

The background of the slide is a blurred image of a businessman in a suit and tie, holding several large, metallic, interlocking gears. The scene is set in what appears to be a modern office or laboratory environment with soft lighting.

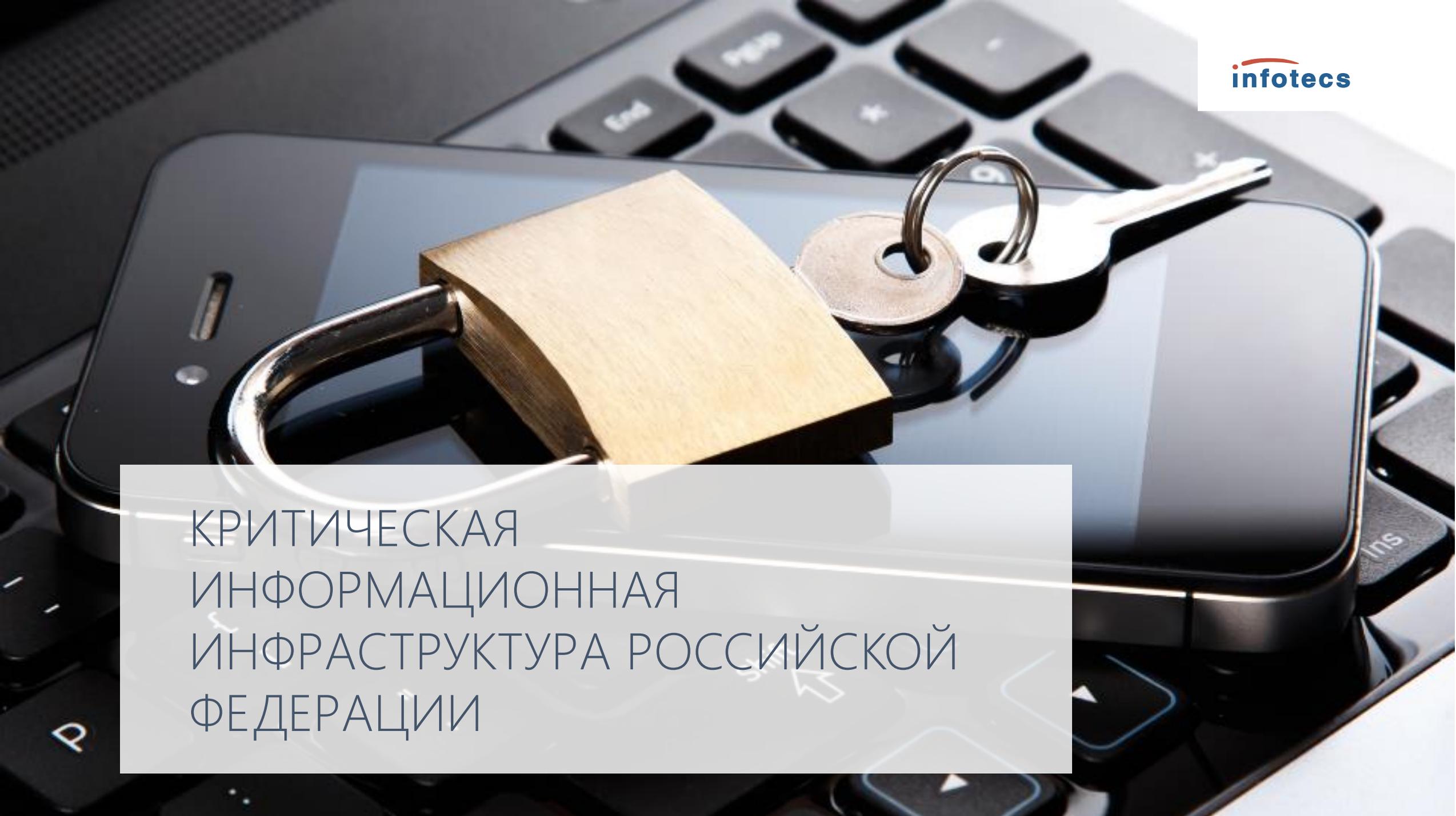
ОСНОВНЫЕ НОВОВВЕДЕНИЯ В ЗАКОНОДАТЕЛЬСТВЕ РФ В ОБЛАСТИ ИБ

Александр Шипков, CISSP

Области рассмотрения изменений

- Критическая информационная инфраструктура Российской Федерации
- Государственные информационные системы
- Персональные данные
- Сертификация средств защиты информации

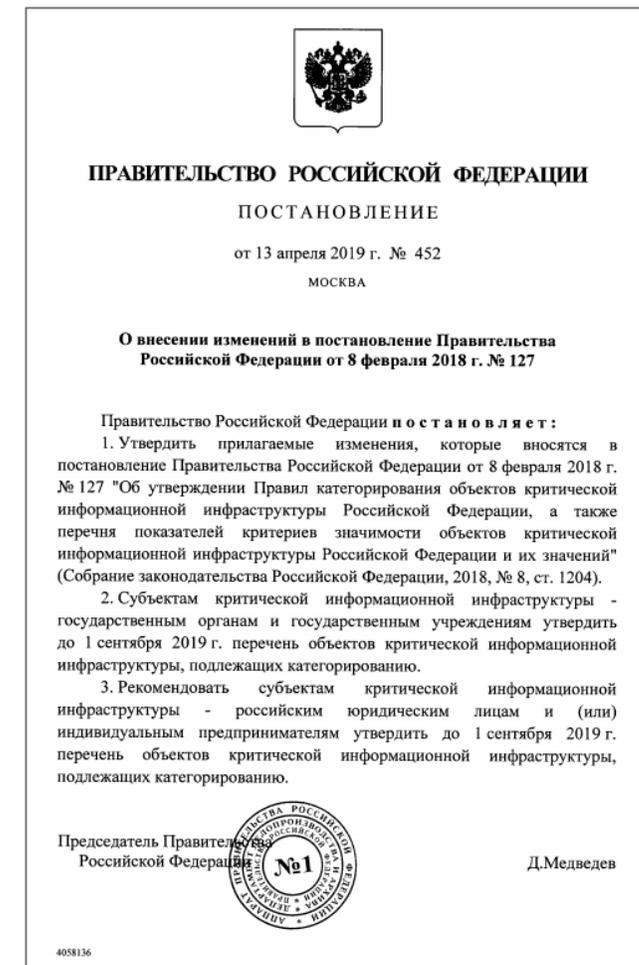


The background of the slide is a close-up photograph of a black smartphone lying on a black laptop keyboard. A large, square brass padlock is attached to the top edge of the phone. A set of keys, including a silver key and a circular metal token, is attached to the padlock's shackle. The scene is lit from the side, creating strong highlights and shadows.

КРИТИЧЕСКАЯ
ИНФОРМАЦИОННАЯ
ИНФРАСТРУКТУРА РОССИЙСКОЙ
ФЕДЕРАЦИИ

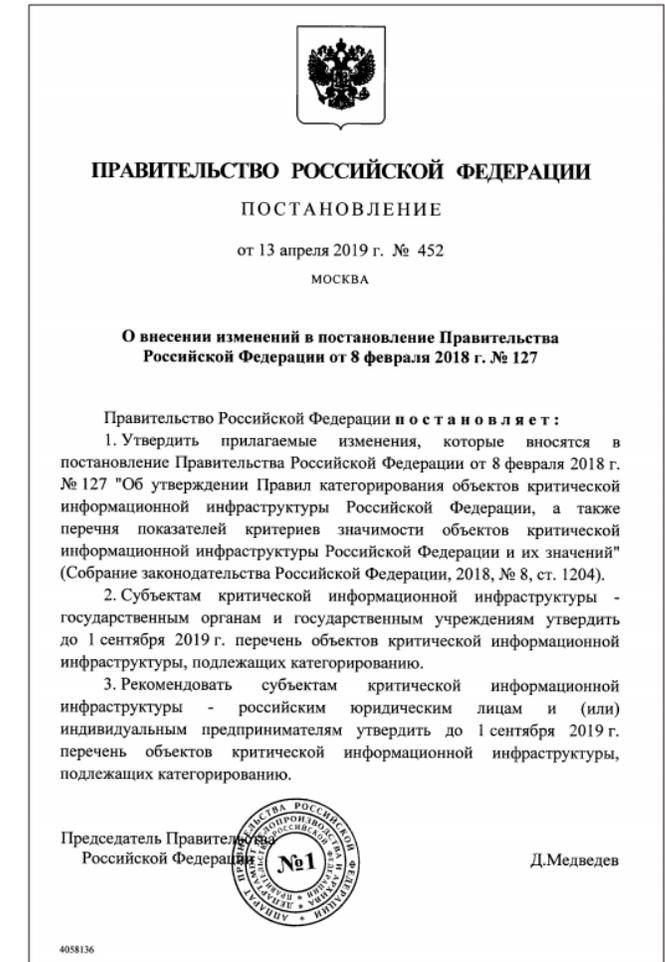
Постановление Правительства №452

- перечень эксплуатируемых объектов подлежит утверждению субъектом критической информационной инфраструктуры до **1 сентября 2019 г.**
- максимальный срок категорирования **не должен превышать одного года** со дня утверждения субъектом критической информационной инфраструктуры перечня объектов (внесения изменений)



Постановление Правительства №452

- перечень объектов в течение 10 рабочих дней после утверждения направляется в печатном и электронном виде во ФСТЭК России
- не реже чем один раз в 5 лет или в случае изменения показателей критериев значимости объектов КИИ – пересмотр установленных категории значимости (в случае изменения категории значимости сведения необходимо отправить во ФСТЭК России)



Проект изменений в Приказ ФСТЭК России №235

С 1 января 2021 года устанавливаются дополнительные требования к стажу и образованию **руководителей и штатных работников** структурных подразделений по безопасности: для руководителей структурных подразделений по безопасности:

- высшее профессиональное образование в области ИБ (или иное высшее профессиональное образование)
- профессиональная переподготовка по ИБ сроком обучения не менее 360 часов
- стаж работы в сфере ИБ не менее трех лет

Для штатных работников структурных подразделений по безопасности:

- высшее профессиональное образование в области ИБ (или иное высшее профессиональное образование)
- профессиональная переподготовка по ИБ сроком обучения не менее 72 часов



ФЕДЕРАЛЬНАЯ СЛУЖБА
ПО ТЕХНИЧЕСКОМУ И ЭКСПОРТНОМУ КОНТРОЛЮ
(ФСТЭК России)

П Р И К А З

« ___ » марта 2019 г. Москва № ___

О внесении изменений в Требования к созданию систем безопасности значимых объектов критической информационной инфраструктуры Российской Федерации и обеспечению их функционирования, утвержденные приказом Федеральной службы по техническому и экспортному контролю от 21 декабря 2017 г. № 235

В соответствии с пунктом 4 части 3 статьи 6 Федерального закона от 26 июля 2017 г. № 187-ФЗ «О безопасности критической информационной инфраструктуры Российской Федерации» (Собрание законодательства Российской Федерации, 2017, № 31, ст. 4736) **П Р И К А З Ы В А Ю**:

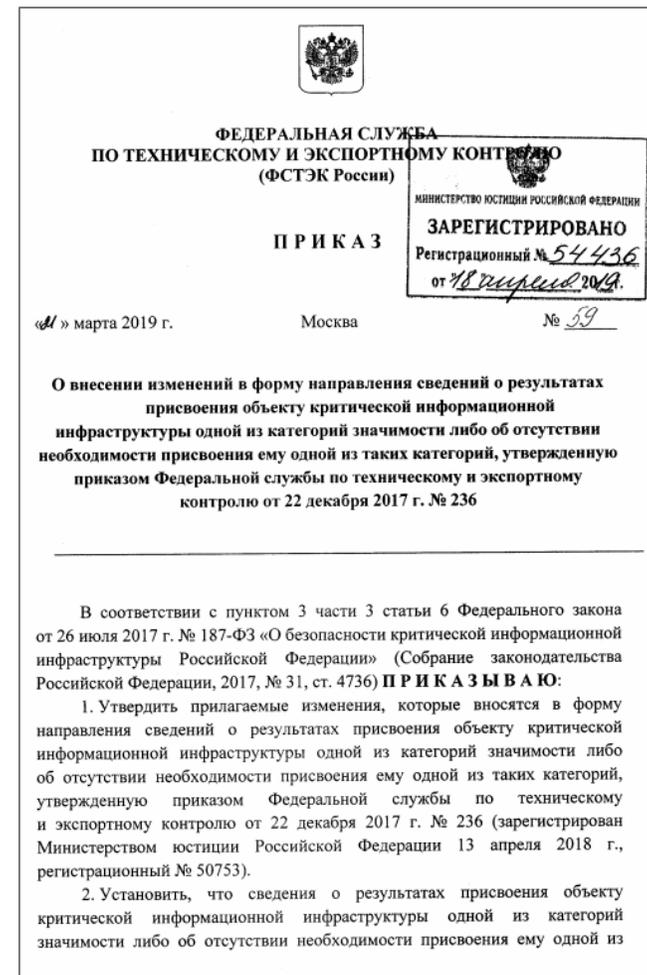
1. Внести в Требования к созданию систем безопасности значимых объектов критической информационной инфраструктуры Российской Федерации и обеспечению их функционирования, утвержденные приказом Федеральной службы по техническому и экспортному контролю от 21 декабря 2017 г. № 235 (зарегистрирован Министерством юстиции Российской Федерации 22 февраля 2018 г., регистрационный № 50118), следующие изменения:

1) предложение первое абзаца второго пункта 3 изложить в следующей редакции:

«Системы безопасности создаются в отношении всех значимых объектов критической информационной инфраструктуры субъекта критической информационной инфраструктуры с учетом значимых объектов

Приказ ФСТЭК России №59

- сведения о критических процессах заменены на сведения о типе объекта (информационная система, автоматизированная система управления, информационно-телекоммуникационная сеть)
- добавлены сведения о ИНН субъекта и КПП его обособленных подразделений (филиалов, представительств), в которых размещаются сегменты распределенного объекта КИИ
- удалены сведения об ущербе, который может быть причинен в результате возникновения компьютерных инцидентов, в соответствии с показателями критериев значимости
- добавлены сведения об обосновании полученных значений по каждому из показателей критериев значимости или обоснование неприменимости показателя к объекту



ФЕДЕРАЛЬНАЯ СЛУЖБА
ПО ТЕХНИЧЕСКОМУ И ЭКСПОРТНОМУ КОНТРОЛЮ
(ФСТЭК России)

МИНИСТЕРСТВО ЮСТИЦИИ РОССИЙСКОЙ ФЕДЕРАЦИИ
ЗАРЕГИСТРИРОВАНО
Регистрационный № 54436
от 28.03.2019.

П Р И К А З

«11» марта 2019 г. Москва № 59

О внесении изменений в форму направления сведений о результатах присвоения объекту критической информационной инфраструктуры одной из категорий значимости либо об отсутствии необходимости присвоения ему одной из таких категорий, утвержденную приказом Федеральной службы по техническому и экспортному контролю от 22 декабря 2017 г. № 236

В соответствии с пунктом 3 части 3 статьи 6 Федерального закона от 26 июля 2017 г. № 187-ФЗ «О безопасности критической информационной инфраструктуры Российской Федерации» (Собрание законодательства Российской Федерации, 2017, № 31, ст. 4736) П Р И К А З Ы В А Ю:

1. Утвердить прилагаемые изменения, которые вносятся в форму направления сведений о результатах присвоения объекту критической информационной инфраструктуры одной из категорий значимости либо об отсутствии необходимости присвоения ему одной из таких категорий, утвержденную приказом Федеральной службы по техническому и экспортному контролю от 22 декабря 2017 г. № 236 (зарегистрирован Министерством юстиции Российской Федерации 13 апреля 2018 г., регистрационный № 50753).

2. Установить, что сведения о результатах присвоения объекту критической информационной инфраструктуры одной из категорий значимости либо об отсутствии необходимости присвоения ему одной из

Приказ ФСТЭК России №60



- при проектировании вновь создаваемых или модернизируемых ЗОКИИ 1 категории значимости в качестве граничных маршрутизаторов, имеющих доступ к информационно-телекоммуникационной сети «Интернет», выбираются маршрутизаторы, сертифицированные на соответствие требованиям по безопасности информации (в части реализованных в них функций безопасности) **(вступает в силу с 1 января 2020 года)**
- входящие в состав значимого объекта 1 категории значимости программные и программно-аппаратные средства, осуществляющие хранение и обработку информации, должны размещаться **на территории Российской Федерации**

ФЕДЕРАЛЬНАЯ СЛУЖБА
ПО ТЕХНИЧЕСКОМУ И ЭКСПОРТНОМУ КОНТРОЛЮ
(ФСТЭК России)

П Р И К А З

«16» марта 2019 г. Москва № 60

О внесении изменений в Требования по обеспечению безопасности значимых объектов критической информационной инфраструктуры Российской Федерации, утвержденные приказом Федеральной службы по техническому и экспортному контролю от 25 декабря 2017 г. № 239

В соответствии с пунктом 4 части 3 статьи 6 Федерального закона от 26 июля 2017 г. № 187-ФЗ «О безопасности критической информационной инфраструктуры Российской Федерации» (Собрание законодательства Российской Федерации, 2017, № 31, ст. 4736) **П Р И К А З Ы В А Ю:**

1. Внести в Требования по обеспечению безопасности значимых объектов критической информационной инфраструктуры Российской Федерации, утвержденные приказом Федеральной службы по техническому и экспортному контролю от 25 декабря 2017 г. № 239 (зарегистрирован Министерством юстиции Российской Федерации 26 марта 2018 г., регистрационный № 50524) (с изменениями, внесенными приказом Федеральной службы по техническому и экспортному контролю от 9 августа 2018 г. № 138 (зарегистрирован Министерством юстиции Российской Федерации 5 сентября 2018 г., регистрационный № 52071), следующие изменения:

1) в пункте 10:

Проект ФЗ о внесении изменений в КоАП РФ

- нарушение порядка **категорирования** объектов КИИ РФ:
 - должностные лица – от 10 000 до 50 000 рублей
 - юридические лица - от 50 000 до 100 000 рублей

- нарушение требований к **созданию** систем безопасности ЗОКИИ и **обеспечению** их функционирования:
 - должностные лица – от 10 000 до 40 000 рублей
 - юридические лица - от 50 000 до 100 000 рублей

- нарушение **требований** по обеспечению безопасности ЗОКИИ, за исключением случаев, повлекших причинение вреда КИИ РФ:
 - должностные лица – от 10 000 до 50 000 рублей
 - юридические лица – от 50 000 до 100 000 рублей

ПРОЕКТ
ФЕДЕРАЛЬНЫЙ ЗАКОН О внесении изменений в Кодекс Российской Федерации об административных правонарушениях в части установления административной ответственности за нарушение законодательства в области обеспечения безопасности критической информационной инфраструктуры Российской Федерации
Статья 1 Внести в Кодекс Российской Федерации об административных правонарушениях следующие изменения:
1) часть 1 статьи 4.5 после слов «частью 2 статьи 12.30 настоящего Кодекса)» дополнить словами «законодательства в области обеспечения безопасности критической информационной инфраструктуры Российской Федерации.»;
2) главу 13 дополнить статьей 13.12.1 следующего содержания: «Статья 13.12.1. Нарушение требований в области обеспечения безопасности критической информационной инфраструктуры Российской Федерации
1. Нарушение порядка категорирования объектов критической информационной инфраструктуры Российской Федерации, – влечет наложение административного штрафа на должностных лиц в размере от десяти тысяч до пятидесяти тысяч рублей; на юридических лиц – от пятидесяти тысяч до ста тысяч рублей.
2. Нарушение требований к созданию систем безопасности значимых объектов критической информационной инфраструктуры Российской Федерации и обеспечению их функционирования, установленных федеральными законами и принятыми в соответствии с ними иными нормативными правовыми актами Российской Федерации, – влечет наложение административного штрафа на должностных лиц в размере от десяти тысяч до сорока тысяч рублей; на юридических лиц – от пятидесяти тысяч до ста тысяч рублей.
3. Нарушение требований по обеспечению безопасности значимых объектов критической информационной инфраструктуры Российской Федерации, установленных федеральными законами и принятыми в соответствии с ними иными нормативными правовыми актами Российской Федерации, за исключением случаев, повлекших причинение вреда критической информационной инфраструктуре Российской Федерации, – влечет наложение административного штрафа на должностных лиц в размере от десяти тысяч до пятидесяти тысяч рублей; на юридических лиц

Проект ФЗ о внесении изменений в КоАП РФ

- **непредставление или нарушение сроков представления сведений** о результатах присвоения объекту КИИ РФ одной из категорий значимости либо об отсутствии необходимости присвоения ему одной из таких категорий:
 - должностные лица – от 10 000 до 50 000 рублей
 - юридические лица – от 50 000 до 100 000 рублей
- **непредставление или нарушение порядка либо сроков представления в ГосСОПКА информации**, предусмотренной законодательством в области обеспечения безопасности КИИ РФ:
 - должностные лица – от 10 000 до 50 000 рублей
 - юридические лица – от 100 000 до 500 000 рублей

ПРОЕКТ
ФЕДЕРАЛЬНЫЙ ЗАКОН О внесении изменений в Кодекс Российской Федерации об административных правонарушениях в части установления административной ответственности за нарушение законодательства в области обеспечения безопасности критической информационной инфраструктуры Российской Федерации
Статья 1 Внести в Кодекс Российской Федерации об административных правонарушениях следующие изменения: 1) часть 1 статьи 4.5 после слов «частью 2 статьи 12.30 настоящего Кодекса)» дополнить словами «законодательства в области обеспечения безопасности критической информационной инфраструктуры Российской Федерации.»; 2) главу 13 дополнить статьей 13.12.1 следующего содержания: «Статья 13.12.1. Нарушение требований в области обеспечения безопасности критической информационной инфраструктуры Российской Федерации 1. Нарушение порядка категорирования объектов критической информационной инфраструктуры Российской Федерации, – влечет наложение административного штрафа на должностных лиц в размере от десяти тысяч до пятидесяти тысяч рублей; на юридических лиц – от пятидесяти тысяч до ста тысяч рублей. 2. Нарушение требований к созданию систем безопасности значимых объектов критической информационной инфраструктуры Российской Федерации и обеспечению их функционирования, установленных федеральными законами и принятыми в соответствии с ними иными нормативными правовыми актами Российской Федерации, – влечет наложение административного штрафа на должностных лиц в размере от десяти тысяч до сорока тысяч рублей; на юридических лиц – от пятидесяти тысяч до ста тысяч рублей. 3. Нарушение требований по обеспечению безопасности значимых объектов критической информационной инфраструктуры Российской Федерации, установленных федеральными законами и принятыми в соответствии с ними иными нормативными правовыми актами Российской Федерации, за исключением случаев, повлекших причинение вреда критической информационной инфраструктуре Российской Федерации, – влечет наложение административного штрафа на должностных лиц в размере от десяти тысяч до пятидесяти тысяч рублей; на юридических лиц

Проект ФЗ о внесении изменений в КоАП РФ

- нарушение **порядка информирования** о компьютерных инцидентах, реагирования на них, принятия мер по ликвидации последствий компьютерных атак, проведенных в отношении ЗОКИИ:
 - должностные лица – от 10 000 до 50 000 рублей
 - юридические лица – от 150 000 до 200 000 рублей

- нарушение **порядка обмена** информацией о компьютерных инцидентах между субъектами КИИ, между субъектами КИИ и уполномоченными органами иностранных государств, международными неправительственными организациями и иностранными организациями, осуществляющими деятельность в области реагирования на компьютерные инциденты:
 - должностные лица – от 20 000 до 50 000 рублей
 - юридические лица – от 100 000 до 200 000 рублей

ПРОЕКТ
ФЕДЕРАЛЬНЫЙ ЗАКОН О внесении изменений в Кодекс Российской Федерации об административных правонарушениях в части установления административной ответственности за нарушение законодательства в области обеспечения безопасности критической информационной инфраструктуры Российской Федерации
Статья 1 Внести в Кодекс Российской Федерации об административных правонарушениях следующие изменения:
1) часть 1 статьи 4.5 после слов «частью 2 статьи 12.30 настоящего Кодекса)» дополнить словами «законодательства в области обеспечения безопасности критической информационной инфраструктуры Российской Федерации.»;
2) главу 13 дополнить статьей 13.12.1 следующего содержания: «Статья 13.12.1. Нарушение требований в области обеспечения безопасности критической информационной инфраструктуры Российской Федерации
1. Нарушение порядка категорирования объектов критической информационной инфраструктуры Российской Федерации, – влечет наложение административного штрафа на должностных лиц в размере от десяти тысяч до пятидесяти тысяч рублей; на юридических лиц – от пятидесяти тысяч до ста тысяч рублей.
2. Нарушение требований к созданию систем безопасности значимых объектов критической информационной инфраструктуры Российской Федерации и обеспечению их функционирования, установленных федеральными законами и принятыми в соответствии с ними иными нормативными правовыми актами Российской Федерации, – влечет наложение административного штрафа на должностных лиц в размере от десяти тысяч до сорока тысяч рублей; на юридических лиц – от пятидесяти тысяч до ста тысяч рублей.
3. Нарушение требований по обеспечению безопасности значимых объектов критической информационной инфраструктуры Российской Федерации, установленных федеральными законами и принятыми в соответствии с ними иными нормативными правовыми актами Российской Федерации, за исключением случаев, повлекших причинение вреда критической информационной инфраструктуре Российской Федерации, – влечет наложение административного штрафа на должностных лиц в размере от десяти тысяч до пятидесяти тысяч рублей; на юридических лиц

A 3D rendered robotic hand, primarily white with blue accents, is shown in a dynamic, reaching pose. The hand is set against a dark blue background with faint, glowing icons of various devices and network connections. A semi-transparent white rectangular box is overlaid on the left side of the image, containing the title text.

ГОСУДАРСТВЕННЫЕ ИНФОРМАЦИОННЫЕ СИСТЕМЫ

Проект ПП «О некоторых вопросах выполнения требований к порядку создания, развития, ввода...»

- для федеральных органов исполнительной власти требование о наличии действующего аттестата соответствия для ввода в действие государственной информационной системы, **приостанавливается до 1 июля 2020 г.**
- руководители федеральных органов исполнительной власти **несут персональную ответственность** за:
 - **выполнение требований законодательства Российской Федерации** о защите информации, содержащейся в государственных информационных системах
 - **своевременное планирование** и эффективность реализации мероприятий по информатизации

**ПРАВИТЕЛЬСТВО РОССИЙСКОЙ ФЕДЕРАЦИИ
ПОСТАНОВЛЕНИЕ**

от « » _____ 2019 г. № ____

МОСКВА

О некоторых вопросах выполнения требований к порядку создания, развития, ввода в эксплуатацию, эксплуатации и вывода из эксплуатации государственных информационных систем и дальнейшего хранения содержащейся в их базах данных информации
Правительство Российской Федерации постановляет:

1. Установить, что:

а) для федеральных органов исполнительной власти действие пункта 19¹ требований к порядку создания, развития, ввода в эксплуатацию, эксплуатации и вывода из эксплуатации государственных информационных систем и дальнейшего хранения содержащейся в их базах данных информации, утвержденных постановлением Правительства Российской Федерации от 6 июля 2015г. № 676 «О требованиях к порядку создания, развития, ввода в эксплуатацию, эксплуатации и вывода из эксплуатации государственных информационных систем и дальнейшего хранения содержащейся в их базах данных информации» (Собрание законодательства Российской Федерации, 2015, № 28, ст. 4241; № 47, ст. 6599; 2017, № 21, ст. 3007), в отношении случая отсутствия действующего аттестата соответствия требованиям безопасности информации, предусмотренного подпунктом «а» пункта 15 указанных требований, приостанавливается до 1 июля 2020 г.;

б) руководители федеральных органов исполнительной власти несут персональную ответственность за:

выполнение требований законодательства Российской Федерации о защите информации, содержащейся в государственных информационных системах, включая выполнение требований устанавливаемых в пределах своих полномочий федеральным органом исполнительной власти в области обеспечения безопасности и федеральным органом исполнительной власти, уполномоченным в области противодействия техническим разведкам и технической защиты информации;

своевременное планирование и эффективность реализации мероприятий по информатизации, направленных на выполнение указанных в абзаце втором настоящего подпункта требований.

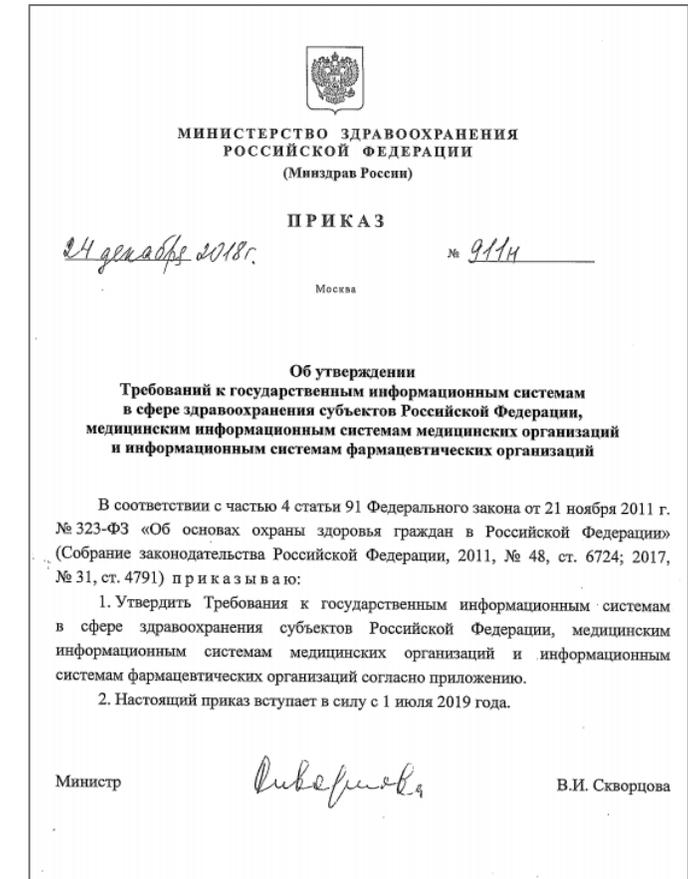
2. Федеральным органам исполнительной власти:

а) в месячный срок обеспечить планирование, при необходимости корректировку и, включение в соответствии с постановлением Правительства Российской Федерации от 24 мая 2010 г. № 365 «О координации мероприятий по использованию информационно-коммуникационных технологий в деятельности государственных органов» (Собрание законодательства Российской Федерации, 2010, № 22, ст. 2778; 2012, № 19, ст. 2419; № 37, ст. 5002; № 43, ст. 5883, 2013, № 48, ст. 6259; 2016, № 20, ст. 2832; 2017, № 29, ст. 4366) в планы информатизации на

Приказ Минздрава России №911н

Программно-технические средства ИС должны:

- располагаться на территории Российской Федерации (вне зависимости от классов и категорий)
- обеспечивать бесперебойное круглосуточное функционирование ИС в непрерывном режиме, за исключением установленных периодов проведения работ по обслуживанию ИС и устранению неисправностей – суммарная длительность не более 4 часов в месяц



МИНИСТЕРСТВО ЗДРАВООХРАНЕНИЯ
РОССИЙСКОЙ ФЕДЕРАЦИИ
(Минздрав России)

ПРИКАЗ

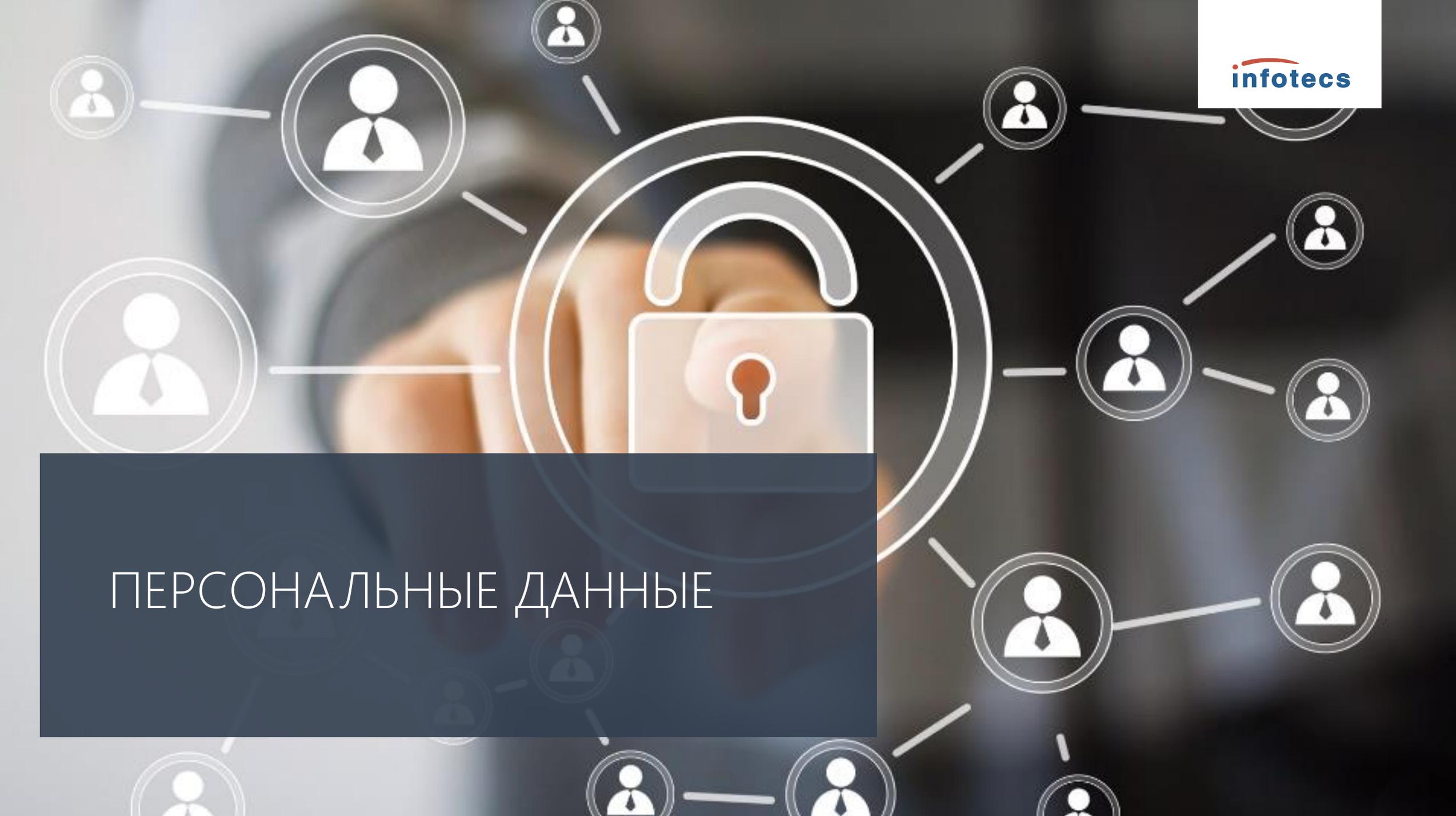
24 декабря 2018г. № 911н
Москва

**Об утверждении
Требований к государственным информационным системам
в сфере здравоохранения субъектов Российской Федерации,
медицинским информационным системам медицинских организаций
и информационным системам фармацевтических организаций**

В соответствии с частью 4 статьи 91 Федерального закона от 21 ноября 2011 г. № 323-ФЗ «Об основах охраны здоровья граждан в Российской Федерации» (Собрание законодательства Российской Федерации, 2011, № 48, ст. 6724; 2017, № 31, ст. 4791) п р и к а з ы в а ю:

1. Утвердить Требования к государственным информационным системам в сфере здравоохранения субъектов Российской Федерации, медицинским информационным системам медицинских организаций и информационным системам фармацевтических организаций согласно приложению.
2. Настоящий приказ вступает в силу с 1 июля 2019 года.

Министр  В.И. Скворцова

The background of the slide is a blurred image of a hand holding a silver padlock. Overlaid on this is a network diagram consisting of several white circular icons, each containing a stylized person in a suit and tie. These icons are connected by thin white lines, forming a web-like structure. A large, semi-transparent dark blue rectangle is positioned in the lower-left quadrant, containing the text 'ПЕРСОНАЛЬНЫЕ ДАННЫЕ' in white, uppercase letters.

ПЕРСОНАЛЬНЫЕ ДАННЫЕ

Проект ФЗ о внесении изменений в ФЗ №152

Добавляется новый объект защиты – информация, полученная из **биоматериала человека, который содержит геномную информацию**, позволяющая получить дополнительные сведения о человеке (о состоянии здоровья и других индивидуальных характеристиках)

Вступает в силу по истечении **180 дней** после дня его официального опубликования

Проект

Вносится Правительством
Российской Федерации

ФЕДЕРАЛЬНЫЙ ЗАКОН

О внесении изменений в статью 11 Федерального закона «О персональных данных» и статью 39.1 Закона Российской Федерации «О защите прав потребителей» в части установления особенностей обработки персональных данных, полученных из биологического и генетического материала человека и оказания услуг, связанных с использованием и обращением биологического и генетического материала человека

Статья 1

Внести в статью 11 Федерального закона «О персональных данных» от 27 июля 2006 года № 152-ФЗ (Собрание законодательства Российской Федерации, 2006, № 31, ст. 3451, 2009, № 48, ст. 5716, № 52, ст. 6439, 2010, № 31, ст. 4173, № 31, ст. 4196, № 49, ст. 6409, 2011, № 23, ст. 3263, № 31, ст. 4701, 2013, № 14, ст. 1651, № 30, ст. 4038, № 51, ст. 6683, 2014, № 23, ст. 2927, № 30, ст. 4217, № 30, ст. 4243, 2016, № 27, ст. 4164, 2017, № 9, ст. 1276, № 27, ст. 3945, № 31, ст. 4772, 2018, № 1, ст. 82) следующие изменения:

- 1) в части 1 слова «и биологические» заменить словами «, биологические и генетические»;
- 2) в части 2 после слов «дактилоскопической регистрации,» дополнить словами «обязательной государственной геномной регистрации.»

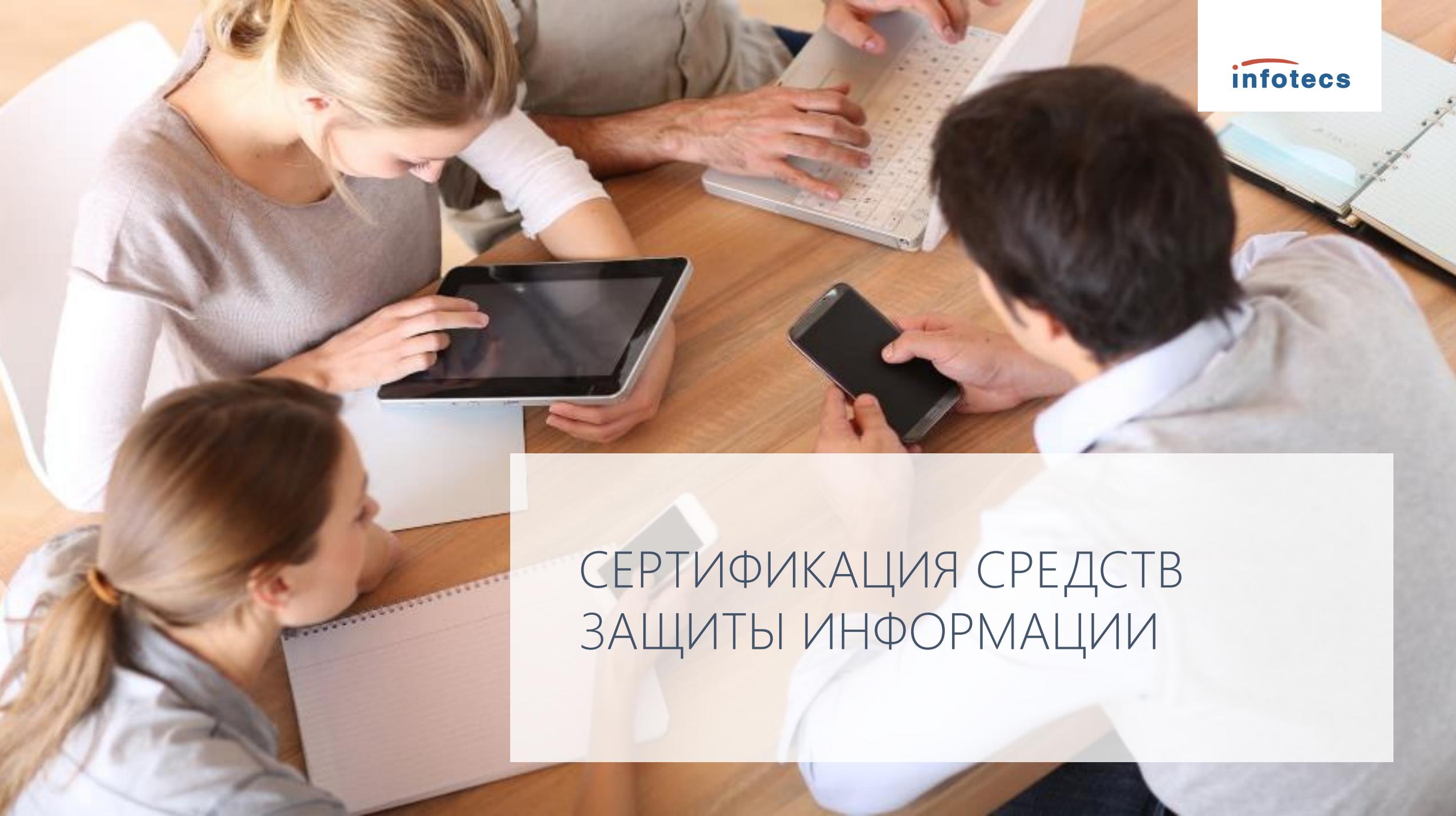
Статья 2

Статью 39.1 Закона Российской Федерации от 7 февраля 1992 года № 2300-1 «О защите прав потребителей» (Ведомости Съезда народных депутатов Российской Федерации и Верховного Совета Российской Федерации, 1992, № 15, ст. 766; Собрание законодательства Российской Федерации, 1996, № 3, ст. 140; 1999, № 51, ст. 6287; 2004, № 52, ст. 5275; 2011, № 30, ст. 4590)

Постановление Правительства Российской Федерации №146

- утверждаются правила организации и осуществления государственного контроля и надзора за обработкой персональных данных
- действие **не распространяется** на контроль и надзор за выполнением **организационных и технических мер** по обеспечению безопасности персональных данных, обрабатываемых в ИСПДн



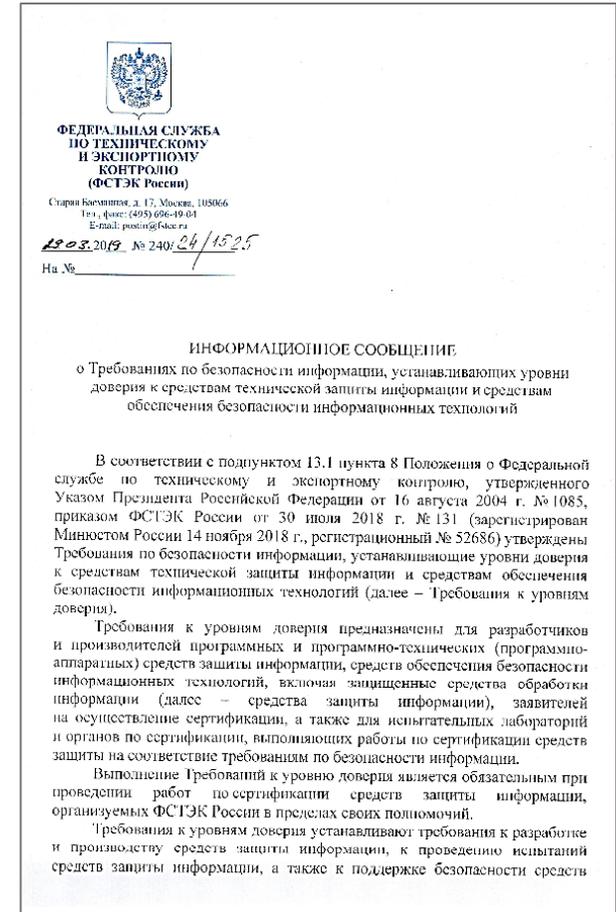
A high-angle photograph of four business professionals (three women and one man) sitting around a wooden table. They are engaged in a meeting, looking at various devices: a tablet, a laptop, and a smartphone. The scene is brightly lit, suggesting an office environment.

СЕРТИФИКАЦИЯ СРЕДСТВ ЗАЩИТЫ ИНФОРМАЦИИ

Информационное сообщение ФСТЭК России № 240/24/1525



- требования к уровню доверия подлежат применению при сертификации средств защиты информации с 1 июня 2019 г.
- действие сертификатов соответствия средств защиты информации, в отношении которых не проведена оценка соответствия требованиям к уровням доверия до 1 января 2020 г., может быть приостановлено



Информационное сообщение ФСТЭК России № 240/24/1525

Тип ИС	Класс/уровень защищенности	Уровень доверия			
		6	5	4	3, 2, 1
ГИС	К1			+	Для ГТ
	К2		+		
	К3	+			
ЗОКИИ	1			+	
	2		+		
	3	+			
АСУ ТП	1			+	
	2		+		
	3	+			
ИСПДн	У31			+	
	У32		+		
	У33	+			
	У34	+			
ИСОП	1				
	2			+	

Ссылки на документы

1. Проект Приказа ФСТЭК России «О внесении изменений в Требования о защите информации, не составляющей государственную тайну, содержащейся в государственных информационных системах, утвержденные приказом Федеральной службы по техническому и экспортному контролю от 11 февраля 2013 г. № 17» -
<https://regulation.gov.ru/Projects/List#npa=90839>
2. Постановление Правительства Российской Федерации от 11.04.2019 № 420 «О внесении изменений в требования к порядку создания, развития, ввода в эксплуатацию, эксплуатации и вывода из эксплуатации государственных информационных систем и дальнейшего хранения содержащейся в их базах данных информации» –
<http://publication.pravo.gov.ru/Document/View/0001201904190009>
3. Проект Постановления Правительства Российской Федерации «О некоторых вопросах выполнения требований к порядку создания, развития, ввода в эксплуатацию, эксплуатации и вывода из эксплуатации государственных информационных систем и дальнейшего хранения содержащейся в их базах данных информации» -
<https://regulation.gov.ru/Projects/List#npa=90740>
4. Приказ Министерства здравоохранения РФ №911н «Требования к государственным информационным системам в сфере здравоохранения субъектов Российской Федерации, медицинским информационным системам медицинских организаций и информационным системам фармацевтических организаций» –
http://spbmiac.ru/wpcontent/uploads/2019/01/2018.12.24_%E2%84%96_911_%D0%BD_%D0%BF%D1%80%D0%B8%D0%BA%D0%B0%D0%B7_%D0%9C%D0%B8%D0%BD%D0%B7%D0%B4%D1%80%D0%B0%D0%B2%D0%B0.pdf
5. Постановление Правительства Российской Федерации от 15.04.2019 № 454 «О внесении изменения в перечень мер, направленных на обеспечение выполнения обязанностей, предусмотренных Федеральным законом "О персональных данных" и принятыми в соответствии с ним нормативными правовыми актами, операторами, являющимися государственными или муниципальными органами» –
<http://publication.pravo.gov.ru/Document/View/0001201904170020>

Ссылки на документы

6. Проект Федерального закона «О внесении изменений в отдельные законодательные акты (в части уточнения процедур идентификации и аутентификации)» -
<https://regulation.gov.ru/projects#npa=89356>
7. Постановление Правительства Российской Федерации от 13.02.2019 № 146 "Об утверждении Правил организации и осуществления государственного контроля и надзора за обработкой персональных данных« –
<http://publication.pravo.gov.ru/Document/View/0001201902150008>
8. Проект ФЗ «О внесении изменений в статью 11 Федерального закона «О персональных данных» и статью 39.1 Закона Российской Федерации «О защите прав потребителей» в части установления особенностей обработки персональных данных, полученных из биологического и генетического материала человека и оказания услуг, связанных с использованием и обращением биологического и генетического материала человека» -
<https://regulation.gov.ru/projects/List/AdvancedSearch#npa=87215>
9. Информационное сообщение ФСТЭК России № 240/24/1525 «о Требованиях по безопасности информации, устанавливающих уровни доверия к средствам технической защиты информации и средствам обеспечения безопасности информационных технологий» -
<https://fstec.ru/component/attachments/download/2287>
10. Постановление Правительства Российской Федерации от 13.04.2019 № 452 «О внесении изменений в постановление Правительства Российской Федерации от 8 февраля 2018 г. № 127» –
<http://publication.pravo.gov.ru/Document/View/0001201904160054>

Ссылки на документы

11. Проект Приказа ФСТЭК России «О внесении изменений в Требования к созданию систем безопасности значимых объектов критической информационной инфраструктуры Российской Федерации и обеспечению их функционирования, утвержденные приказом Федеральной службы по техническому и экспортному контролю от 21 декабря 2017 г. № 235» – <https://regulation.gov.ru/projects#npa=89049>
12. Приказ ФСТЭК России от 21.03.2019 № 59 «О внесении изменений в форму направления сведений о результатах присвоения объекту критической информационной инфраструктуры одной из категорий значимости либо об отсутствии необходимости присвоения ему одной из таких категорий, утвержденную приказом Федеральной службы по техническому и экспортному контролю от 22 декабря 2017 г. № 236» - <http://publication.pravo.gov.ru/Document/View/0001201904190035>
13. Приказ ФСТЭК России от 26.03.2019 № 60 «О внесении изменений в Требования по обеспечению безопасности значимых объектов критической информационной инфраструктуры Российской Федерации, утвержденные приказом Федеральной службы по техническому и экспортному контролю от 25 декабря 2017 г. № 239» – <http://publication.pravo.gov.ru/Document/View/0001201904190031>
14. Проект Федерального закона «О внесении изменений в Кодекс Российской Федерации об административных правонарушениях (в части установления ответственности за нарушение требований по обеспечению безопасности объектов критической информационной инфраструктуры)» – https://regulation.gov.ru/projects?fbclid=IwAR14PGFrJOD8l4agi2sUC976AsII_VAqsE8yZxkHTJvmy5cJxppbq5kYEbw#npa=89944
15. Приказ ФСТЭК России от 3 апреля 2018 г. №55 «Положение о системе сертификации средств защиты информации» – <https://fstec.ru/component/attachments/download/1883>
16. Приказ Минздрава России от 4 марта 2019 г. № 110н «Об отработке персональных данных в Министерстве здравоохранения Российской Федерации» – <https://cdnimg.rg.ru/pril/169/62/39/54755.pdf>

Спасибо
за внимание!

Александр Шипков, CISSP
Aleksandr.Shipkov@infotecs.ru