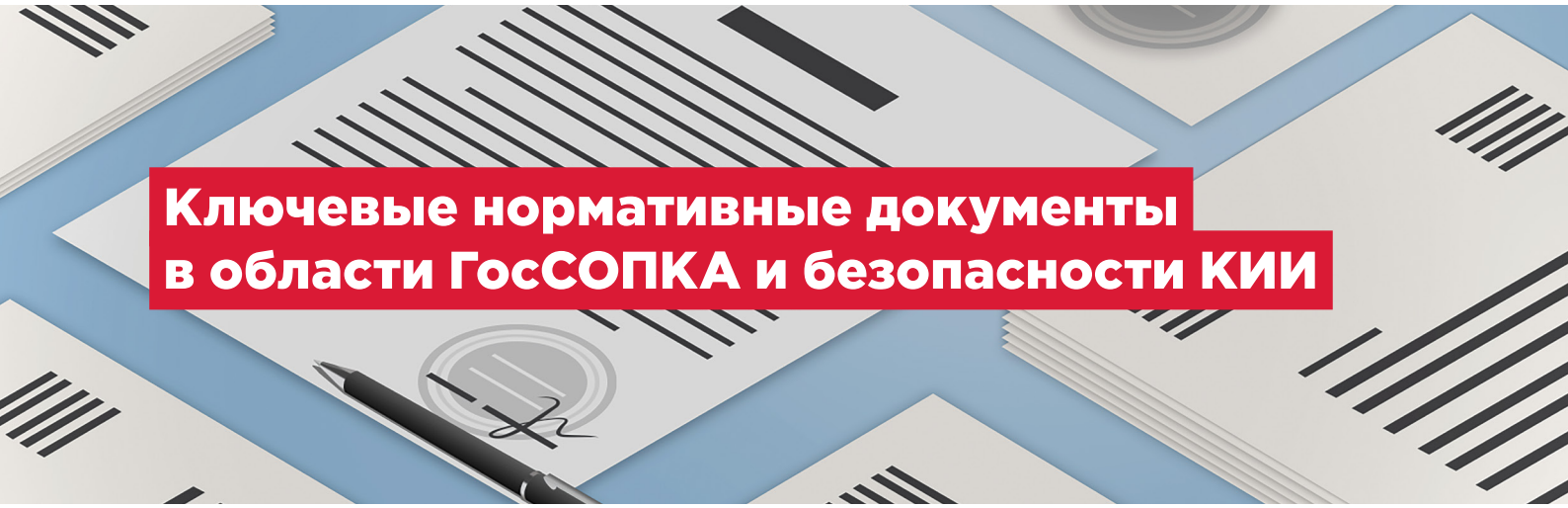
POSITIVE TECHNOLOGIES



Ключевые 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.

Ключевые НПА в сфере защиты КИИ

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.

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.

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 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.

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.

Ключевые НПА в сфере ГосСОПКА

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.

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.

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.

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»

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

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...»

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.

Полный список нормативных документов в области ГосСОПКА и безопасности КИИ вы можете скачать на сайте Positive Technologies

О компании

ptsecurity.com
pt@ptsecurity.com

facebook.com/PositiveTechnologies
facebook.com/PHDays

Positive Technologies — один из лидеров европейского рынка систем анализа защищенности и соответствия стандартам, а также защиты веб-приложений. Организации во многих странах мира используют решения Positive Technologies для оценки уровня безопасности своих сетей и приложений, для выполнения требований регулирующих организаций и блокирования атак в режиме реального времени. Благодаря многолетним исследованиям специалисты Positive Technologies заслужили репутацию экспертов международного уровня в вопросах защиты SCADA- и ERP-систем, крупнейших банков и телеком-операторов.

Деятельность компании лицензирована Минобороны России, ФСБ России и ФСТЭК России, продукция сертифицирована Минобороны России и ФСТЭК России.

Terminology_SV_A4.RUS.0015.11.JUL.23.2019