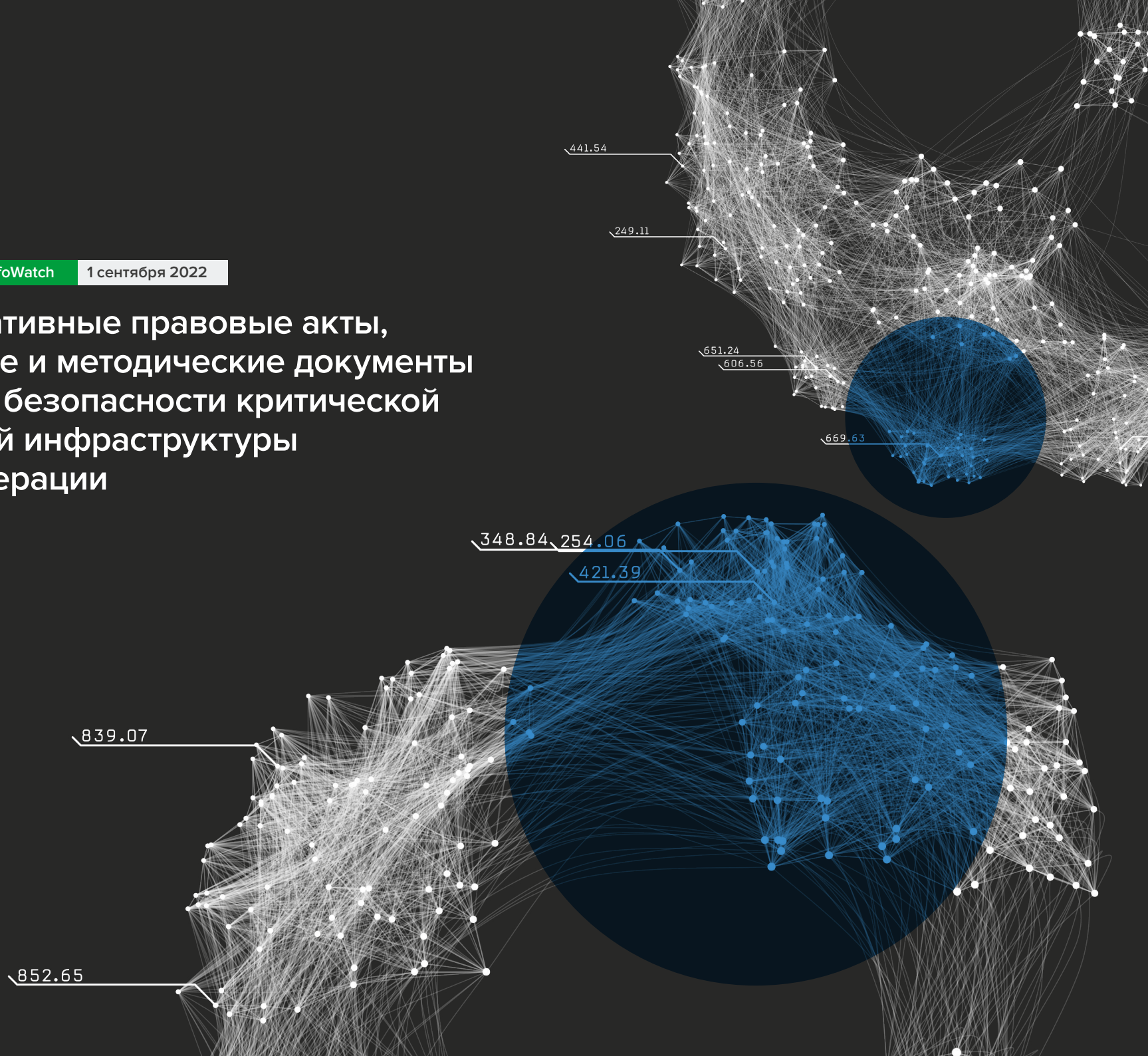
INFOWATCH®

Экспертно-аналитический центр InfoWatch | 1 сентября 2022

Основные нормативные правовые акты, организационные и методические документы по обеспечению безопасности критической информационной инфраструктуры Российской Федерации



Оглавление

Федеральные законы

Федеральный закон от 26 июля 2017 № 187-ФЗ «О безопасности критической информационной инфраструктуры Российской Федерации». Вступил в силу 1 января 2018.

Федеральный закон от 26 июля 2017 № 193-ФЗ «О внесении изменений в отдельные законодательные акты Российской Федерации в связи с принятием федерального закона „О безопасности критической информационной инфраструктуры Российской Федерации“»:

— Закон Российской Федерации от 21 июля 1993 № 5485-I «О государственной тайне» (пункт 4 статьи 5)

— Федеральный закон от 7 июля 2003 № 126-ФЗ «О связи» (пункт 11 статьи 12, пункт 1 статьи 46)

— Федеральный закон от 26 декабря 2008 № 294-ФЗ «О защите прав юридических лиц и индивидуальных предпринимателей при осуществлении государственного контроля (надзора) и муниципального контроля» (часть 31 статьи 1)

Вступил в силу 1 января 2018.

Федеральный закон от 26 июля 2017 № 194-ФЗ «О внесении изменений в Уголовный кодекс Российской Федерации и статью 151 Уголовно-процессуального кодекса Российской Федерации в связи с принятием Федерального закона „О безопасности критической информационной инфраструктуры Российской Федерации“»:

— Уголовный кодекс Российской Федерации (статья 274.1 «Неправомерное воздействие на критическую информационную инфраструктуру Российской Федерации)»

— Уголовно-процессуальный кодекс Российской Федерации (статья 151)

Вступил в силу 1 января 2018.

Федеральный закон от 26 мая 2021 № 141-ФЗ «О внесении изменений в Кодекс Российской Федерации об административных правонарушениях»:

— Статья 13.12.1. Нарушение требований в области обеспечения безопасности критической информационной инфраструктуры Российской Федерации

— Статья 19.7.15. Непредставление сведений, предусмотренных законодательством в области обеспечения безопасности критической информационной инфраструктуры Российской Федерации

— Статья 23.90. Федеральный орган исполнительной власти, уполномоченный в области обеспечения безопасности критической информационной инфраструктуры Российской Федерации

— Статья 23.91. Федеральный орган исполнительной власти, уполномоченный в области обеспечения функционирования государственной системы обнаружения, предупреждения и ликвидации последствий компьютерных атак на информационные ресурсы Российской Федерации

Вступил в силу по истечении десяти дней после официальной публикации — 6 июня 2021, за исключением абзацев третьего и четвёртого пункта 2 статьи 1 настоящего Федерального закона. Абзацы третий и четвёртый пункта 2 статьи 1 настоящего Федерального закона вступили в силу с 1 сентября 2021 (часть 1 статьи 13.12.1).

Указы Президента Российской Федерации

Указ Президента РФ от 15 января 2013 № 31с «О создании государственной системы обнаружения, предупреждения и ликвидации последствий компьютерных атак на информационные ресурсы Российской Федерации». Опубликован и вступил в силу 15 января 2013.

Указ Президента РФ от 12 декабря 2014 № К 1274 «О Концепции государственной системы обнаружения, предупреждения и ликвидации последствий компьютерных атак на информационные ресурсы Российской Федерации». Выписка из Концепции государственной системы обнаружения, предупреждения и ликвидации последствий компьютерных атак на информационные ресурсы Российской Федерации. Опубликован 12 декабря 2014.

Указ Президента РФ от 25 ноября 2017 № 569 «О внесении изменений в Положение о Федеральной службе по техническому и экспортному контролю, утвержденное Указом Президента Российской Федерации от 16 августа 2004 № 1085». Опубликован 25 ноября 2017.

Указ Президента РФ от 22 декабря 2017 № 620 «О совершенствовании государственной системы обнаружения, предупреждения и ликвидации последствий компьютерных атак на информационные ресурсы Российской Федерации». Опубликован 22 декабря 2017.

Указ Президента РФ от 2 марта 2018 № 98 «О внесении изменения в перечень сведений, отнесённых к государственной тайне, утверждённый Указом Президента Российской Федерации от 30 ноября 1995 № 1203». Опубликован 2 марта 2018.

Указ Президента РФ от 14 апреля 2022 № 203 «О Межведомственной комиссии Совета Безопасности Российской Федерации по вопросам обеспечения технологического суверенитета государства в сфере развития критической информационной инфраструктуры Российской Федерации». Опубликован 14 апреля 2022.

Указ Президента РФ от 30 марта 2022 № 166 «О мерах по обеспечению технологической независимости и безопасности критической информационной инфраструктуры Российской Федерации». Опубликован 30 марта 2022.

Указ Президента РФ от 1 мая 2022 № 250 «О дополнительных мерах по обеспечению информационной безопасности Российской Федерации». Опубликован 1 мая 2022.

Постановления Правительства Российской Федерации

Постановление Правительства РФ от 13 апреля 2019 № 452 «О внесении изменений в постановление Правительства Российской Федерации от 8 февраля 2018 № 127». Опубликовано 16 апреля 2019.

Постановление Правительства РФ от 17 февраля 2018 № 162 «Об утверждении Правил осуществления государственного контроля в области обеспечения безопасности значимых объектов критической информационной инфраструктуры Российской Федерации». Опубликовано 21 февраля 2018 (fstec.ru, consultant.ru).

Постановление Правительства РФ от 8 февраля 2018 № 127 (ред. от 13 апреля 2019) «Об утверждении Правил категорирования объектов критической информационной инфраструктуры Российской Федерации, а также перечня показателей критериев значимости объектов критической информационной инфраструктуры Российской Федерации и их значений». Опубликовано 16 апреля 2019.

Постановление Правительства РФ от 8 июня 2019 № 743 «Об утверждении Правил подготовки и использования ресурсов единой сети электросвязи Российской Федерации для обеспечения функционирования значимых объектов критической информационной инфраструктуры». Опубликовано 11 июня 2019 (pravo.gov.ru, docs.cntd.ru).

Постановление Правительства РФ от 11 июля 2018 № 808 «О внесении изменения в Правила организации повышения квалификации специалистов по ЗИ и должностных лиц, ответственных за организацию ЗИ в ОГВ, ОМС, организациях с госучастием и организациях ОПК». Опубликовано 13 июля 2018.

Постановление Правительства РФ от 7 октября 2019 № 1285 «Об утверждении Правил предоставления субсидий из федерального бюджета на создание отраслевого центра Государственной системы обнаружения, предупреждения и ликвидации последствий компьютерных атак (ГосСОПКА) и включение его в систему автоматизированного обмена информацией об актуальных киберугрозах». Опубликовано 9 октября 2019.

Постановление Правительства РФ от 24 июня 2021 № 981 «Об утверждении Правил формирования и утверждения перечня критически важных объектов». Опубликовано 28 июня 2021.

Постановление Правительства РФ от 23 октября 2021 № 1815 «Об утверждении перечня случаев осуществления сбора и обработки используемых для идентификации либо идентификации и аутентификации биометрических персональных данных в информационных системах организаций, осуществляющих идентификацию и (или) аутентификацию с использованием биометрических персональных данных физических лиц, а также случаев использования организациями, за исключением кредитных организаций, некредитных финансовых организаций, которые осуществляют указанные в части первой статьи 761 Федерального закона „О Центральном банке Российской Федерации (Банке России)“ виды деятельности, субъектами национальной платёжной системы, индивидуальными предпринимателями указанных информационных систем для идентификации либо идентификации и аутентификации физического лица, выразившего согласие на их проведение». Опубликовано 26 октября 2021.

Из перечня случаев осуществления сбора и обработки биометрических персональных данных при проходе на территорию организаций посредством системы контроля и управления доступа организации-субъекты КИИ исключены.

Постановление Правительства РФ от 24 декабря 2021 № 2431 «О внесении изменений в Правила категорирования объектов критической информационной инфраструктуры Российской Федерации». Опубликовано 27 декабря 2021.

Постановление Правительства РФ от 19 августа 2022 № 1463 «О внесении изменения в Правила категорирования объектов критической информационной инфраструктуры Российской Федерации». Опубликовано 23 августа 2022.

Постановление Правительства РФ от 22 августа 2022 № 1478 «Об утверждении требований к программному обеспечению, в том числе в составе программно-аппаратных комплексов, используемому органами государственной власти, заказчиками, осуществляющими закупки в соответствии с Федеральным законом „О закупках товаров, работ, услуг отдельными видами юридических лиц“ (за исключением организаций с муниципальным участием), на принадлежащих им значимых объектах критической информационной инфраструктуры Российской Федерации, Правил согласования закупок иностранного программного обеспечения, в том числе в составе программно-аппаратных комплексов, в целях его использования заказчиками, осуществляющими закупки в соответствии с Федеральным законом „О закупках товаров, работ, услуг отдельными видами юридических лиц“ (за исключением организаций с муниципальным участием), на принадлежащих им значимых объектах критической информационной инфраструктуры Российской Федерации, а также закупок услуг, необходимых для использования этого программного обеспечения на таких объектах, и Правил перехода на преимущественное использование российского программного обеспечения, в том числе в составе программно-аппаратных комплексов, органов государственной власти, заказчиков, осуществляющих закупки в соответствии с Федеральным законом „О закупках товаров, работ, услуг отдельными видами юридических лиц“ (за исключением организаций с муниципальным участием), на принадлежащих им значимых объектах критической информационной инфраструктуры Российской Федерации». Опубликовано 26 августа 2022.

Распоряжение Правительства РФ от 22 июня 2022 № 1661-р (во исполнение Указа № 250) об утверждении ключевых органов (организаций), которым необходимо осуществить мероприятия по оценке уровня защищённости своих информационных систем с привлечением организаций, имеющих соответствующие лицензии ФСБ России и ФСТЭК России. Опубликовано 24 июня 2022.

Постановление Правительства РФ от 15 июля 2022 № 1272 «Об утверждении типового положения о заместителе руководителя органа (организации), ответственном за обеспечение информационной безопасности в органе (организации), и типового положения о структурном подразделении в органе (организации), обеспечивающем информационную безопасность органа (организации)». Опубликовано 19 июля 2022.

Приказы и сообщения Федеральной службы по техническому и экспортному контролю

Приказ ФСТЭК России от 6 декабря 2017 № 227 «Об утверждении Порядка ведения реестра значимых объектов критической информационной инфраструктуры Российской Федерации» (зарегистрировано в Минюсте России 8 февраля 2018 № 49966). Опубликован 9 февраля 2018 (fstec.ru, pravo.gov.ru).

Приказ ФСТЭК России от 11 декабря 2017 № 229 «Об утверждении формы акта проверки, составляемого по итогам проведения государственного контроля в области обеспечения безопасности значимых объектов критической информационной инфраструктуры Российской Федерации» (зарегистрировано в Минюсте России 28 декабря 2017 № 49500). Опубликован 28 декабря 2017 (fstec.ru, pravo.gov.ru).

Приказ ФСТЭК России от 21 декабря 2017 № 235 (ред. от 27 марта 2019) «Об утверждении Требований к созданию систем безопасности значимых объектов критической информационной инфраструктуры Российской Федерации и обеспечению их функционирования» (зарегистрировано в Минюсте России 22 февраля 2018 № 50118). Опубликован 14 июня 2019. Редакция действует с 1 января 2021.

Информационное сообщение ФСТЭК России от 4 мая 2018 № 240/22/2339. «О методических документах по вопросам обеспечения безопасности информации в ключевых системах информационной инфраструктуры Российской Федерации». Опубликовано 4 мая 2018.

Приказ ФСТЭК России от 27 марта 2019 № 64 «О внесении изменений в Требования к созданию систем безопасности значимых объектов критической информационной инфраструктуры Российской Федерации и обеспечению их функционирования, утверждённые приказом Федеральной службы по техническому и экспортному контролю от 21 декабря 2017 № 235» (зарегистрировано в Минюсте России 13 июня 2019 № 54920). Опубликован 14 июня 2019 (fstec.ru, pravo.gov.ru).

Приказ ФСТЭК России от 22 декабря 2017 № 236 (ред. от 21 марта 2019) «Об утверждении формы направления сведений о результатах присвоения объекту критической информационной инфраструктуры одной из категорий значимости либо об отсутствии необходимости присвоения ему одной из таких категорий» (зарегистрировано в Минюсте России 13 апреля 2018 № 50753). Опубликован 19 апреля 2019.

Приказ ФСТЭК России от 21 марта 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, утверждённую приказом Федеральной службы по техническому и экспортному контролю от 22 декабря 2017 № 236» (зарегистрировано в Минюсте России 18 апреля 2019 № 54436). Опубликован 19 апреля 2019.

Приказ ФСТЭК России от 25 декабря 2017 № 239 (в ред. 9 августа 2018 № 138, от 26 марта 2019 № 60, от 20 февраля 2020 № 35) «Об утверждении Требований по обеспечению безопасности значимых объектов критической информационной инфраструктуры Российской Федерации» (зарегистрировано в Минюсте России 26 марта 2018 № 50524). Опубликован 14 сентября 2020.

Приказ ФСТЭК России от 20 февраля 2020 № 35 «О внесении изменений в требования по обеспечению безопасности значимых объектов критической информационной инфраструктуры Российской Федерации, утверждённые приказом Федеральной службы по техническому и экспортному контролю от 25 декабря 2017 № 239 (зарегистрировано в Минюсте России 11 сентября 2020 № 59793). Опубликован 14 сентября 2020, вступил в силу 25 сентября 2020, пп.7, 8 изменений вступают в силу 1 января 2023.

Приказ ФСТЭК России от 26 марта 2019 № 60 «О внесении изменений в Требования по обеспечению безопасности значимых объектов критической информационной инфраструктуры Российской Федерации, утверждённые приказом Федеральной службы по техническому и экспортному контролю от 25 декабря 2017 № 239» (зарегистрировано в Минюсте России 18 апреля 2019 № 54443). Опубликован 19 апреля 2019.

Приказ ФСТЭК России от 28 мая 2020 № 75 «Об утверждении порядка согласования субъектом критической информационной инфраструктуры российской федерации с Федеральной службой по техническому и экспортному контролю подключения значимого объекта критической информационной инфраструктуры Российской Федерации к сети связи общего пользования» (зарегистрировано в Минюсте России 15 сентября 2020 № 59866). Опубликован 28 мая 2020.

Приказ ФСТЭК России от 26 апреля 2018 № 72 «О внесении изменений в Регламент Федеральной службы по техническому и экспортному контролю, утверждённый приказом ФСТЭК России от 12 мая 2005 № 167» (зарегистрировано в Минюсте РФ 18 мая 2018 № 51127). В том числе:

— Абзац второй пункта 9 изложить в следующей редакции: «Обеспечения безопасности значимых объектов критической информационной инфраструктуры»

— В абзаце третьем пункта 15 слова «информации в ключевых системах» заменить словом «критической»

Вступил в силу 1 июня 2018.

Приказ ФСТЭК России № 76 от 2 июня 2020 «Об утверждении Требований по безопасности информации, устанавливающих уровни доверия к средствам технической защиты информации и средствам обеспечения безопасности информационных технологий» (зарегистрирован Минюстом России 11 сентября 2020). Отменил приказ ФСТЭК России № 131 от 30 июля 2018 «Об утверждении Требований по безопасности информации, устанавливающих уровни доверия к средствам технической защиты информации и средствам обеспечения безопасности информационных технологий», дата отмены — с 1 января 2021. Приказ вступает в силу:

— С 1 января 2022 — седьмой абзац пункта 12.2 и девятый абзац пункта 12.4

— С 1 января 2024 — пятый абзац пункта 12.5

— С 1 января 2028 — пятый абзац пункта 12.3

Смотрите также

Информационное сообщение ФСТЭК России от 15 октября 2020 № 240/24/4268. Об утверждении требований по безопасности информации, устанавливающих уровни доверия к средствам технической защиты информации и средствам обеспечения безопасности информационных технологий (fstec.ru).

Выписка из Требований по безопасности информации, утверждённых приказом ФСТЭК России от 2 июня 2020 № 76.

Методический документ «Методика оценки угроз безопасности информации». Утверждён ФСТЭК России 5 февраля 2021. Опубликован 5 февраля 2021.

Приказ ФСТЭК России от 14 марта 2014 № 31 (в ред. от 23 марта 2017 № 49, от 9 августа 2018 № 138, от 15 марта 2021 № 46) «Об утверждении требований к обеспечению защиты информации в автоматизированных системах управления производственными и технологическими процессами на критически важных объектах, потенциально опасных объектах, а также объектах, представляющих повышенную опасность для жизни и здоровья людей и для окружающей природной среды» (зарегистрировано в Минюсте России 30 июня 2014 № 32919).

Информационное сообщение ФСТЭК России от 17 апреля 2020 № 240/84/611. По вопросам представления перечней объектов критической информационной инфраструктуры, подлежащих категорированию, и направления сведений о результатах присвоения объекту критической информационной инфраструктуры одной из категорий значимости либо об отсутствии необходимости присвоения ему одной из таких категорий (fstec.ru).

Приказ ФСТЭК России от 23 марта 2017 № 49 «О внесении изменений в Состав и содержание организационных и технических мер по обеспечению безопасности персональных данных при их обработке в информационных системах персональных данных, утверждённые приказом Федеральной службы по техническому и экспортному контролю от 18 февраля 2013 № 21, и в Требования к обеспечению защиты информации в автоматизированных системах управления производственными и технологическими процессами на критически важных объектах, потенциально опасных объектах, а также объектах, представляющих повышенную опасность для жизни и здоровья людей и для окружающей природной среды, утверждённые приказом Федеральной службы по техническому и экспортному контролю от 14 марта 2014 № 31» (зарегистрировано в Минюсте России 25 апреля 2017 № 46487).

Приказ ФСТЭК России от 9 августа 2018 № 138 «О внесении изменений в Требования к обеспечению защиты информации в автоматизированных системах управления производственными и технологическими процессами на критически важных объектах, потенциально опасных объектах, а также объектах, представляющих повышенную опасность для жизни и здоровья людей и для окружающей природной среды, утверждённые приказом Федеральной службы по техническому и экспортному контролю от 14 марта 2014 № 31, и в Требования по обеспечению безопасности значимых объектов критической информационной инфраструктуры Российской Федерации, утверждённые приказом Федеральной службы по техническому и экспортному контролю от 25 декабря 2017 № 239» (зарегистрировано в Минюсте России 5 сентября 2018 № 52071). Опубликован 6 сентября 2018.

Приказ ФСТЭК России от 15 марта 2021 № 46 «О внесении изменений в Требования к обеспечению защиты информации в автоматизированных системах управления производственными и технологическими процессами на критически важных объектах, потенциально опасных объектах, а также объектах, представляющих повышенную опасность для жизни и здоровья людей и для окружающей природной среды, утверждённые приказом Федеральной службы по техническому и экспортному контролю от 14 марта 2014 № 31» (зарегистрирован 1 июля 2021 № 64063).

Письмо ФСТЭК России от 20 марта 2020 № 240/84/389. Рекомендации по обеспечению безопасности объектов критической информационной инфраструктуры при реализации дистанционного режима исполнения должностных обязанностей работниками субъектов критической информационной инфраструктуры (fstec.ru).

Информационное сообщение ФСТЭК России от 18 июня 2021 № 240/82/1037. О порядке представления субъектами критической информационной инфраструктуры сведений о результатах присвоения объектам критической информационной инфраструктуры одной из категорий значимости либо об отсутствии необходимости присвоения им одной из таких категорий.

Информационное сообщение ФСТЭК России от 18 декабря 2021 № 240/81/2547. О порядке представления субъектами критической информационной инфраструктуры сведений о результатах присвоения объектам критической информационной инфраструктуры одной из категорий значимости либо об отсутствии необходимости присвоения им одной из таких категорий.

Письмо ФСТЭК России от 28 февраля 2022 № 240/22/952 о мерах по повышению защищённости информационной инфраструктуры Российской Федерации.

Письмо ФСТЭК России от 6 марта 2022 № 240/22/1172 о мерах по повышению защищённости информационной инфраструктуры Российской Федерации.

Информационное сообщение ФСТЭК России от 24 марта 2022 № 240/22/1549. О мерах по повышению защищённости информационной инфраструктуры (fstec.ru).

Приказ ФСТЭК России от 10 февраля 2022 № 26 «О внесении изменений в Порядок ведения реестра значимых объектов критической информационной инфраструктуры Российской Федерации, утверждённый приказом Федеральной службы по техническому и экспортному контролю от 6 декабря 2017 № 227» (pravo.gov.ru).

Информационное сообщение ФСТЭК России от 28 июня 2022 № 240/83/1698. О порядке представления субъектами критической информационной инфраструктуры сведений о результатах присвоения объектам критической информационной инфраструктуры одной из категорий значимости либо об отсутствии необходимости присвоения ему одной из таких категорий.

Информационное сообщение ФСТЭК России от 28 февраля 2018 № 240/11/879. О методических рекомендациях по формированию аналитического прогноза по укомплектованию подразделений по обеспечению безопасности значимых объектов критической информационной инфраструктуры, противодействию иностранным техническим разведкам и технической защите информации подготовленными кадрами, утверждённых ФСТЭК России 30 сентября 2016 (в ред. от 9 февраля 2021).

Информационное сообщение ФСТЭК России от 23 апреля 2018 № 240/11/1868. О методических рекомендациях по разработке программ профессиональной переподготовки и повышения квалификации специалистов, работающих в области обеспечения безопасности значимых объектов критической информационной инфраструктуры, противодействия иностранным техническим разведкам и технической защиты информации, разработанных и утверждённых 16 апреля 2018.

Приказы и рекомендации Федеральной службы безопасности Российской Федерации

Приказ ФСБ РФ от 24 июля 2018 № 366 «О Национальном координационном центре по компьютерным инцидентам» (зарегистрирован в Минюсте России 6 сентября 2018 № 52109). Опубликован 10 сентября 2018.

Приказ ФСБ РФ от 24 июля 2018 № 367 «Об утверждении Перечня информации, представляемой в государственную систему обнаружения, предупреждения и ликвидации последствий компьютерных атак на информационные ресурсы Российской Федерации и Порядка представления информации в государственную систему обнаружения, предупреждения и ликвидации последствий компьютерных атак на информационные ресурсы Российской Федерации» (зарегистрирован в Минюсте России 6 сентября 2018 № 52108). Опубликован 10 сентября 2018.

Приказ ФСБ РФ от 24 июля 2018 № 368 «Об утверждении Порядка обмена информацией о компьютерных инцидентах между субъектами критической информационной инфраструктуры Российской Федерации, между субъектами критической информационной инфраструктуры Российской Федерации и уполномоченными органами иностранных государств, международными неправительственными организациями и иностранными организациями, осуществляющими деятельность в области реагирования на компьютерные инциденты, и Порядка получения субъектами критической информационной инфраструктуры Российской Федерации информации о средствах и способах проведения компьютерных атак и о методах их предупреждения и обнаружения» (регистрация в Минюсте России 6 сентября 2018 № 52107). Опубликован 10 сентября 2018.

Приказ ФСБ РФ от 6 мая 2019 № 196 «Об утверждении требований к средствам, предназначенным для обнаружения, предупреждения и ликвидации последствий компьютерных атак и реагирования на компьютерные инциденты» (зарегистрирован в Минюсте России 31 мая 2019 № 54801). Опубликован 31 мая 2019.

Приказ ФСБ РФ от 19 июня 2019 № 281 «Об утверждении Порядка, технических условий установки и эксплуатации средств, предназначенных для обнаружения, предупреждения и ликвидации последствий компьютерных атак и реагирования на компьютерные инциденты, за исключением средств, предназначенных для поиска признаков компьютерных атак в сетях электросвязи, используемых для организации взаимодействия объектов критической информационной инфраструктуры Российской Федерации» (зарегистрирован в Минюсте России 16 июля 2019 № 55285). Опубликован 17 июля 2019.

Приказ ФСБ РФ от 19 июня 2019 № 282 «Об утверждении Порядка информирования ФСБ России о компьютерных инцидентах, реагирования на них, принятия мер по ликвидации последствий компьютерных атак, проведённых в отношении значимых объектов критической информационной инфраструктуры Российской Федерации» (зарегистрирован в Минюсте России 16 июля 2019 № 55284). Опубликован 17 июля 2019.

Приказ ФСБ РФ от 7 июля 2022 № 348 «О внесении изменений в Порядок информирования ФСБ России о компьютерных инцидентах, реагирования на них, принятия мер по ликвидации последствий компьютерных атак, проведённых в отношении значимых объектов критической информационной инфраструктуры Российской Федерации, утверждённый приказом ФСБ России от 19 июня 2019 № 282» (зарегистрирован 5 августа 2022 № 69513).

После 24 февраля 2022 Национальный координационный центр по компьютерным инцидентам (НКЦКИ) выпустил ряд писем и рекомендаций по защите, обнаружению и ликвидации последствий компьютерных атак. Далее приведены некоторые из них

- О мерах повышения уровня защищённости информационных ресурсов Российской Федерации от целенаправленных компьютерных атак. ALRT-20220302.1. 2 марта 2022. Уровень угрозы — высокий. TLP — white
- Угроза эксплуатации уязвимостей в оборудовании компании Cisco. ALRT-20220303.1. 3 марта 2022. Уровень угрозы — критический. TLP — white
- Рекомендации по повышению уровня защищённости российских веб-приложений. ALRT-20220311.1. 11 марта 2022. TLP — white
- Рекомендации по первоочередным мерам, направленным на обнаружение, предупреждение и ликвидацию последствий компьютерных атак. ALRT-20220316.1. 16 марта 2022. TLP — white
- Рекомендации по защите от угроз фишинговых и вредоносных писем. ALRT-20220325.1. 25 марта 2022. TLP — white
- Рекомендации по защите информационной инфраструктуры компании от компьютерных атак с использованием программ-шифровальщиков. ALRT-20220325.2. 25 марта 2022. TLP — white
- Обобщённые рекомендации по минимизации возможных угроз информационной безопасности информационным ресурсам Российской Федерации. ALRT-20220329.1. 29 марта 2022. TLP — white

Приказы Минцифры Российской Федерации

Приказ Минцифры РФ от 17 марта 2020 N° 114 «Об утверждении Порядка и Технических условий установки и эксплуатации средств, предназначенных для поиска признаков компьютерных атак в сетях электросвязи, используемых для организации взаимодействия объектов критической информационной инфраструктуры Российской Федерации» (зарегистрирован в Минюсте России 25 июня 2020 N° 58753). Опубликован 25 июня 2020.

Приказ Минцифры РФ от 28 декабря 2020 N° 777 «Об утверждении Рекомендаций по проведению сертификации оборудования связи, используемого в составе сети связи общего пользования, обеспечивающей функционирование значимых объектов критической информационной инфраструктуры» (ДСП).

Приказ Минцифры РФ от 28 декабря 2020 N° 779 «Об утверждении организационно-технических мер по обеспечению информационной безопасности ресурсов сети связи общего пользования, используемых значимыми объектами критической информационной инфраструктуры» (ДСП).

Рекомендации

Согласованы со ФСТЭК и ФСБ России

Методические рекомендации от 26 июня 2019 по категорированию объектов критической информационной инфраструктуры, принадлежащих субъектам критической информационной инфраструктуры, функционирующим в сфере связи. Введены в действие для опытного использования в тестовом режиме решением исполкома общественно-государственного объединения «Ассоциация документальной электросвязи». Согласованы:

— 8 Центр ФСБ России (исх. N° 149/2/7- 370 от 5 апреля 2019)

— Общественно-государственное объединение «Ассоциация документальной электросвязи» (протокол от 27 марта 2019)

— ФСТЭК России (исх. N° 240/25/1221 от 18 марта 2019)

Методические рекомендации Минэнерго России по определению и категорированию объектов критической информационной инфраструктуры топливно-энергетического комплекса. Опубликованы 1 сентября 2019. Согласованы Минэнерго и ФСТЭК России.

8 Центр ФСБ России. N°149/2/7-200 от 24 декабря 2016 «Методические рекомендации по созданию ведомственных и корпоративных центров государственной системы обнаружения, предупреждения и ликвидации последствий компьютерных атак на информационные ресурсы Российской Федерации» (по запросу).

8 Центр ФСБ России. «Временный порядок включения корпоративных центров в государственную систему обнаружения, предупреждения и ликвидации последствий компьютерных атак на информационные ресурсы Российской Федерации».

Бизнес-центр «Верейская плаза III»
121357, Москва, Верейская улица, 29, стр. 134

+7 495 22 900 22, +7 499 37 251 74
sales@infowatch.ru

infowatch.ru /InfoWatchOut /InfoWatch