ЦИФРОВОЙ РЕГИОН

ЧУДПО РЦБ

Безопасность критической информационной инфраструктуры Российской Федерации

Лекция 1. Основы законодательства в области обеспечения безопасности КИИ РФ

ЦИФРОВОЙ РЕГИОН

ЧУДПО РЦБ

В настоящее время существует следующая система нормативных правовых актов по вопросам обеспечения безопасности критической информационной инфраструктуры Российской Федерации:

Федеральные законы

Нормативные правовые акты Президента Российской Федерации

УКАЗ
ПРЕЗИДЕНТА РОССИЙСКОЙ ФЕДЕРАЦИИ

Нормативные правовые акты федеральных органов исполнительной власти

Нормативные правовые акты Правительства Российской Федерации

Федеральные законы

Федеральный закон от 26 июля 2017 г. N 187-ФЗ «О безопасности критической информационной инфраструктуры Российской Федерации»

Федеральный закон от 26 июля 2017 г. N 193-ФЗ «О внесении изменений в отдельные законодательные акты Российской Федерации в связи с принятием Федерального закона «О безопасности КИИ РФ»

РОССИЙСКАЯ ФЕДЕРАЦИЯ

ФЕДЕРАЛЬНЫЙ ЗАКОН

О безопасности критической информационной инфраструктуры Российской Федерации

Принят Государственной Думой 12 июля 2017 года

Одобрен Советом Федерации 19 июля 2017 года

Статья 1. **Сфера действия настоящего Федерального закона**

Настоящий Федеральный закон регулирует отношения в области обеспечения безопасности критической информационной инфраструктуры Российской Федерации (далее также – критическая информационная инфраструктура) в целях ее устойчивого функционирования при проведении в отношении ее компьютерных атак.

Статья 2. **Основные понятия, используемые в настоящем Федеральном законе**

Для целей настоящего Федерального закона используются следующие основные понятия:

2) в порядке, установленном ФСБ России, получать от указанного органа информацию о средствах и способах проведения компьютерных атак, а также о методах их предупреждения и обнаружения

1) получать от ФСТЭК России информацию, необходимую для обеспечения безопасности значимых объектов КИИ

3) при наличии согласия ФСБ России за свой счет приобретать, арендовать, устанавливать и обслуживать средства, предназначенные для обнаружения, предупреждения и ликвидации последствий компьютерных атак и реагирования на компьютерные инциденты

4) разрабатывать и осуществлять мероприятия по обеспечению безопасности ЗОКИИ

ОБЯЗАН

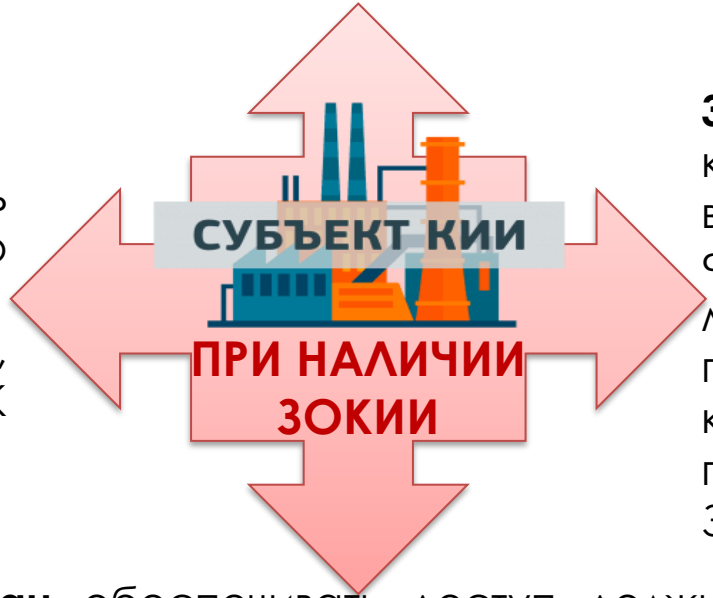
1) незамедлительно информировать о компьютерных инцидентах ФСБ России, а также Центральный банк Российской Федерации

2) оказывать содействие должностным лицам ФСБ России в обнаружении, предупреждении и ликвидации последствий компьютерных атак, установлении причин и условий возникновения компьютерных инцидентов

3) в случае установки на объектах КИИ средств, предназначенных для обнаружения, предупреждения и ликвидации последствий компьютерных атак и реагирования на компьютерные инциденты, обеспечивать выполнение технических условий установки и эксплуатации таких средств, их сохранность

2) обязан выполнять предписания должностных лиц ФСТЭК России об устранении нарушений в части соблюдения требований по обеспечению безопасности ЗОКИИ, выданные этими лицами в соответствии со своей компетенцией

1) обязан соблюдать требования по обеспечению безопасности ЗОКИИ, установленные ФСТЭК России



3) обязан реагировать на компьютерные инциденты в порядке, утвержденном ФСБ России, принимать меры по ликвидации последствий компьютерных атак, проведенных в отношении ЗОКИИ

4) обязан обеспечивать доступ должностным лицам ФСТЭК России, к ЗОКИИ при реализации этими лицами установленных полномочий

ЦИФРОВОЙ РЕГИОН

ЧУДПО РЦБ

В Федеральном законе от 26 июля 2017 г. N 187-ФЗ в Статье 4. «Принципы обеспечения безопасности КИИ» принципами **обеспечения безопасности КИИ** являются:

- законность
- непрерывность и комплексность
- приоритет предотвращения компьютерных атак