

Нормативно-правовые акты,
организационные и методические
документы по обеспечению
безопасности критической
информационной инфраструктуры
Российской Федерации



Оглавление

[Федеральные законы](#)

[Указы Президента Российской Федерации](#)

[Постановления Правительства Российской Федерации](#)

[Приказы и сообщения Федеральной службы по техническому и экспортному контролю](#)

[Приказы Федеральной службы безопасности Российской Федерации](#)

[Приказы Минцифры России](#)

[Рекомендации](#)

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 № 5485-1 «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)
- **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)
- **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

Настоящий Федеральный закон [вступает в силу](#) по истечении десяти дней после дня его официального опубликования, за исключением абзацев третьего и четвертого пункта 2 статьи 1 настоящего Федерального закона. Абзацы третий и четвертый пункта 2 статьи 1 настоящего Федерального закона вступают в силу с 1 сентября 2021 (часть 1 статьи 13.12.1).

Указы Президента Российской Федерации

- **Указ Президента Российской Федерации 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 с 15 января 2013](#)
- **Указ Президента Российской Федерации № К 1274 от 12 декабря 2014** «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
- **Указ Президента Российской Федерации 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 Российской Федерации 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 Российской Федерации от 2 марта 2018 № 98** «[О внесении изменения](#) в перечень сведений, отнесенных к государственной тайне, утвержденный Указом Президента Российской Федерации от 30 ноября 1995 № 1203»

Постановления Правительства Российской Федерации

- **Постановление Правительства Российской Федерации 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 Российской Федерации от 13 апреля 2019 № 452** «О внесении изменений в постановление Правительства Российской Федерации от 8 февраля 2018 № 127». [Опубликовано 16 апреля 2019](#)
- **Постановление Правительства Российской Федерации 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 Российской Федерации 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» ([pravo.gov.ru](#), [cntd.ru](#))
- **Постановление Правительства Российской Федерации № 808 от 11 июля 2018** «[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»
- **Постановление Правительства Российской Федерации 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»

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). Опубликовано 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). Опубликовано 28 декабря 2017 (fstec.ru, pravo.gov.ru)
- **Приказ ФСТЭК России от 21 декабря 2017 № 235** (ред. от 13 июня 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](#)
- **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](#)
- **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 № 9793). [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 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 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 России 18 мая 2018 № 51127). [Вступил в силу 1 июня 2018](#)

- **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)

- **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» (зарегистрировано в Минюсте России 11 сентября 2020)
 - ФСТЭК России. [Информационное сообщение](#). «Об утверждении требований по безопасности информации, устанавливающих уровни доверия к средствам технической защиты информации и средствам обеспечения безопасности информационных технологий от 15 октября 2020 № 240/24/4268

- [Выписка из Требований](#) по безопасности информации, утверждённых приказом ФСТЭК России от 2 июня 2020 № 76
- Приказ 76-2020 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. Частично 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
- **ФСТЭК России. 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) «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)
- **ФСТЭК России. Информационное сообщение.** 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 [от 17 апреля 2020 № 240/84/611](#)
- **ФСТЭК России. Рекомендации** по обеспечению безопасности объектов критической информационной инфраструктуры при реализации дистанционного режима исполнения должностных обязанностей работниками субъектов критической информационной инфраструктуры. Письмо ФСТЭК России от [20 марта 2020 № 240/84/389](#)
- **ФСТЭК России. Информационное сообщение.** О методических документах по вопросам обеспечения безопасности информации в ключевых системах информационной инфраструктуры Российской Федерации [от 4 мая 2018 № 240/22/2339](#)
- **ФСТЭК России. Информационное сообщение.** 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 редакции от 28 февраля 2018) от 28 февраля 2018 № 240/11/879

Приказы Федеральной службы безопасности Российской Федерации

- **ФСТЭК России. Информационное сообщение.** 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](#)
- **Приказ Федеральной службы безопасности Российской Федерации от 24 июля 2018 № 366** «О Национальном координационном центре по компьютерным инцидентам» (зарегистрировано в Минюсте России 6 сентября 2018 № 52109). [Опубликован 10 сентября 2018](#)
- **Приказ Федеральной службы безопасности Российской Федерации 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» (зарегистрировано в Минюсте России 6 сентября 2018 № 52108). [Опубликован 10 сентября 2018](#)
- **Приказ Федеральной службы безопасности Российской Федерации 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, 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» (зарегистрировано в Минюсте России 6 сентября 2018 № 52107). [Опубликован 10 сентября 2018](#)
- **Приказ Федеральной службы безопасности Российской Федерации от 6 мая 2019 № 196** «Об утверждении требований к средствам, предназначенным для обнаружения, предупреждения и ликвидации последствий компьютерных атак и реагирования на компьютерные инциденты» (зарегистрировано в Минюсте России 31 мая 2019 № 54801). [Опубликован 31 мая 2019](#)

- **Приказ Федеральной службы безопасности Российской Федерации 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» (зарегистрировано в Минюсте России 16 июля 2019 № 55285). [Опубликован 17 июля 2019](#)
- **Приказ Федеральной службы безопасности Российской Федерации от 19 июня 2019 № 282** «Об утверждении Порядка информирования ФСБ России о компьютерных инцидентах, реагирования на них, принятия мер по ликвидации последствий компьютерных атак, проведенных в отношении значимых объектов критической информационной инфраструктуры Российской Федерации» (зарегистрировано в Минюсте России 16 июля 2019 № 55284). [Опубликован 17 июля 2019](#)

Приказы Минцифры России

- **Приказ Министерства цифрового развития, связи и массовых коммуникаций Российской Федерации от 17 марта 2020 № 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» (зарегистрировано в Минюсте России 25 июня 2020 № 58753). [Опубликован 25 июня 2020](#)
- **Приказ Министерства цифрового развития, связи и массовых коммуникаций Российской Федерации от 28 декабря 2020 № 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 Министерства цифрового развития, связи и массовых коммуникаций Российской Федерации от 28 декабря 2020 № 779** «Об утверждении организационно-технических мер по обеспечению информационной безопасности ресурсов сети связи общего пользования, используемых значимыми объектами критической информационной инфраструктуры» (ДСП)

Рекомендации

Приведены рекомендации, согласованные со ФСТЭК России и ФСБ России

- **Методические рекомендации 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 Общественного государственного объединения «Ассоциация документальной электросвязи» от 26 июня 2019
 - [Согласовано](#). 8 Центр ФСБ России (исх. № 149/2/7-370 от 5 апреля 2019). Общественно-государственное объединение «Ассоциация документальной электросвязи» (протокол от 27 марта 2019). ФСТЭК России (исх. № 240/25/1221 от 18 марта 2019)
- **Минэнерго России.** Методические рекомендации по определению и категорированию объектов критической информационной инфраструктуры топливно-энергетического комплекса. Опубликовано 1 сентября 2019
 - [Согласовано](#). Минэнерго России, ФСТЭК России
- **8 Центр ФСБ России. Рекомендации № 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»