# Вопросы обеспечения безопасности критической информационной инфраструктуры Российской Федерации

ТОРБЕНКО Елена Борисовна
Заместитель начальника управления ФСТЭК России

# Система нормативных правовых актов в области обеспечения безопасности объектов критической информационной инфраструктуры Российской Федерации

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

## Нормативные правовые акты Президента 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 Российской Федерации от 16 августа 2004 г. № 1085»

Указ Президента РФ «О внесении изменений в Указ Президента РФ от 15 января 2013 г. № 31с «О создании государственной системы обнаружения, предупреждения и ликвидации компьютерных атак»

Указ Президента РФ от 2 марта 2018 г. «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 Российской Федерации, а также перечня показателей критериев значимости объектов критической информационной инфраструктуры Российской Федерации и их значений» от 8 февраля 2018 г. № 127

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

Постановление Правительства РФ «Об утверждении правил подготовки и использования ресурсов единой сети электросвязи Российской Федерации для обеспечения функционирования значимых объектов критической информационной инфраструктуры» 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» от 21 декабря 2017 г. № 235 (зарегистрирован Минюстом России 22 февраля 2018 г., рег. № 50118)

Приказ ФСТЭК России «Об утверждении формы направления сведений о результатах присвоения объекту КИИ одной из категорий значимости» от 22 декабря 2017 г. № 236 (зарегистрирован Минюстом России 13 апреля 2018 г., рег. № 50753)

Приказ ФСТЭК России «Об утверждении требований по обеспечению безопасности значимых объектов КИИ» от 25 декабря 2017 г. № 239 (зарегистрирован Минюстом России 26 марта 2018 г., рег. № 50524)

Приказ ФСТЭК России «Об утверждении формы акта проверки» от 11 декабря 2017 г. № 229 (зарегистрирован Минюстом России 28 декабря 2017 г., рег. № 49500)

Приказ ФСТЭК России «Об утверждении порядка ведения реестра значимых объектов КИИ» от 6 декабря 2017 г. № 227 (зарегистрирован Минюстом России 8 февраля 2018 г., рег. № 49966)

Приказ ФСТЭК России «Об утверждении Порядка согласования субъектом КИИ РФ с ФСТЭК России подключения значимого объекта КИИ к сети связи общего пользования» от 8 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»

- ФСТЭК России
- ФСБ России
- Минкомсвязи России

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

Постановление 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**

Постановление Правительства Российской Федерации от 17 февраля 2018 г. № 162

**Об утверждении Правил осуществления государственного контроля в области обеспечения безопасности значимых объектов критической информационной инфраструктуры**

Приказ ФСТЭК России от 25 декабря 2017 г. № 239

**Об утверждении требований по обеспечению безопасности значимых объектов КИИ**

(зарегистрирован Минюстом России 26 марта 2018 г., рег. № 50524)

Приказ ФСТЭК России от 21 декабря 2017 г. № 235

**Об утверждении требований к созданию систем безопасности значимых объектов КИИ**

(зарегистрирован Минюстом России 22 февраля 2018 г., рег. № 50118)

Приказ ФСТЭК России от 11 декабря 2017 г. № 229

**Об утверждении формы акта проверки**

(зарегистрирован Минюстом России 28 декабря 2017 г., рег. № 49500)

Приказ ФСТЭК России от 22 декабря 2017 г. № 236

**Об утверждении формы направления сведений о результатах присвоения объекту КИИ одной из категорий значимости**

(зарегистрирован Минюстом России 13 апреля 2018 г., рег. № 50753)

Приказ ФСТЭК России от 6 декабря 2017 г. № 227

**Об утверждении порядка ведения реестра значимых объектов КИИ**

(зарегистрирован Минюстом России 8 февраля 2018 г., рег. № 49966)

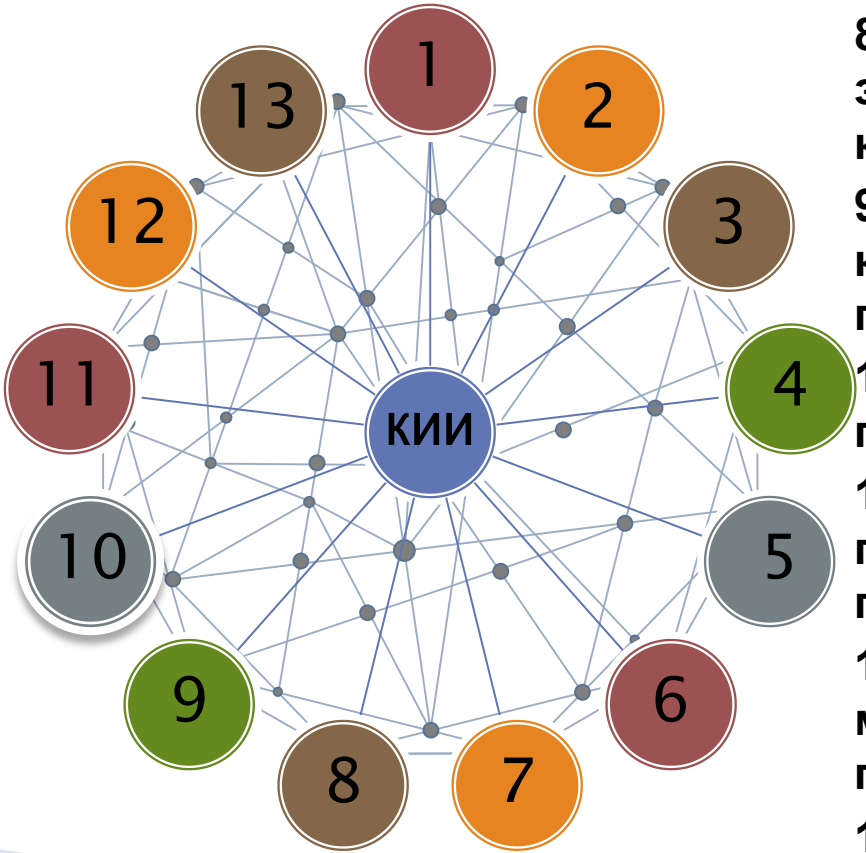
Приказ ФСТЭК России от 8 мая 2020 г. № 75

Об утверждении Порядка согласования субъектом КИИ РФ с ФСТЭК России подключения значимого объекта КИИ к сети связи общего пользования

(на регистрации в Минюсте России )

# ФЗ «О безопасности критической информационной инфраструктуры Российской Федерации»

1.Сфера здравоохранения
2.Сфера науки
3.Сфера транспорта
4.Сфера связи
5.Сфера атомной энергии
6.Банковская сфера и иные сферы финансового рынка
7.Сфера энергетики




8.Сфера топливно-энергетического комплекса
9.Сфера ракетно-космической промышленности
10.Сфера химической промышленности
11.Сфера горнодобывающей промышленности
12.Сфера металлургической промышленности
13.Сфера оборонной промышленности

# Этапы обеспечения безопасности КИИ

# Текущие результаты категорирования

***Более 52 000 объектов КИИ, подлежащих категорированию***

*от более 5000 субъектов*


***Завершена процедура категорирования в отношении более 24 000 объектов КИИ***

# Текущие результаты категорирования

# А в чем проблема?

# А в чем проблема?

Отсутствие отраслевого регулирования

***Различные системы в различных отраслях***

АСУ ТП

ИС

ИТКС

# А в чем проблема?

Отсутствие знаний у субъекта КИИ

***Знать и читать законодательство***

***Знать свое хозяйство***

Нежелание субъекта КИИ выполнять требования

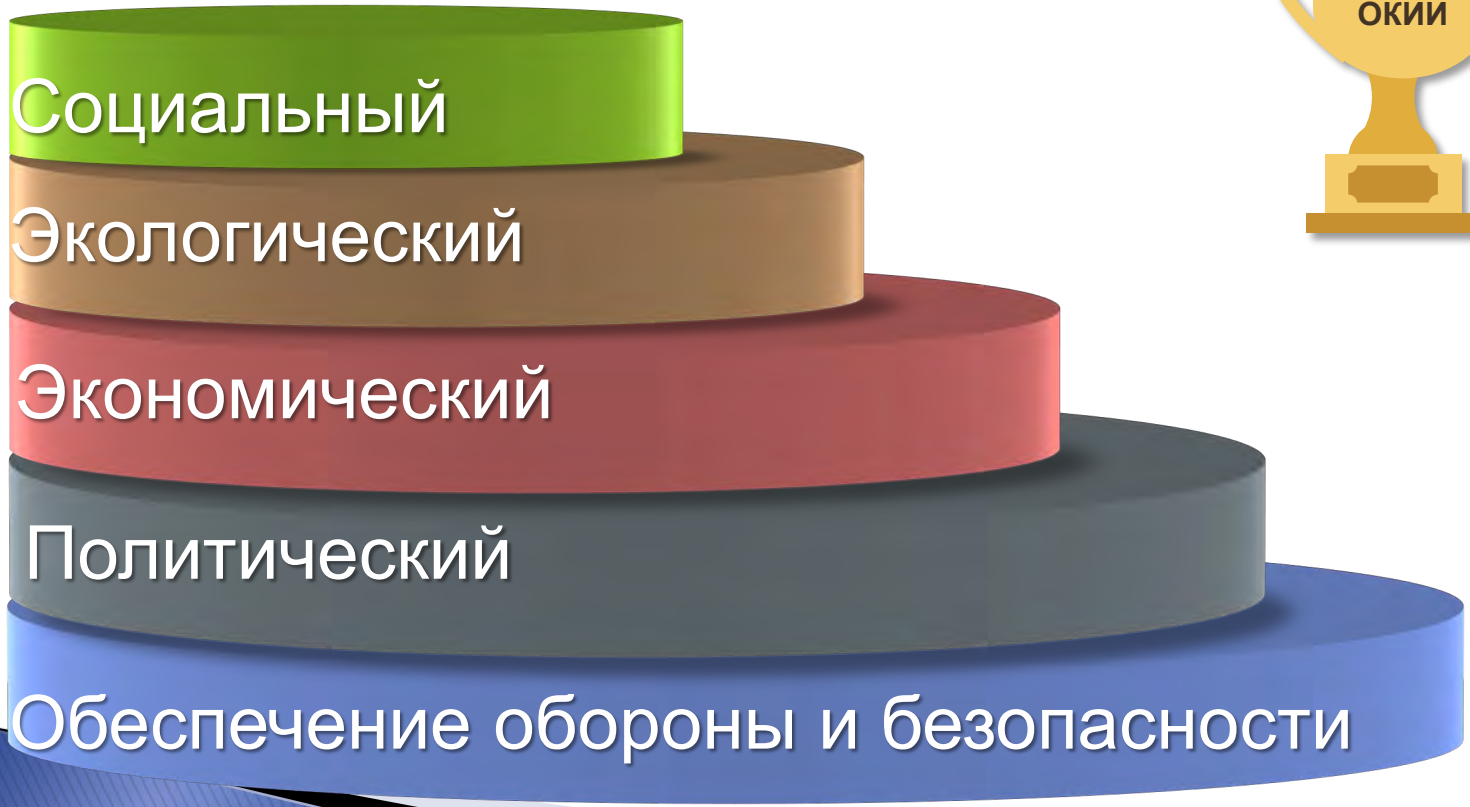
***Здраво оценивать последствия***

# А в чем проблема?

Что
на предприятии
отнести к КИИ

# А в чем проблема?

## Показатели значимости



# На что обратить внимание?


Угрозы, реализуемые внешним нарушителем

Связи с внешними сетями

Рассматриваются не все возможные сценарии атак

Замедление автоматизируемого процесса

Не учитывается зависимость одного ОКИИ (процесса) от другого ОКИИ (процесса)

## *II Требования к силам обеспечения безопасности*

**Руководитель структурного подразделения по безопасности**

- высшее профессиональное образование
  - по направлению подготовки в области информационной безопасности
  - иное высшее профессиональное образование и обучение по программе профессиональной переподготовки по направлению "Информационная безопасность" (не менее 360 часов)
- наличие стажа работы в сфере информационной безопасности не менее 3 лет

**Штатные работники структурного подразделения по безопасности**

- высшее профессиональное образование
  - по направлению подготовки в области информационной безопасности
  - иное высшее профессиональное образование и прохождение обучения по программе повышения квалификации по направлению "Информационная безопасность" (не менее 72 часов)

прохождение не реже одного раза в 5 лет обучения по программам повышения квалификации по направлению «Информационная безопасность»

*Вступление в силу с 1 января 2021 г.*

# СПАСИБО ЗА ВНИМАНИЕ!

ТОРБЕНКО Елена Борисовна
Заместитель начальника управления ФСТЭК России