессе управления качеством системы».
- ГОСТ Р 59335-2021 «Системная инженерия. Защита информации в процессе управления знаниями о системе».
- ГОСТ Р 59336-2021 «Системная инженерия. Защита информации в процессе планирования проекта».
- ГОСТ Р 59337-2021 «Системная инженерия. Защита информации в процессе оценки и контроля проекта».
- ГОСТ Р 59338-2021 «Системная инженерия. Защита информации в процессе управления решениями».
- ГОСТ Р 59339-2021 «Системная инженерия. Защита информации в процессе управления рисками для системы».
- ГОСТ Р 59340-2021 «Системная инженерия. Защита информации в процессе управления конфигурацией системы».
- ГОСТ Р 59342-2021 «Системная инженерия. Защита информации в процессе измерений системы».
- ГОСТ Р 59344-2021 «Системная инженерия. Защита информации в процессе анализа бизнеса или назначения системы».
- ГОСТ Р 59345-2021 «Системная инженерия. Защита информации в процессе определения потребностей и требований заинтересованной стороны для системы».
- ГОСТ Р 59347-2021 «Системная инженерия. Защита информации в процессе определения архитектуры системы».
- ГОСТ Р 59348-2021 «Системная инженерия. Защита информации в процессе определения проекта».

- ГОСТ Р 59350-2021 «Системная инженерия. Защита информации в процессе реализации системы».
- ГОСТ Р 59351-2021 «Системная инженерия. Защита информации в процессе комплексирования системы».
- ГОСТ Р 59353-2021 «Системная инженерия. Защита информации в процессе передачи системы».
- ГОСТ Р 59354-2021 «Системная инженерия. Защита информации в процессе аттестации системы».
- ГОСТ Р 59355-2021 «Системная инженерия. Защита информации в процессе функционирования системы».
- ГОСТ Р 59357-2021 «Системная инженерия. Защита информации в процессе изъятия и списания системы».

Отраслевые изменения

15. Минцифры представило для общественного обсуждения проект ведомственного приказа «Об определении порядка защиты сетей связи и информационных систем операторов связи от несанкционированного доступа к ним и передаваемой по ним информации при функционировании системы обеспечения экстренных оперативных служб по единому номеру «112».

16. Минцифры представило для общественного обсуждения проект постановления Правительства Российской Федерации «Об утверждении Правил предоставления субсидий из федерального бюджета российскому юридическому лицу на разработку и реализацию на регулярной основе программы кибергигиены и повышения грамотности широких слоев населения по вопросам информационной безопасности».