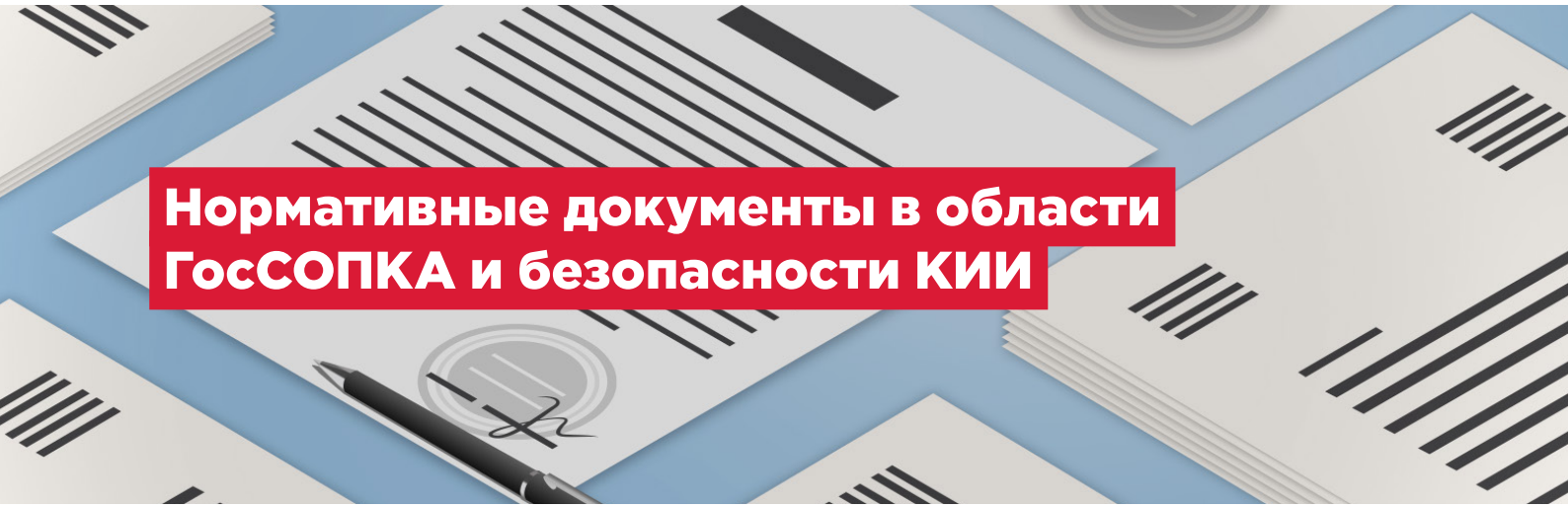

Нормативные документы в области ГосСОПКА и безопасности КИИ

Что такое КИИ

Согласно закону № 187-ФЗ, к **объектам критической информационной инфраструктуры** относятся информационные системы, информационно-телекоммуникационные сети, автоматизированные системы управления субъектов критической информационной инфраструктуры в одной из следующих сфер: здравоохранение, наука, транспорт, связь, энергетика, банки и иные организации финансового рынка, топливно-энергетический комплекс, атомная энергия, оборона, ракетно-космическая, горнодобывающая, металлургическая и химическая промышленности.

Подмножеством всех объектов КИИ являются **значимые объекты КИИ** — те объекты, которым присвоена одна из категорий значимости в результате категорирования.

К **субъектам КИИ** относятся владельцы объектов КИИ, а также организации, которые обеспечивают их взаимодействие.

НПА в сфере защиты КИИ

Федеральные законы

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

Определяет основные принципы обеспечения безопасности, полномочия госорганов, а также права, обязанности и ответственность субъектов КИИ. Предусмотрены категорирование объектов, ведение реестра значимых объектов, оценка состояния защищенности, госконтроль, создание специальных систем безопасности.

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"»

Дополняет Уголовный кодекс статьей 274.1, которая предусматривает наказания за неправомерное воздействие на КИИ РФ.

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"»

Вносит изменения в федеральные законы о государственной тайне, связи и защите прав юридических лиц и ИП при осуществлении государственного контроля (надзора).

Акты Президента РФ

Указ Президента Российской Федерации от 25.11.2017 № 569 «О внесении изменений в Положение о Федеральной службе по техническому и экспортному контролю...»

Наделяет ФСТЭК России полномочиями в области обеспечения безопасности КИИ, в том числе функцией государственного контроля.

Указ Президента РФ от 02.03.2018 № 98 «О внесении изменения в перечень сведений, отнесенных к государственной тайне...»

Относит к гостайне информацию о мерах обеспечения безопасности КИИ и о состоянии ее защищенности от атак. ФСБ России и ФСТЭК России назначены государственными органами, наделенными полномочиями по распоряжению сведениями, отнесенными к государственной тайне.

Акты Правительства РФ

Постановление Правительства РФ 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 РФ и их значений»

Устанавливает порядок и сроки категорирования объектов КИИ.

Постановление Правительства РФ от 17.02.2018 № 162 «Об утверждении Правил осуществления государственного контроля в области обеспечения безопасности значимых объектов критической информационной инфраструктуры Российской Федерации»

Определяет правила проведения плановых и внеплановых проверок в области обеспечения безопасности значимых объектов КИИ.

Проект постановления Правительства РФ «Об утверждении порядка подготовки и использования ресурсов единой сети электросвязи Российской Федерации для обеспечения функционирования значимых объектов критической информационной инфраструктуры» (подготовлен Минкомсвязью России 17 ноября 2017 г.)

Устанавливает три категории сетей электросвязи, ресурсы которых используются для обеспечения функционирования значимых объектов КИИ. Определяет, что́ должно быть предусмотрено в договоре (госконтракте) субъекта КИИ с оператором связи о подготовке и использовании ресурсов сети электросвязи.

Ведомственные акты

Приказ ФСТЭК России от 06.12.2017 № 227 «Об утверждении Порядка ведения реестра значимых объектов критической информационной инфраструктуры Российской Федерации»

Определяет сведения о значимом объекте КИИ, необходимые для внесения в реестр. Решение о включении в реестр принимается в течение 30 дней со дня получения ФСТЭК России сведений от субъекта КИИ. Не реже чем один раз в месяц ФСТЭК России направляет сведения из реестра в ГосСОПКА.

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»

Определяет форму акта по итогам проверки значимого субъекта КИИ.

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»

Устанавливает требования к силам обеспечения безопасности значимых объектов, программным и программно-аппаратным средствам, документам по безопасности значимых объектов, функционированию системы безопасности.

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»

Определяет набор сведений о результатах присвоения объекту КИИ категории значимости, который необходимо направить во ФСТЭК России. Сведения сгруппированы в девять разделов.

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

Устанавливает требования к обеспечению безопасности значимых объектов КИИ в ходе создания, эксплуатации и вывода их из эксплуатации, к организационным и техническим мерам защиты информации и определяет состав мер для каждой категории значимости объекта.

Приказ ФСТЭК России от 26.04.2018 № 72 «О внесении изменений в Регламент Федеральной службы по техническому и экспортному контролю, утвержденный приказом ФСТЭК России от 12 мая 2005 г. № 167»

Относит обеспечение безопасности значимых объектов КИИ к нормативно-правовому регулированию вопросов ФСТЭК России. Слова «информации в ключевых системах» заменяет словом «критической».

Проект приказа ФСТЭК России «О внесении изменений в Требования к обеспечению защиты информации в автоматизированных системах управления производственными и технологическими процессами на критически важных объектах, потенциально опасных объектах...»

Определяет список изменений в приказы № 31 и 239. Состав мер защиты информации и их базовые наборы по классу защищенности АСУ изложены в новой редакции.

Информационные сообщения

Информационное сообщение ФСТЭК России от 24.08.2018 № 240/25/3752 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

Регулятор приводит рекомендуемую форму перечня объектов КИИ для ее подачи во ФСТЭК России. Рекомендуется прикладывать электронную копию перечня и сведений о результатах категорирования.

Что такое ГосСОПКА

ГосСОПКА — государственная система обнаружения, предупреждения и ликвидации последствий компьютерных атак, направленных на информационные ресурсы Российской Федерации.

Цель системы — объединить усилия для предотвращения и противодействия кибератакам на критически важные информационные инфраструктуры. Для этого создан **Национальный координационный центр по компьютерным инцидентам** (НКЦКИ), который организует сбор и обмен информацией об инцидентах между субъектами КИИ, координирует мероприятия по реагированию, предоставляет методические рекомендации по предупреждению компьютерных атак.

НПА в сфере ГосСОПКА

Акты Президента РФ

Основные направления государственной политики в области обеспечения безопасности автоматизированных систем управления производственными и технологическими процессами критически важных объектов инфраструктуры Российской Федерации (Утверждены Президентом РФ 3 февраля 2012 г., № 803)

Документ вводит понятие единой государственной системы обнаружения и предупреждения компьютерных атак на критически важную информационную инфраструктуру. Дает определение силам и средствам обнаружения и предупреждения атак, а также силам и средствам ликвидации последствий инцидентов.

Указ Президента РФ от 15.01.2013 № 31с «О создании государственной системы обнаружения, предупреждения и ликвидации последствий компьютерных атак на информационные ресурсы Российской Федерации»

Инициирует создание ГосСОПКА, определяет основные задачи системы. На ФСБ России возлагает полномочия по созданию и обеспечению функционирования ГосСОПКА.

Концепция государственной системы обнаружения, предупреждения и ликвидации последствий компьютерных атак на информационные ресурсы Российской Федерации, утвержденная Президентом РФ 12 декабря 2014 г. № К 1274

Определяет назначение, функции и принципы создания ГосСОПКА, а также виды обеспечения, необходимые для ее создания и функционирования.

План развертывания ведомственных сегментов государственной системы обнаружения, предупреждения и ликвидации последствий компьютерных атак, утвержденный Президентом РФ 21 августа 2015 г., № 9397 (документ ограниченного доступа)

Определяет перечень органов государственной власти, которым необходимо создать ведомственные сегменты ГосСОПКА, и указывает сроки.

Указ Президента РФ от 22.12.2017 № 620 «О совершенствовании государственной системы обнаружения, предупреждения и ликвидации последствий компьютерных атак на информационные ресурсы Российской Федерации»

Определяет задачи ГосСОПКА и ФСБ России в сфере обеспечения функционирования системы.

Ведомственные акты

Методические рекомендации по созданию ведомственных и корпоративных центров государственной системы обнаружения, предупреждения и ликвидации последствий компьютерных атак на информационные ресурсы Российской Федерации от 27.12.2016 (документ ограниченного доступа)

Документ детализирует порядок создания ведомственных и корпоративных центров ГосСОПКА, их функции, а также технические и организационные меры защиты информации.

«Временный порядок включения корпоративных центров в государственную систему обнаружения, предупреждения и ликвидации последствий компьютерных атак...» (документ ограниченного доступа)

Определяет состав документов и уровень квалификации специалистов группы реагирования, необходимые для подключения к ГосСОПКА.

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

Инициирует создание Национального координационного центра по компьютерным инцидентам, определяет его задачи и права.

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...»

Устанавливает набор параметров инцидентов для передачи в НКЦКИ (не позднее 24 часов с момента их обнаружения) и способы передачи информации.

Приказ ФСБ России от 24.07.2018 № 368 «Об утверждении Порядка обмена информацией о компьютерных инцидентах между субъектами критической информационной инфраструктуры Российской Федерации...»

Определяет способы передачи информации об инциденте другим субъектам КИИ и получения сведений субъектами КИИ об атаках. Обмен информацией с иностранными организациями осуществляет НКЦКИ.

Методические рекомендации по обнаружению компьютерных атак на информационные ресурсы Российской Федерации (документ ограниченного доступа)

Определяют порядок действий по обнаружению атак, классифицируют атаки и дают рекомендации по повышению уровня защищенности объектов атаки.

Методические рекомендации по установлению причин и ликвидации последствий компьютерных инцидентов, связанных с функционированием информационных ресурсов Российской Федерации (документ ограниченного доступа)

Определяют порядок и основные задачи при реагировании на инциденты. Устанавливают классы инцидентов.

Методические рекомендации по проведению мероприятий по оценке степени защищенности от компьютерных атак

Определяют основные задачи, порядок и этапы проведения мероприятий по оценке степени защищенности. Устанавливают порядок оценки возможностей злоумышленника при атаках.

Требования к подразделениям и должностным лицам субъектов государственной системы обнаружения, предупреждения и ликвидации последствий компьютерных атак на информационные ресурсы Российской Федерации (документ ограниченного доступа)

Документ определяет основные задачи подразделений и должностных лиц субъекта ГосСОПКА, требования к кадровому обеспечению и деятельности центров ГосСОПКА. Распределяет роли сотрудников центра ГосСОПКА по трем линиям реагирования. Выделяет три класса центров ГосСОПКА в зависимости от объема функций, выполняемых центром самостоятельно.

Регламент взаимодействия подразделений Федеральной службы безопасности Российской Федерации и организации при осуществлении информационного обмена в области обнаружения, предупреждения и ликвидации последствий компьютерных атак

Определяет режимы и порядок взаимодействия подразделений ФСБ России с другими организациями. Устанавливает функции подразделений, формы информационного взаимодействия, типы передаваемых сообщений и их виды.

Проект приказа ФСБ России «Об утверждении Требований к средствам, предназначенным для обнаружения, предупреждения и ликвидации последствий компьютерных атак и реагирования на компьютерные инциденты»

Определяет требования к функциональным возможностям и характеристикам технических средств, необходимых для решения задач центров ГосСОПКА.

Проект приказа ФСБ России «Об утверждении порядка, технических условий установки и эксплуатации средств, предназначенных для обнаружения, предупреждения и ликвидации последствий компьютерных атак и реагирования на компьютерные инциденты...»

Обязывает субъекта КИИ согласовывать с НКЦКИ установку средств ГосСОПКА и уведомлять о приеме их в эксплуатацию. Определяет необходимые для согласования сведения. Срок согласования — до 45 календарных дней.

Проект приказа ФСБ России «Об утверждении Порядка информирования ФСБ России о компьютерных инцидентах, реагирования на них, принятия мер по ликвидации последствий компьютерных атак...»

Определяет состав плана реагирования на инциденты и принятия мер по ликвидации последствий, разрабатываемого субъектом КИИ. Обязует информировать НКЦКИ о результатах реагирования и ликвидации последствий не позднее 48 часов после завершения мероприятий.

Проект приказа Минкомсвязи России «Об утверждении порядка, технических условий установки и эксплуатации средств, предназначенных для поиска признаков компьютерных атак в сетях электросвязи, используемых для организации взаимодействия объектов критической информационной инфраструктуры»

Определяет единый подход к установке и эксплуатации средств, предназначенных для поиска признаков атак в сетях электросвязи. Описывает порядок установки и эксплуатации средства поиска атак. Информация о необходимости установки средства поиска атак направляется в уполномоченный орган в области связи.