



Основные изменения в нормативной правовой базе ФСБ России в сфере ГосСОПКА

Иван Пыхтин



НАЦИОНАЛЬНЫЙ КООРДИНАЦИОННЫЙ ЦЕНТР
ПО КОМПЬЮТЕРНЫМ ИНЦИДЕНТАМ



Внесенные изменения:

- обязывают субъектов КИИ взаимодействовать с ГосСОПКА и информировать НКЦКИ о компьютерных атаках
- обязывают субъектов, имеющих значимые объекты КИИ, использовать российское ПО и соответствующие требованиям программно-аппаратные средства
- расширяют полномочия ФСБ России

Расширение круга субъектов ГосСОПКА



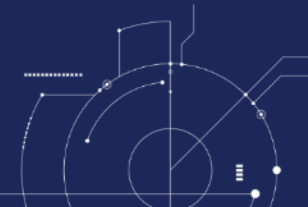
Внесённые изменения распространяют действие Федерального закона № 187-ФЗ на руководителей следующих органов и организаций:

- государственных органов (за исключением ФСБ России, СВР России, ФСО России, ГУСПа, ФСТЭК России)
- государственных унитарных предприятий
- государственных учреждений
- государственных фондов
- государственных корпораций (компаний)
- российских юридических лиц, которые, находятся под контролем РФ, и (или) субъекта РФ, и (или) контролируемых ими совместно или по отдельности

Издано 7 приказов ФСБ России



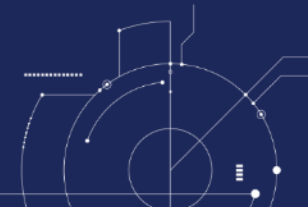
- Об утверждении порядка получения субъектами КИИ информации о средствах и способах проведения КА и о методах их предупреждения и обнаружения
- О внесении изменений в Положение о НКЦКИ
- Об утверждении порядка обмена информацией о КА и КИ
- Об установлении требований к средствам ГосСОПКА
- Об утверждении порядка информирования ФСБ России о КА и КИ, принятия мер по ликвидации последствий КА в отношении 30 КИИ
- Об утверждении порядка осуществления непрерывного взаимодействия субъектов КИИ с ГосСОПКА
- Об утверждении порядка и технических условий установки и эксплуатации средств ГосСОПКА



«О внесении изменений в Положение о Национальном координационном центре по компьютерным инцидентам, утвержденное приказом ФСБ России от 24 июля 2018 г. № 366»

Ключевые изменения:

- теперь НКЦКИ осуществляет координацию деятельности не только субъектов КИИ, но и аккредитованных центров ГосСОПКА, а также органов и организаций, установленных 58-ФЗ
- НКЦКИ наделяется правом от своего имени заключать соглашения о научно-техническом сотрудничестве, разрабатывать и заключать регламенты взаимодействия
- НКЦКИ наделяется правом запрашивать у субъектов КИИ, центров ГосСОПКА, и органов (организаций) результаты проведенных мероприятий, направленных на защиту от КА в отношении принадлежащих им информационных ресурсов, а также информацию об устранении уязвимостей



«Об утверждении Порядка обмена информацией о КА и КИ между субъектами КИИ РФ, между субъектами КИИ РФ и уполномоченными органами иностранных государств, международными, международными неправительственными организациями и иностранными организациями, осуществляющими деятельность в области реагирования на КИ»

Утратил силу: приказ ФСБ России от 24.07.2018 № 368

Ключевые изменения:

- новым приказом регулируется не только порядок обмена о КИ, но и о КА
- время информирования НКЦКИ субъекта КИИ при получении сведений от иностранной (международной) организации увеличено с 12 часов до 48 часов
- установлена обязанность субъектов КИИ при получении информации о КА и КИ, связанных с функционированием объекта КИИ другого субъекта КИИ, информировать НКЦКИ не позднее 12 часов с момента получения такой информации



«Об утверждении Порядка получения субъектами КИИ РФ информации о средствах и способах проведения компьютерных атак и о методах их предупреждения и обнаружения»

Субъекты КИИ обязаны получать информацию путём:

- обращения к официальному сайту cert.gov.ru
- направления запросов в НКЦКИ с использованием технической инфраструктуры НКЦКИ либо посредством почтовой или электронной связи на адреса, указанные на сайте cert.gov.ru

! срок ответа на запрос увеличен с 5 до 30 рабочих дней

Приказ ФСБ России от 25.12.2025 № 547

«Об утверждении Порядка информирования ФСБ России о КА и КИ, реагирования на них, принятия мер по ликвидации последствий КА, проведенных в отношении значимых объектов КИИ РФ и иных информационных ресурсов РФ, принадлежащих органам и организациям, на которые возложены обязанности, предусмотренные частью 4 статьи 9 Федерального закона от 26 июля 2017 г. № 187-ФЗ»

Утратили силу: приказы ФСБ России от 19.06.2019 № 282 и от 07.07.2022 № 348

Ключевые изменения:

- субъекты КИИ и руководители органов (организаций) информируют ФСБ России не только о КИ, но и о КА
- сроки информирования:

Субъекты КИИ о КИ



3 часа — для значимых объектов КИИ

24 часа — для иных объектов КИИ

Субъекты КИИ о КА

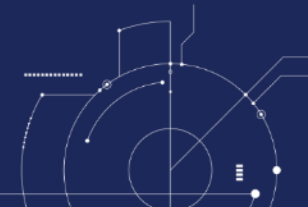


24 часа

Органы и организации о КА и КИ

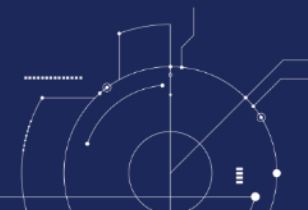


24 часа



Ключевые изменения:

- проект плана реагирования с привлечением субъектом КИИ подразделений и должностных лиц ФСБ России, направляются не в ФСБ России, а в 8 Центр ФСБ России
- руководители органов и организаций обязаны определить состав подразделений и должностных лиц ответственных за проведение мероприятий по реагированию на КИ и принятию мер по ликвидации последствий КА
- органы (организации) направляют в НКЦКИ информацию о результатах реагирования на КИ, принятия мер по ликвидации последствий КА и восстановлению функционирования и проверке работоспособности информационных ресурсов РФ



«Об утверждении Порядка и Технических условий установки и эксплуатации средств, предназначенных для обнаружения, предупреждения и ликвидации последствий КА и реагирования на КИ, в том числе средств, предназначенных для поиска признаков КА, за исключением средств, предназначенных для поиска признаков КА в сетях электросвязи, используемых для организации взаимодействия объектов КИИ РФ»

Утратил силу: приказ ФСБ России от 19.06.2019 № 281

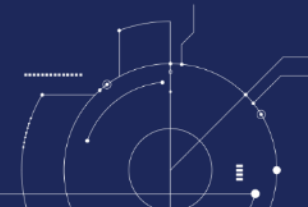
Ключевые изменения:

- субъект КИИ и орган или организация самостоятельно определяют необходимость установки средств ГосСОПКА
- установка, настройка, проверка работоспособности и подключение средств ГосСОПКА проводятся субъектом КИИ или органом (организацией) самостоятельно либо с привлечением аккредитованного центра ГосСОПКА или организации, имеющей соглашение с ФСБ России (НКЦКИ)



Ключевые изменения:

- после установки и подключения средств ГосСОПКА субъект КИИ должен проинформировать об этом НКЦКИ в течение 15 дней и предоставить перечень используемых средств ГосСОПКА
- необходимость установки средств ППКА для субъектов КИИ или органов (организаций) определяет ФСБ России
- установка средств ППКА осуществляется силами и средствами ФСБ России на безвозмездной основе
- эксплуатация средств ППКА, их техническое обслуживание, замена или демонтаж осуществляется ФСБ России



«Об установлении Требований к средствам, предназначенным для обнаружения, предупреждения и ликвидации последствий КА и реагирования на КИ, в том числе к средствам, предназначенным для поиска признаков КА»

Утратил силу: приказ ФСБ России от 06.05.2019 № 196

Ключевые изменения:

- разграничены понятия «средства ППКА» и «средства ППКА в сетях электросвязи»
- расширены и детализированы требования к средствам предупреждения и ликвидации последствий
- средства обнаружения и средства ППКА должны иметь сертификаты соответствия требованиям ФСБ России к средствам обнаружения КА
- убраны требования по визуализации, построения сводных отчетов и хранения информации к средствам обнаружения, средствам предупреждения и средствам ликвидации последствий



«Об утверждении Порядка осуществления непрерывного взаимодействия субъектов КИИ, которым на праве собственности, аренды или ином законном основании принадлежат значимые объекты КИИ РФ, а также руководителей органов и организаций, на которых возложены обязанности, предусмотренные частью 4 статьи 9 Федерального закона от 26 июля 2017 г. № 187-ФЗ, с ГосСОПКА»

Ключевые изменения:

- непрерывное взаимодействие осуществляется посредством подключения к технической инфраструктуре НКЦКИ, соответственно субъекты КИИ, имеющие 30 КИИ, а также органы и организации обязаны подключиться к технической инфраструктуре НКЦКИ
- резервные каналы (почтовый адрес и адрес электронной почты) используются только при наличии технических сбоев и (или) отсутствия связи с личным кабинетом
- подключение осуществляется после заключения регламента взаимодействия



Спасибо за внимание!

<https://gossopka.ru/>

<https://cert.gov.ru/>



НАЦИОНАЛЬНЫЙ КООРДИНАЦИОННЫЙ ЦЕНТР
ПО КОМПЬЮТЕРНЫМ ИНЦИДЕНТАМ