Проблемные вопросы реализации Федерального закона «О безопасности критической информационной инфраструктуры Российской Федерации»

Зенкин Павел Сергеевич
Начальник отдела управления ФСТЭК России

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»
от 24 июля 2018 г. № 366

Приказ ФСБ России
«Об утверждении перечня информации, представляемой в ГосСОПКА и порядка ее представления»
от 24 июля 2019 г. № 367

Приказ ФСБ России
«Об утверждении порядка информирования ФСБ России о компьютерных инцидентах и реагирования на них»
от 16 июля 2019 г. № 282

Приказ ФСБ России
«Об утверждении порядка, технических условий, установки и эксплуатации средств обнаружения, предупреждения и ликвидации компьютерных атак»
от 19 июня 2019 г. № 281

Приказ ФСБ России
«Об утверждении порядка об обмене информации о компьютерных инцидентах между субъектами КИИ»
от 24 июля 2018 г. № 368

Приказ Минкомсвязи России
«Об утверждении порядка и технических условий установки и эксплуатации средств предназначенных для поиска признаков компьютерных атак в сетях электросвязи»
от 17 марта 2020 г. № 114

Приказ ФСБ России
«Об утверждении требований к средствам обнаружения, предупреждения и ликвидации компьютерных атак»
от 6 мая 2019 г. № 196

Разработаны: - ФСТЭК России - ФСБ России - Минцифры России

Кодекс РФ об административных правонарушениях

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 в размере:**
на должностных лиц – **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 **наделяется ФСТЭК России**

Нормативные правовые акты в области обеспечения безопасности КИИ, разработанные ФСТЭК России

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

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

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

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

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

Приказ ФСТЭК России
от 21 декабря 2017 г.
№ 235
«Об утверждении Требований к созда-нию систем безопас-ности значимых объектов КИИ РФ и обеспечению их функционирования»

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

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»

- внесены изменения

- планируется внести изменения

Изменения в Правилах категорирования объектов КИИ

ПРАВИТЕЛЬСТВО РОССИЙСКОЙ ФЕДЕРАЦИИ

ПОСТАНОВЛЕНИЕ

от 24 декабря 2021 г. № 2431

МОСКВА

О внесении изменений в Правила категорирования объектов критической информационной инфраструктуры Российской Федерации

Правительство Российской Федерации **п о с т а н о в л я е т :**

Дополнить Правила категорирования объектов критической информационной инфраструктуры Российской Федерации, утвержденные постановлением Правительства Российской Федерации от 8 февраля 2018 г. № 127 "Об утверждении Правил категорирования объектов критической информационной инфраструктуры Российской Федерации, а также перечня показателей критериев значимости объектов критической информационной инфраструктуры Российской Федерации и их значений" (Собрание законодательства Российской Федерации, 2018, № 8, ст. 1204; 2019, № 16, ст. 1955), пунктами 19^1 и 19^2 следующего содержания:

"19^1. В случае изменения сведений, указанных в подпунктах "а" - "е" пункта 17 настоящих Правил, субъект критической информационной инфраструктуры направляет в федеральный орган исполнительной власти, уполномоченный в области обеспечения безопасности критической информационной инфраструктуры, новые сведения в печатном и электронном виде не позднее 20 рабочих дней со дня их изменения по форме, предусмотренной пунктом 18 настоящих Правил.

19^2. Государственные органы и российские юридические лица, выполняющие функции по разработке, проведению или реализации государственной политики и (или) нормативно-правовому регулированию в установленной сфере деятельности, осуществляют мониторинг

5392674

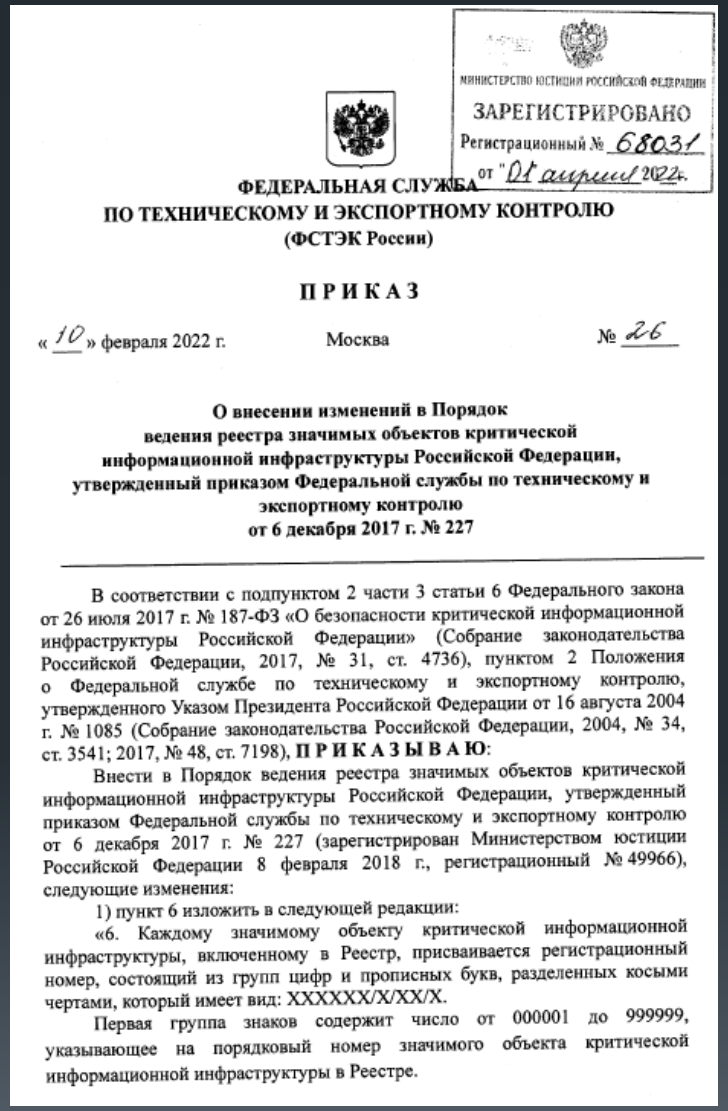
- 19^1. В случае изменения сведений, указанных в подпунктах "а" - "е" пункта 17 настоящих Правил, субъект критической информационной инфраструктуры направляет в ФСТЭК России, новые сведения в печатном и электронном виде не позднее 20 рабочих дней со дня их изменения по форме, предусмотренной пунктом 18 настоящих Правил.

- 19^2. Государственные органы и российские юридические лица, выполняющие функции по разработке, проведению или реализации государственной политики и (или) нормативно-правовому регулированию в установленной сфере деятельности, осуществляют мониторинг представления субъектами критической информационной инфраструктуры, выполняющими функции (полномочия) или осуществляющими виды деятельности в соответствующих областях (сферах), актуальных и достоверных сведений, указанных в подпунктах "а" - "е" пункта 17 настоящих Правил.

- Мониторинг осуществляется регулярно путем запроса и оценки информации о сроках представления, актуальности и достоверности сведений, указанных в подпунктах "а" - "е" пункта 17 настоящих Правил.

- При выявлении по результатам мониторинга нарушения сроков работ по категорированию, представления в ФСТЭК России, неактуальных либо недостоверных сведений государственные органы и российские юридические лица, указанные в абзаце первом настоящего пункта, направляют в ФСТЭК России, сведения о выявленных нарушениях.

Изменение порядка ведения реестра значимых объектов КИИ



МИНИСТЕРСТВО ЮСТИЦИИ РОССИЙСКОЙ ФЕДЕРАЦИИ
ЗАРЕГИСТРИРОВАНО
Регистрационный № 68031
от "01" апреля 2022 г.

ФЕДЕРАЛЬНАЯ СЛУЖБА
ПО ТЕХНИЧЕСКОМУ И ЭКСПОРТНОМУ КОНТРОЛЮ
(ФСТЭК России)

П Р И К А З

« 10 » февраля 2022 г. Москва № 26

О внесении изменений в Порядок ведения реестра значимых объектов критической информационной инфраструктуры Российской Федерации, утвержденный приказом Федеральной службы по техническому и экспортному контролю от 6 декабря 2017 г. № 227

В соответствии с подпунктом 2 части 3 статьи 6 Федерального закона от 26 июля 2017 г. № 187-ФЗ «О безопасности критической информационной инфраструктуры Российской Федерации» (Собрание законодательства Российской Федерации, 2017, № 31, ст. 4736), пунктом 2 Положения о Федеральной службе по техническому и экспортному контролю, утвержденного Указом Президента Российской Федерации от 16 августа 2004 г. № 1085 (Собрание законодательства Российской Федерации, 2004, № 34, ст. 3541; 2017, № 48, ст. 7198), **П Р И К А З Ы В А Ю**:

Внести в Порядок ведения реестра значимых объектов критической информационной инфраструктуры Российской Федерации, утвержденный приказом Федеральной службы по техническому и экспортному контролю от 6 декабря 2017 г. № 227 (зарегистрирован Министерством юстиции Российской Федерации 8 февраля 2018 г., регистрационный № 49966), следующие изменения:

1) пункт 6 изложить в следующей редакции:

«6. Каждому значимому объекту критической информационной инфраструктуры, включенному в Реестр, присваивается регистрационный номер, состоящий из групп цифр и прописных букв, разделенных косыми чертами, который имеет вид: XXXXXX/X/XX/X.

Первая группа знаков содержит число от 000001 до 999999, указывающее на порядковый номер значимого объекта критической информационной инфраструктуры в Реестре.

Сведения из Реестра могут предоставляться государственным органам или российским юридическим лицам, выполняющим функции по разработке, проведению или реализации государственной политики и (или) нормативно-правовому регулированию в установленной сфере ежеквартально, либо их запросам

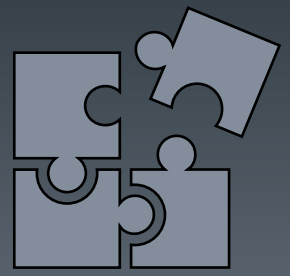
Требования к организации защиты

Система безопасности ЗОКИИ

Проблемы обеспечения безопасности ЗОКИИ

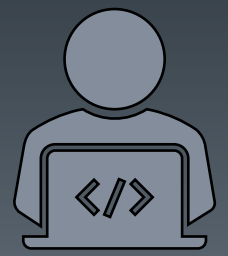
Недостаточный уровень квалификации специалистов по информационной безопасности

Низкий уровень информативности в области безопасности КИИ

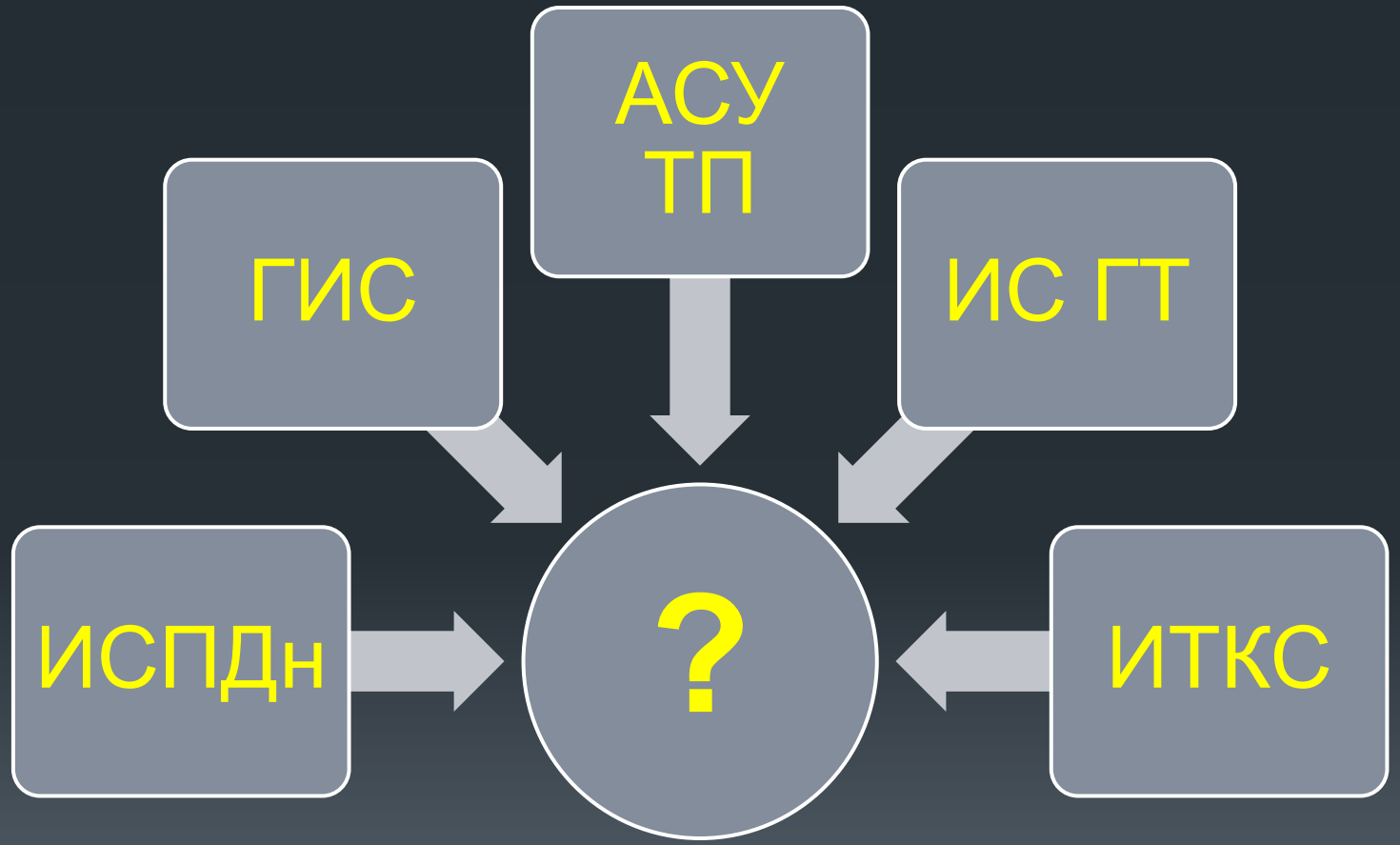


Отсутствие единых подходов к защите информации

Недостаточный уровень применения разработчиками мер по безопасной разработке ПО



Проблемные вопросы обеспечения безопасности ЗОКИИ



Особенности реализации требований

Значимый объект КИИ обрабатывает ГТ	Законодательство РФ о государственной тайне	
Значимый объект КИИ является ГИС	Приказ ФСТЭК России от 11 февраля 2013 г. № 17	***Приказ ФСТЭК России от 25 декабря 2017 г. № 239***
Значимый объект КИИ является ИСПДн	Постановление Правительства РФ от 1 ноября 2012 г. № 1119	***Приказ ФСТЭК России от 25 декабря 2017 г. № 239***
Значимый объект КИИ является ИТКС	***Приказ ФСТЭК России от 25 декабря 2017 г. № 239***	Нормативные правовые акты Минкомсвязи России
Значимый объект КИИ является АСУ ТП	***Приказ ФСТЭК России от 25 декабря 2017 г. № 239***	

Меры по обеспечению безопасности значимого объекта КИИ

17 групп мер

- Аудит безопасности (АУД)
- Управление конфигурацией (УКФ)
- Управление обновлениями программного обеспечения (ОПО)
- Планирование мероприятий по обеспечению безопасности (ПЛН)
- Реагирование на инциденты информационной безопасности (ИНЦ)
- Информирование и обучение персонала (ИПО)
- Защита технических средств и систем (ЗТС)
- Обеспечение действий в нештатных (непредвиденных) ситуациях (ДНС)
- Идентификация и аутентификация (ИАФ)
- Управление доступом (УПД)
- Ограничение программной среды (ОПС)
- Защита машинных носителей информации (ЗНИ)
- Антивирусная защита (АВЗ)
- Предотвращение вторжений (компьютерных атак) (СОВ)
- Обеспечение целостности (ОЦЛ)
- Обеспечение доступности (ОДТ)
- Защита информационной (автоматизированной) системы (сети) и ее компонентов (ЗИС)

СПАСИБО ЗА ВНИМАНИЕ!

Зенкин Павел Сергеевич
Начальник отдела управления ФСТЭК России