Изменения законодательства в области обеспечения безопасности критической информационной инфраструктуры Российской Федерации

Начальник отдела Управления ФСТЭК России
по Дальневосточному федеральному округу
Локтионов Андрей Викторович

Система нормативных правовых актов в области обеспечения безопасности КИИ РФ

Федеральный закон от 26 июля 2017 г. № 187-ФЗ
«О безопасности критической информационной инфраструктуры Российской Федерации»

Указ Президента РФ от 25 ноября 2017 г. № 569
«О внесении изменений в Положение о Федеральной службе по техническому и экспортному контролю, утвержденное Указом Президента РФ от 16 августа 2004 г. № 1085»

Указ Президента РФ от 22 декабря 2017 г. № 620
«О совершенствовании государственной системы обнаружения, предупреждения и ликвидации последствий компьютерных атак на информационные ресурсы РФ»

Указ Президента РФ от 2 марта 2018 г. № 98
«О внесении изменений в перечень сведений, отнесенных к государственной тайне, утвержденный Указом Президента РФ от 30 ноября 1995 г. № 1203»

Нормативные правовые акты Правительства Российской Федерации

Постановление Правительства РФ
«Об утверждении Правил категорирования объектов критической информационной инфраструктуры РФ, а также перечня показателей критериев значимости объектов КИИ РФ и их значений»
от 8 февраля 2018 г. № 127

Постановление Правительства РФ
«Об утверждении Правил осуществления государственного контроля в области обеспечения безопасности значимых КИИ РФ»
от 17 февраля 2018 г. №162

Постановление Правительства РФ
«Об утверждении Правил подготовки и использования ресурсов единой сети электросвязи РФ для обеспечения функционирования значимых объектов КИИ РФ»
от 8 июня 2019 г. № 743

Нормативные правовые акты федеральных органов исполнительной власти

Приказ ФСТЭК России
«Об утверждении Требований к созданию систем безопасности значимых объектов КИИ РФ и обеспечению их функционирования»
от 21 декабря 2017 г. № 235

Приказ ФСТЭК России
«Об утверждении формы направления сведений о результатах присвоения объекту КИИ РФ одной из категорий значимости»
от 22 декабря 2017 г. № 236

Приказ ФСТЭК России
«Об утверждении Требований по обеспечению безопасности значимых объектов КИИ РФ»
от 25 декабря 2017 г. № 239

Приказ ФСТЭК России
«Об утверждении порядка ведения реестра значимых объектов КИИ РФ» от 6 декабря 2017 г. № 227

Приказ ФСТЭК России
«Об утверждении формы акта проверки, составляемого по итогам проведения гос. контроля в области ОБ КИИ РФ» от 11 декабря 2017 г. № 229

Приказ ФСТЭК России
«Об утверждении Порядка согласования субъектом КИИ РФ … подключения ЗО КИИ РФ к сети связи общего пользования» от 28 мая 2020 г. № 75

Приказ ФСБ России
«Об утверждении Положения о Национальном координационном центре по компьютерным инцидентам»

Приказ ФСБ России
«Об утверждении перечня информации, представляемой в ГосСОПКА и порядка ее представления»

Приказ ФСБ России
«Об утверждении порядка информирования ФСБ России о компьютерных инцидентах и реагирования на них»

Приказ ФСБ России
«Об утверждении порядка, технических условий, установки и эксплуатации средств обнаружения, предупреждения и ликвидации компьютерных атак»

Приказ ФСБ России
«Об утверждении порядка об обмене информации о компьютерных инцидентах между субъектами КИИ»

Приказ Минкомсвязи России
«Об утверждении порядка, технических условий, установки и эксплуатации средств обнаружения, предупреждения и ликвидации компьютерных атак на сетях связи»

Приказ ФСБ России
«Об утверждении требований к средствам обнаружения, предупреждения и ликвидации компьютерных атак»

Разработаны: - ФСТЭК России - ФСБ России - Минцифры России

Нормативные правовые акты в области обеспечения безопасности КИИ, разработанные ФСТЭК России, изданные и измененные в 2020 году

Приказ ФСТЭК России
от 25 декабря 2017 г.
№ 239
(приказ ФСТЭК России
от 20 февраля 2020 г. № 35)

«Об утверждении Требований по обеспечению безопасности значимых объектов КИИ Российской Федерации»

внесены изменения

Приказ ФСТЭК России
от 28 мая 2020 г.
№ 75
«Об утверждении Порядка согласования субъектом КИИ РФ с ФСТЭК России подключения значимого объекта КИИ РФ к сети связи общего пользования»

вновь издан

Требования по обеспечению безопасности ЗО КИИ РФ,

утвержденные приказом ФСТЭК России от 25 декабря 2017 г. № 239

(с изменениями, внесенными приказом ФСТЭК России от 20 февраля 2020 г. № 35)

ФСТЭК России

от 20 февраля 2020 г.
№ 35

ПРИКАЗ
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

I. Общие положения

II. Требования к обеспечению безопасности в ходе создания, эксплуатации и вывода из эксплуатации значимых объектов

III. Требования к организационным и техническим мерам, принимаемым для обеспечения безопасности значимых объектов

IV. Требования к программным и программно-аппаратным средствам, применяемым для обеспечения безопасности значимых объектов

Приложение

Состав мер по обеспечению безопасности для значимого объекта соответствующей категории значимости

Разработаны во исполнение поручений Президента и Правительства Российской Федерации

При разработке **учтено мнение** экспертов крупнейших субъектов КИИ

Прошли **общественное обсуждение**

Согласованы с **Минкомсвязью России**

Приказ **зарегистрирован** Минюстом России 11 сентября 2020 г. № 59793

Требования по обеспечению безопасности ЗО КИИ РФ,

утвержденные приказом ФСТЭК России от 25 декабря 2017 г. № 239

(с изменениями, внесенными приказом ФСТЭК России от 20 февраля 2020 г. № 35)

1. Определены признаки модернизации ЗО КИИ

2. Определены требования по безопасности к программным и программно-аппаратным средствам, применяемым для обеспечения безопасности ЗО КИИ

3. Смягчены требования по удаленному взаимодействию ЗО КИИ

4. Введены условия допущения удаленного доступа к компонентам объектов КИИ и определены меры по обеспечению безопасности такого доступа

С 1 января 2023 г.

Введены требования к специальному прикладному ПО, обеспечивающему выполнение функций ЗО КИИ по назначению

Проверка САМОСТОЯТЕЛЬНО, лицензиатом или интегратором на этапе проектирования

Введены новые требования к СЗИ (6 УД)

Проверка на этапе предварительных испытаний САМОСТОЯТЕЛЬНО или лицензиатом

Требования по обеспечению безопасности ЗО КИИ РФ,

утвержденные приказом ФСТЭК России от 25 декабря 2017 г. № 239

(с изменениями, внесенными приказом ФСТЭК России от 20 февраля 2020 г. № 35)

Новые требования к специальному прикладному ПО

Требования по безопасной разработке

Требования к поддержке безопасности

для значимых объектов 1 категории

Наличие описания структуры ПО на уровне подсистем и результатов сопоставления функций ПО и интерфейсов, описанных в функциональной спецификации, с его подсистемами

Наличие процедур информирования субъекта КИИ об окончании производства и (или) поддержки ПО

Проведение динамического анализа кода программы

Требования по обеспечению безопасности ЗО КИИ РФ,

утвержденные приказом ФСТЭК России от 25 декабря 2017 г. № 239

(с изменениями, внесенными приказом ФСТЭК России от 20 февраля 2020 г. № 35)

Новые требования к контролю удаленного доступа

В значимом объекте не допускается

наличие удаленного доступа к программным и программно-аппаратным средствам, в том числе СЗИ, для обновления или управления со стороны лиц, не являющихся работниками субъекта КИИ

наличие локального бесконтактного доступа к программным и программно-аппаратным средствам, в том числе СЗИ, для обновления или управления со стороны лиц, не являющихся работниками субъекта КИИ

а также работниками его дочерних и зависимых обществ

В случае технической невозможности исключения удаленного доступа к программным и программно-аппаратным средствам, в том числе СЗИ, в ЗО КИИ принимаются компенсирующие меры

Требования по обеспечению безопасности ЗО КИИ РФ,

утвержденные приказом ФСТЭК России от 25 декабря 2017 г. № 239

(с изменениями, внесенными приказом ФСТЭК России от 20 февраля 2020 г. № 35)

Требования к входящим в состав значимого объекта программным и программно-аппаратным средствам

!

Входящие в состав значимого объекта 1 и 2 категории значимости программные и программно-аппаратные средства, осуществляющие хранение и обработку информации, должны размещаться на территории Российской Федерации

За исключением случаев,

когда размещение указанных средств осуществляется в зарубежных обособленных подразделениях субъекта КИИ (филиалах, представительствах), а также случаев, установленных законодательством Российской Федерации и (или) международными договорами Российской Федерации

Порядок согласования подключения значимого объекта КИИ к сети связи общего пользования

Разработан во исполнение постановления Правительства РФ «Об утверждении Правил подготовки и использования ресурсов единой сети электросвязи РФ для обеспечения функционирования значимых объектов КИИ РФ» от 8 июня 2019 г. № 743

МИНИСТЕРСТВО ЮСТИЦИИ РОССИЙСКОЙ ФЕДЕРАЦИИ
ЗАРЕГИСТРИРОВАНО
Регистрационный № 59866
от "15" сентября 2020 г.

ФЕДЕРАЛЬНАЯ СЛУЖБА
ПО ТЕХНИЧЕСКОМУ И ЭКСПОРТНОМУ КОНТРОЛЮ
(ФСТЭК России)

П Р И К А З

«18» мая 2020 г. Москва № 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

В соответствии с пунктом 3 Правил подготовки и использования ресурсов единой сети электросвязи Российской Федерации для обеспечения функционирования значимых объектов критической информационной инфраструктуры, утвержденных постановлением Правительства Российской Федерации от 8 июня 2019 г. № 743 (Собрание законодательства Российской Федерации, 2019, № 24, ст. 3099), **П Р И К А З Ы В А Ю:**

Утвердить прилагаемый Порядок 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.

ДИРЕКТОР ФЕДЕРАЛЬНОЙ СЛУЖБЫ
ПО ТЕХНИЧЕСКОМУ И ЭКСПОРТНОМУ КОНТРОЛЮ

В.СЕЛИН

Приложение
к Порядку согласования субъектом КИИ РФ
с Федеральной службой
по техническому и экспортному контролю
подключения значимого объекта КИИ РФ
к сети связи общего пользования,
утвержденному приказом ФСТЭК России
от 28 мая 2020 г. № 75

Рекомендуемый образец

Сведения
о значимом объекте КИИ РФ, в отношении которого планируется подключение к сети связи общего пользования

Наименование субъекта КИИ _____
указывается полное и сокращенное (при наличии) наименование
Адрес в пределах места нахождения субъекта КИИ _____
Идентификационный номер налогоплательщика
Адрес для переписки_____

1.	Наименование значимого объекта, планируемого к подключению к сети связи общего пользования; регистрационный номер в реестре значимых объектов КИИ	
2.	Цель подключения значимого объекта к сети связи общего пользования	
3.	Тип подключения значимого объекта к сети связи общего пользования (проводной, беспроводной); наименование протоколов сетевого взаимодействия, используемых для целей подключения	
4.	Наименование, модель средств обеспечения безопасности значимого объекта, применяемых при его подключении к сети связи общего пользования; версии программного обеспечения средств	
5.	Номера сертификатов соответствия и даты их выдачи (для средств, прошедших оценку соответствия в форме обязательной сертификации)	

Согласование подключения

До ввода значимого объекта КИИ в действие

До заключения договора с оператором связи

В случае если значимый объект на момент его включения в реестр значимых объектов КИИ РФ имел подключение к сети связи общего пользования, то согласование не требуется

Порядок согласования подключения значимого объекта КИИ к сети связи общего пользования

Представление в ФСТЭК России сведений, указанных в Порядке

Приложение к сведениям необходимых документов

Направление сведений с сопроводительным письмом в ФСТЭК России

ФСТЭК России оценивает достаточность применяемых средств в соответствии с Требованиями приказов № 235 и № 239

20 дней

Принимается решение о согласовании либо об отказе в согласовании подключения ЗО КИИ к ССОП

В случае, если сведений недостаточно

ФСТЭК России запрашивает дополнительные сведения

Основания для отказа в согласовании подключения значимого объекта к ССОП

- Представление неполных сведений и документов
- Несоответствие СЗИ декларированным
- Несоответствие СЗИ Требованиям по ОБ ЗО КИИ и Требованиям по созданию систем ОБ ЗО КИИ и обеспечению их функционирования

Изменения в Кодекс РФ об административных правонарушениях, внесенные Федеральным законом от 26 мая 2021 г. № 141-ФЗ

Статья 13.12.1
Нарушение требований в области обеспечения безопасности критической информационной инфраструктуры Российской Федерации

Нарушение требований к созданию систем безопасности ЗО КИИ РФ и обеспечению их функционирования, либо требований по ОБ ЗО КИИ РФ, установленных федеральными законами и принятыми в соответствии с ними иными НПА РФ, если такие действия (бездействия) не содержат уголовно наказуемого деяния, -
влечет наложение административного штрафа
на должностных лиц в размере от 10 тыс. до 50 тыс. руб.;
на юридических лиц – от 50 тыс. до 100 тыс. руб.

Статья 19.7.15
Непредставление сведений, предусмотренных законодательством в области обеспечения безопасности критической информационной инфраструктуры Российской Федерации

Предусмотрены штрафы за непредставление или нарушение сроков представления сведений о результатах присвоения объекту КИИ РФ категории значимости либо об отсутствии необходимости присвоения ему такой категории

Полномочиями по рассмотрению дел об административных правонарушениях, предусмотренных частью 1 статьи 13.12.1 и частью 1 статьи 19.7.15 КоАП, наделена ФСТЭК России

Изменения законодательства в области обеспечения безопасности критической информационной инфраструктуры Российской Федерации

Начальник отдела Управления ФСТЭК России
по Дальневосточному федеральному округу
Локтионов Андрей Викторович

Первоочередные меры по повышению уровня безопасности критической информационной инфраструктуры

Создание штатного подразделения по обеспечению безопасности значимых объектов КИИ

Проведение инвентаризации ПО и оборудования, входящих в состав значимых объектов КИИ

Разработка организационно-распорядительных документов, регламентирующих защиту значимых объектов КИИ

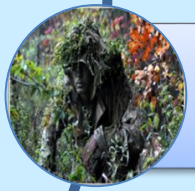
Меры обеспечения безопасности объектов КИИ:

- **усиление мер по защите периметра АСУ ТП**
- **принятие мер по поддержанию безопасного состояния систем**
- **постоянный мониторинг безопасности систем**
- **управление инцидентами информационной безопасности**

Типичные недостатки по результатам анализа сведений о категорировании

Занижение значимости объектов КИИ

Игнорирование сроков реализации 187-ФЗ



Сокрытие объектов КИИ

Привлечение к категорирова-нию сторонних организаций

Импортное ПО и оборудование

Связи с внешними сетями

Низкий потенциал нарушителя

Реализован только базовый набор мер

Типичные недостатки по результатам анализа сведений о категорировании

«Уполномоченные» лица по ОБ КИИ фактически не наделены полномочиями принимать необходимые решения

Непрофильные подразделения безопасности (IT, юристы, экономисты…)

Нет организационно-распорядительных документов

Не реализуются меры по информированию специалистов, эксплуатирующих объекты

Объекты эксплуатируются несколькими организациями, а их ответственность и функции по ОБ КИИ не определены

АРМ администраторов АСУ ТП не включены в состав объектов КИИ и (или) не защищены

Объекты являются территориально распределенными, что вызывает дополнительные сложности в обеспечении их безопасности, которые не учтены

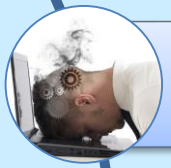
Применяются средств защиты информации, не прошедшие оценку соответствия

Не рассматриваются угрозы, реализуемые внешним нарушителем (через внешние сети)

Необоснованно не рассматривается возможность реализации компьютерных атак на объекты

Недостатки на объектах КИИ

Планы конкретных мероприятий по реализации 187-ФЗ отсутствуют



Специалисты по ОБ КИИ отсутствуют, находятся в подчинении у служб ИТ или перегружены

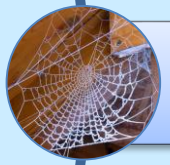
Организационно-распорядительные документы в соответствие требованиям 187-ФЗ не приведены

Не все угрозы безопасности информации (УБИ) определены или нейтрализованы

Персонал об УБИ и правилах безопасной работы не осведомлён

Не все объекты КИИ категорированы

Не все уязвимости нейтрализованы



Средства антивирусной защиты и система обнаружения вторжений не обновляются

Средства защиты информации настроены некорректно

Персонал с инструкциями не ознакомлен

Недостатки на объектах КИИ

Применение наложенных СЗИ, пагубно влияющих на технологический процесс

Не все технические меры по ОБ КИИ приняты

Не минимизированы права доступа

Оценка соответствия СЗИ и систем ОБ не осуществлена

АРМ администрирования компонентов ЗО КИИ в их состав не входят

Модернизация ОБ КИИ не спланирована

Недостатки на объектах КИИ

Не осуществляется учет и контроль съемных МНИ и подключаемых СВТ

АРМ управления СЗИ не защищаются

SOC не готов к APT-атакам

Инструкции персоналу перегружены

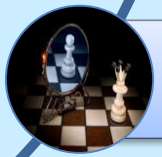
Категорирование создаваемых объектов не проводится

Рассматривается нарушитель с низким потенциалом

Небезопасная архитектура сети

Редко осуществляется анализ защищенности

Отсутствует контроль за интегратором АСУ



Состав ОКИИ не соответствует приведенному в сведениях