

Система
нормативных правовых, методических и информационных документов по проблематике обеспечения безопасности критической информационной инфраструктуры Российской Федерации
 (версия по состоянию на 31.03.2022)

Основы государственной политики Российской Федерации в области международной информационной безопасности на период до 2020 года, утверждены Президентом Российской Федерации 24.07.2013 № Пр-1753	Указ Президента Российской Федерации от 15.01.2013 № 31с «О создании Государственной системы обнаружения, предупреждения и ликвидации последствий компьютерных атак на информационные ресурсы Российской Федерации»
Основные направления государственной политики в области обеспечения безопасности автоматизированных систем управления производственными и технологическими процессами критически важных объектов инфраструктуры Российской Федерации, утвержденные Президентом Российской Федерации 03.02.2012 г. № 803	Выписка из Концепции государственной системы обнаружения, предупреждения и ликвидации последствий компьютерных атак на информационные ресурсы Российской Федерации, утвержденной Президентом Российской Федерации 12.12.2014 № К 1274
Указ Президента Российской Федерации от 09.05.2017 г. № 203 «О Стратегии развития информационного общества в Российской Федерации на 2017 – 2030 годы»	План развертывания ведомственных сегментов государственной системы обнаружения, предупреждения и ликвидации последствий компьютерных атак, утвержденный Президентом Российской Федерации 21.08.2015 № 9397*
Указ Президента Российской Федерации от 05.01.2016 № 646 «Об утверждении Доктрины информационной безопасности Российской Федерации»	Постановление Правительства Российской Федерации от 24 мая 2010 № 365 «О координации мероприятий по использованию информационно-коммуникационных технологий в деятельности государственных органов» Постановление Правительства Российской Федерации от 6 июля 2017 г. № 803 «О внесении изменений в постановление Правительства Российской Федерации от 24 мая 2010 г. № 365»

Федеральный закон от 26.07.2017 № 187-ФЗ
«О безопасности критической информационной инфраструктуры Российской Федерации»

Федеральный закон от 26.07.2017 № 193-ФЗ «О внесении изменений в отдельные законодательные акты Российской Федерации в связи с принятием Федерального закона «О безопасности критической информационной инфраструктуры Российской Федерации»	Федеральный закон от 26.07.2017 № 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»
--	---

Федеральный закон от 26.05.2021 № 141-ФЗ "О внесении изменений в Кодекс Российской Федерации об административных правонарушениях"

Указ Президента Российской Федерации от 25.11.2017 № 569 «О внесении изменений в Положение о Федеральной службе по техническому и экспортному контролю, утвержденное Указом Президента Российской Федерации от 16 августа 2004 г. № 1085»	Указ Президента Российской Федерации от 22.12.2017 № 620 «О совершенствовании Государственной системы обнаружения, предупреждения и ликвидации последствий компьютерных атак на информационные ресурсы Российской Федерации»
Указ Президента Российской Федерации от 02.03.2018 № 98 «О внесении изменения в перечень сведений, отнесенных к государственной тайне, утвержденный Указом Президента Российской Федерации от 30 ноября 1995 г. № 1203»	Указ Президента Российской Федерации от 27.02.2018 № 89 «О внесении изменений в Положение о Федеральной службе охраны Российской Федерации, утвержденное Указом Президента Российской Федерации от 7 августа 2004 г. № 1013»
Постановление Правительства Российской Федерации от 21.12.2019 № 1746 «Об установлении запрета на допуск отдельных видов товаров, происходящих из иностранных государств, и внесении изменений в некоторые акты Правительства Российской Федерации»	Указ Президента Российской Федерации от 30.03.2022 № 166 «О мерах по обеспечению технологической независимости и безопасности критической информационной инфраструктуры Российской Федерации»
Постановление Правительства Российской Федерации от 08.02.2018 № 127 «Об утверждении Правил категорирования объектов критической информационной инфраструктуры Российской Федерации, а также перечня показателей критериев значимости объектов критической информационной инфраструктуры Российской Федерации»	Постановление Правительства Российской Федерации от 17.02.2018 № 162 «Об утверждении Правил осуществления государственного контроля в области обеспечения безопасности значимых объектов критической информационной инфраструктуры Российской Федерации»
Постановление Правительства Российской Федерации от 13 апреля 2019 г. № 452 «О внесении изменений в постановление Правительства Российской Федерации от 8 февраля 2018 г. № 127».	Постановление Правительства Российской Федерации от 08.06.2019 № 743 «Об утверждении Правил подготовки и использования ресурсов единой сети электросвязи Российской Федерации для обеспечения безопасности значимых объектов критической информационной инфраструктуры»
Постановление Правительства Российской Федерации от 24 декабря 2021 г. № 2431 «О внесении изменений в Правила категорирования объектов критической информационной инфраструктуры Российской Федерации».	

Приказ ФСБ России от 24.07.2018 № 366 «О Национальном координационном центре по компьютерным инцидентам»

Приказ ФСТЭК России от 06.12.2017 № 227 «Об утверждении Порядка ведения реестра значимых объектов критической информационной инфраструктуры Российской Федерации»	Приказ ФСБ России от 24.07.2018 № 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»
Приказ ФСТЭК России от 11.12.2017 № 229 «Об утверждении формы акта проверки, составляемого по итогам проведения государственного контроля в области обеспечения безопасности значимых объектов критической информационной инфраструктуры Российской Федерации»	Приказ ФСБ России от 24.07.2018 № 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»

Приказ ФСТЭК России от 21.12.2017 № 235 «Об утверждении Требований к созданию систем безопасности значимых объектов критической информационной инфраструктуры Российской Федерации и обеспечению их функционирования»

Приказ ФСТЭК России от 27.03.2019 № 64 «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»	Приказ ФСБ России от 06.05.2019 № 196 «Об утверждении требований к средствам, предназначенным для обнаружения, предупреждения и ликвидации последствий компьютерных атак и реагирования на компьютерные инциденты»
---	--

Приказ ФСТЭК России от 22.12.2017 № 236 «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»

Приказ ФСТЭК России от 21 марта 2019 г. № 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»	Приказ ФСБ России от 19.06.2019 № 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»
---	---

Приказ ФСТЭК России от 25.12.2017 № 239 «Об утверждении Требований по обеспечению безопасности значимых объектов критической информационной инфраструктуры Российской Федерации»

Приказ ФСТЭК России от 09 августа 2018 г. № 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, утвержденные приказом Федеральной службы по техническому и экспортному контролю от 14 марта 2014 г. № 31, и 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»	Приказ ФСБ России от 19.06.2019 № 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»
--	---

Приказ ФСТЭК России от 26 марта 2019 г. № 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»

Приказ ФСТЭК России от 20.02.2020 № 35 «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»	Приказ Минкомсвязи России от 17.03.2020 № 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»
--	---

Приказ ФСТЭК России от 28.05.2020 № 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»

Расширенный перечень сведений, подлежащих засекречиванию, ФСТЭК России* (в части раскрытия и конкретизации пункта 119 Перечня сведений, отнесенных к государственной тайне, утвержденного Указом Президента Российской Федерации от 30 ноября 1995 г. № 1203)	Приказ Минцифры России от 28.12.2020 № 777 «Об утверждении Рекомендаций по проведению сертификации оборудования связи, используемого в составе сетей связи общего пользования, обеспечивающей функционирование значимых объектов критической информационной инфраструктуры»*
---	--

Приказ ФСТЭК России от 18 апреля 2021 г. № 77 «Об утверждении Порядка организации и проведения работ по аттестации объектов информатизации на соответствие требованиям о защите информации ограниченного доступа, не составляющей государственную тайну»

Информационное сообщение ФСТЭК России о Требованиях по безопасности информации, устанавливающих уровни доверия к средствам технической защиты информации и средствам обеспечения безопасности информационных технологий от 29.03.2019 № 240/24/1525	Приказ Минцифры России от 28.12.2020 № 779 «Об утверждении организационно-технических мер по обеспечению информационной безопасности ресурсов сети связи общего пользования, используемых значимыми объектами критической информационной инфраструктуры»*
---	---

Информационное сообщение ФСТЭК России о методических документах по вопросам обеспечения безопасности информации в ключевых системах информационной инфраструктуры Российской Федерации от 4.05.2018 № 240/22/2339

Информационное сообщение ФСТЭК России 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 24.08.2018 № 240/25/3752 (фактически утратило силу)	Требования к подразделениям и должностным лицам субъекта ГосСОПКА*
--	--

Информационное сообщение ФСТЭК России о разработанной ФСТЭК России примерной программе повышения квалификации специалистов, работающих в области обеспечения безопасности значимых объектов критической информационной инфраструктуры от 17.12.2018 № 240/11/5453

Перечень нормативных правовых актов или отдельных их частей, оценка соблюдения которых является предметом государственного контроля (надзора) в области обеспечения безопасности значимых объектов критической информационной инфраструктуры Российской Федерации, утвержденный приказом ФСТЭК России от 16.07.2019 № 135	Регламент информационного взаимодействия
---	--

Рекомендации по обеспечению безопасности объектов критической информационной инфраструктуры при реализации дистанционного режима исполнения должностных обязанностей работниками субъектов критической информационной инфраструктуры (письмо ФСТЭК России от 20.03.2020 № 240/84/389)

Информационное сообщение ФСТЭК России от 17.04.2020 № 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	Методические рекомендации по обнаружению компьютерных атак на информационные ресурсы*
--	---

Субсидирование

Постановление Правительства Российской Федерации от 07.10.2019 № 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» (в ред. постановлений Правительства от 28.09.2020 № 1556 и от 26.01.2021 № 50)	Методические рекомендации по установлению причин и ликвидации последствий компьютерных атак*
Приказ Минкомсвязи от 30.10.2019 № 629 «О конкурсной комиссии Министерства цифрового развития, связи и массовых коммуникаций Российской Федерации по предоставлению Министерством цифрового развития, связи и массовых коммуникаций Российской Федерации 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»	Методические рекомендации по проведению мероприятий по оценке защищенности от компьютерных атак

Дополнительные документы

Методические рекомендации по категорированию объектов критической информационной инфраструктуры, принадлежащих субъектам критической информационной инфраструктуры, функционирующим в сфере связи, согласованные 8 Центром ФСБ России и ФСТЭК России**	Варианты организации защищенного канала
Методические рекомендации «Категорирование объектов критической информационной инфраструктуры», разработанные ООО «СТЭП ЛЮДЖИК»****	Методические рекомендации по созданию ведомственных и корпоративных центров государственной системы обнаружения, предупреждения и ликвидации последствий компьютерных атак на информационные ресурсы Российской Федерации, от 24.12.2016 № 149/2/7-200
Методические рекомендации по категорированию объектов критической информационной инфраструктуры сферы здравоохранения *****	Временный порядок включения корпоративных центров в ГосСОПКА

* - Документы, имеющие ограничительные пометки
 ** - Внимание, данные рекомендации не учитывают постановление Правительства Российской Федерации от 13 апреля 2019 г. № 452 «О внесении изменений в постановление Правительства Российской Федерации от 8 февраля 2018 г. № 127» и приказ ФСТЭК России от 21 марта 2019 г. № 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://www.rans.ru/images/metec_KII.pdf).
 *** - Внимание, данные рекомендации не в полной мере учитывают постановление Правительства Российской Федерации от 13 апреля 2019 г. № 452 (<https://minenergo.gov.ru/view-pdf/11357/102517>).
 **** - <https://step.ru/upload/iblock/878/87877a75035badbaed3ab8f792ea0ca5.pdf>
 ***** - http://aciso.ru/files/docs/metodichka_2_0.pdf
 ***** - <https://minzdrav.gov.ru/documents/9646-metodicheskie-rekomendatsii-po-kategorirovaniyu-ob-ektov-kriticheskoy-informatsionnoy-infrastruktury-sfery-zdravoohraneniya>