

The background of the slide is a photograph of a businessman in a dark suit and blue tie, holding several large, metallic, 3D-rendered gears. The gears are arranged in a way that suggests a complex mechanical or industrial process. The lighting is bright, highlighting the metallic texture of the gears.

**Реализация Федерального закона
от 26 июля 2017 года № 187-ФЗ
«О безопасности критической
информационной инфраструктуры
Российской Федерации»**

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

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 нее компьютерных атак.

Настоящий Федеральный закон вступил в силу с **1 января 2018 года!!!**

Объекты

- Информационные системы
- Информационно-телекоммуникационные сети
- Автоматизированные системы управления субъектов критической информационной инфраструктуры

Субъекты

- Владельцы объекта КИИ
- Лица или организации, обеспечивающие взаимодействие объектов КИИ между собой
- Лицо, эксплуатирующее объект КИИ

Объекты КИИ

Наука

Оборонная
промышленность

Здравоохранение

Транспорт

Отрасли связи

Банковская и
финансовая сфера

Энергетика

ТЭК

Атомная
энергетика

Ракетно-
промышленный
комплекс

Химическая
промышленность

Металлургическая
промышленность

Горно-
добывающая
промышленность

Регуляторы



Федеральная служба по техническому и экспортному контролю

ФСТЭК России

<http://fstec.ru>



Федеральная служба безопасности Российской Федерации

ФСБ России

<http://www.fsb.ru>



Министерство связи и массовых коммуникаций Российской Федерации

Минкомсвязь России

<http://minsvyaz.ru>

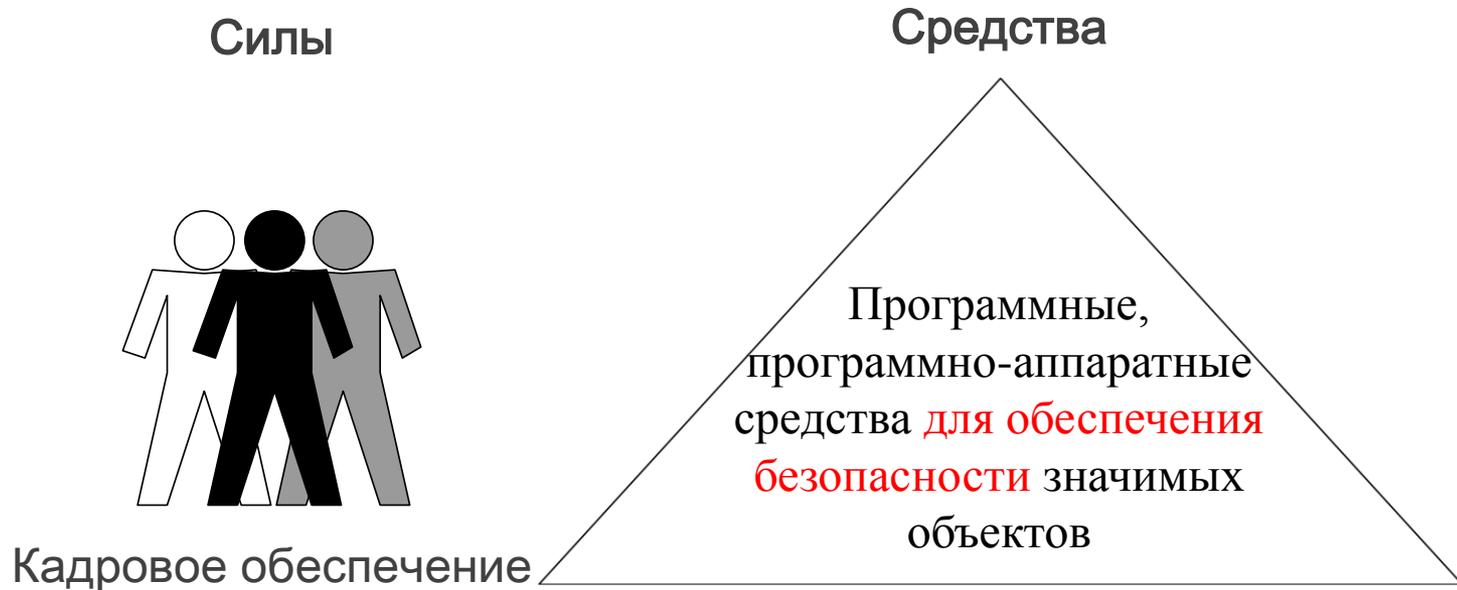


Центральный банк Российской Федерации

Банк России

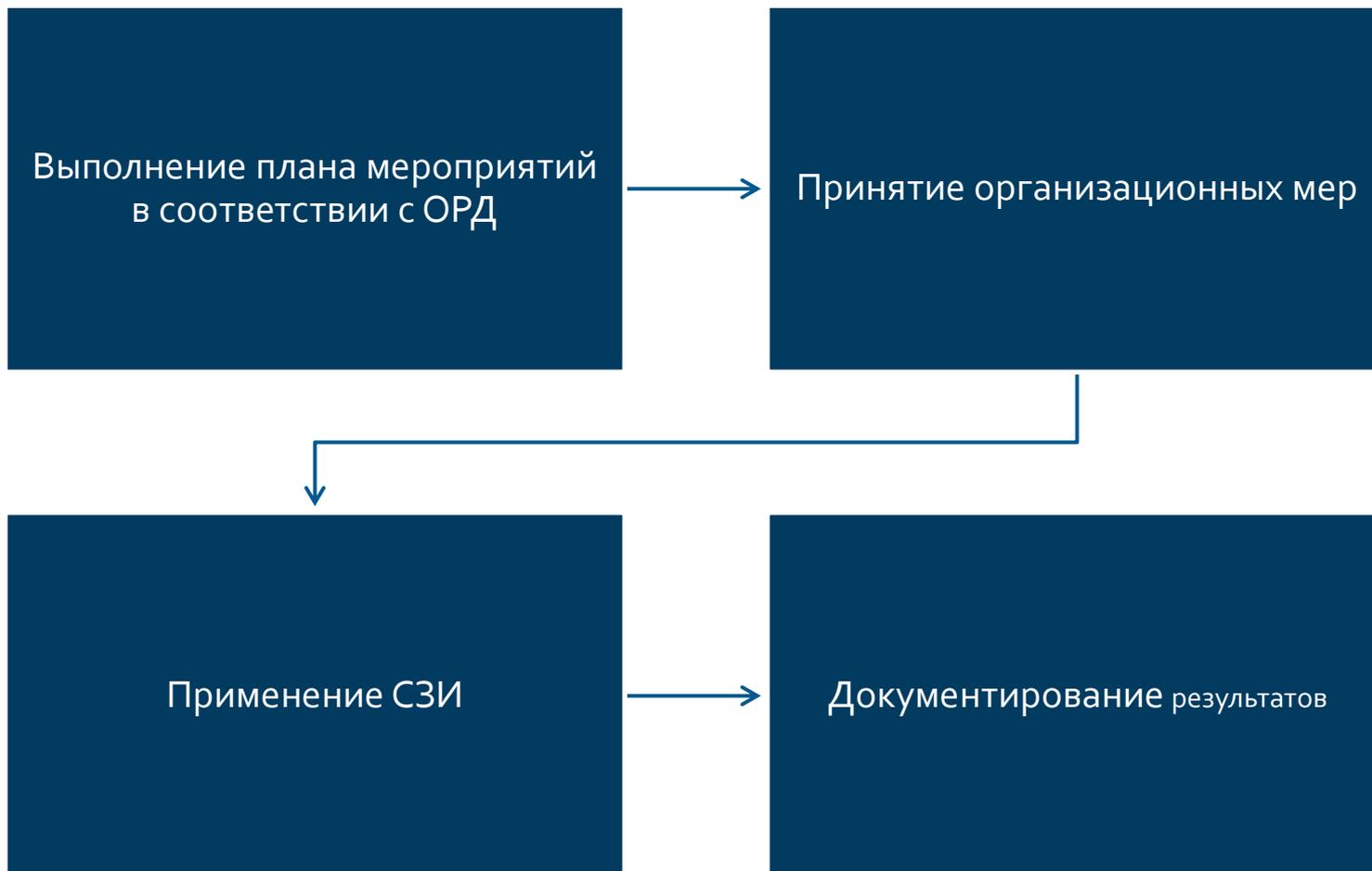
<http://www.cbr.ru>

Необходимые ресурсы



Организационно-распорядительные документы

Реализация мероприятий по обеспечению безопасности значимых объектов



Контроль состояния безопасности значимых объектов

Внутренний контроль организации работ по обеспечению безопасности значимых объектов и эффективности принимаемых организационных и технических мер

Внешняя оценка (внешний аудит) состояния безопасности значимых объектов

Проводит комиссия, назначаемая субъектом КИИ, в состав которой входят работники структурного подразделений эксплуатирующих значимые объекты

Проводят организации, имеющие лицензии на деятельность в области ЗИ

Акт, подписываемый членами комиссии и утверждаемый руководителем субъекта (уполномоченным лицом) Выявленные замечания подлежат устранению в порядке и сроки, установленные руководителем субъекта КИИ (уполномоченным лицом)

Совершенствование безопасности значимых объектов

Проведение анализа функционирования системы безопасности, состояния безопасности значимых объектов

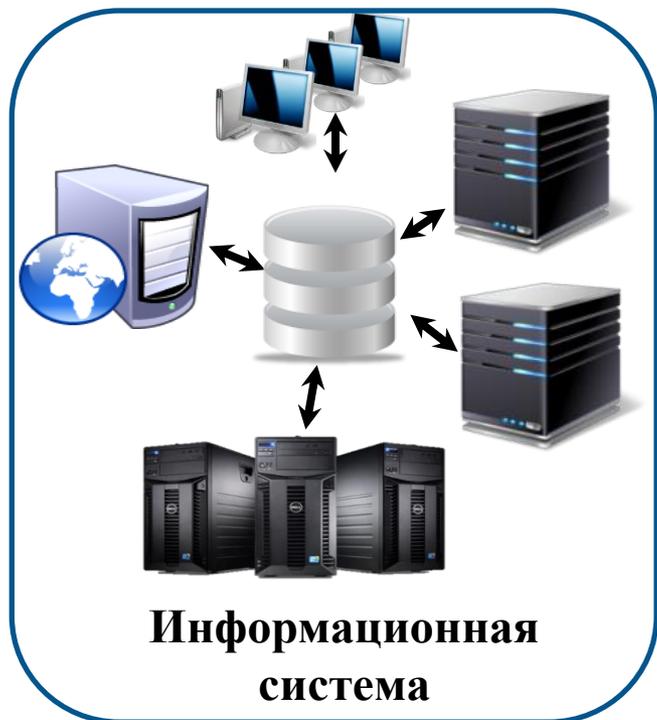
Предложения представляются руководителю субъекта КИИ

Разработка предложений по развитию системы безопасности по совершенствованию безопасности значимых объектов

Предложения могут быть внесены в план мероприятий (по решению руководителя субъекта КИИ)

Осуществляется структурным подразделением по безопасности, специалистами по безопасности с участием подразделений (работников), эксплуатирующих значимые объекты, и подразделений (работников), обеспечивающих функционирование значимых объектов

Соответствие категорий значимых объектов и потенциала нарушителей



Соответствие категории и класса средства защиты информации



Категория

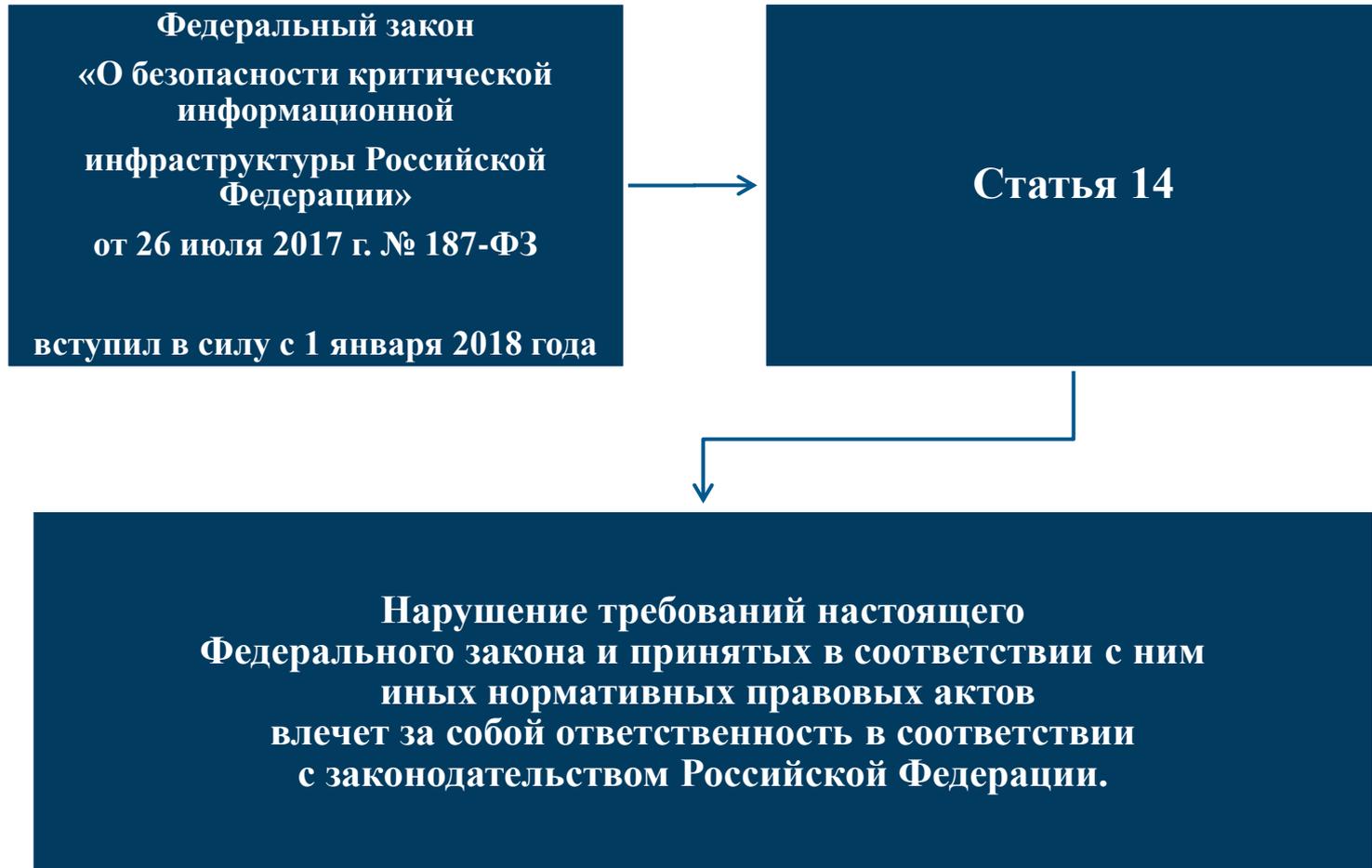


Класс защиты средства защиты информации

Во всех категориях значимых объектов - средства вычислительной техники не ниже 5 класса.

В значимых объектах 1 и 2 категорий – средства защиты информации, прошедшие проверку не ниже чем по 4 уровню контроля отсутствия недеklarированных возможностей

Ну, и наконец...



**Уголовный кодекс
Российской Федерации
С изменениями, внесенными
ФЗ-194 от 26.07.2017**



**Статья 274.1.
Неправомерное воздействие
на критическую
информационную
инфраструктуру Российской
Федерации**



Части 1-5

Создание, распространение и (или) использование компьютерных программ либо иной компьютерной информации, заведомо предназначенных для неправомерного воздействия на критическую информационную инфраструктуру Российской Федерации, в том числе для уничтожения, блокирования, модификации, копирования информации, содержащейся в ней, или нейтрализации средств защиты указанной информации, - наказываются принудительными работами на срок до пяти лет с ограничением свободы на срок до двух лет или без такового либо лишением свободы на срок от двух до пяти лет со штрафом в размере от пятисот тысяч до одного миллиона рублей или в размере заработной платы или иного дохода осужденного за период от одного года до трех лет.

Неправомерный доступ к охраняемой компьютерной информации, содержащейся в критической информационной инфраструктуре Российской Федерации, в том числе с использованием компьютерных программ либо иной компьютерной информации, которые заведомо предназначены для неправомерного воздействия на критическую информационную инфраструктуру Российской Федерации, или иных вредоносных компьютерных программ, если он повлек причинение вреда критической информационной инфраструктуре Российской Федерации, - наказывается принудительными работами на срок до пяти лет со штрафом в размере от пятисот тысяч до одного миллиона рублей или в размере заработной платы или иного дохода осужденного за период от одного года до трех лет и с ограничением свободы на срок до двух лет или без такового либо лишением свободы на срок от двух до шести лет со штрафом в размере от пятисот тысяч до одного миллиона рублей или в размере заработной платы или иного дохода осужденного за период от одного года до трех лет.

Часть 3

Нарушение правил эксплуатации средств хранения, обработки или передачи охраняемой компьютерной информации, содержащейся в критической информационной инфраструктуре Российской Федерации, или информационных систем, информационно-телекоммуникационных сетей, автоматизированных систем управления, сетей электросвязи, относящихся к критической информационной инфраструктуре Российской Федерации, либо правил доступа к указанным информации, информационным системам, информационно-телекоммуникационным сетям, автоматизированным системам управления, сетям электросвязи, если оно повлекло причинение вреда критической информационной инфраструктуре Российской Федерации, - наказывается принудительными работами на срок до пяти лет с лишением права занимать определенные должности или заниматься определенной деятельностью на срок до трех лет или без такового либо лишением свободы на срок до шести лет с лишением права занимать определенные должности или заниматься определенной деятельностью на срок до трех лет или без такового.

Часть 4

Деяния, предусмотренные частью первой, второй или третьей настоящей статьи, совершенные группой лиц по предварительному сговору или организованной группой, или лицом с использованием своего служебного положения, - наказываются лишением свободы на срок от трех до восьми лет с лишением права занимать определенные должности или заниматься определенной деятельностью на срок до трех лет или без такового.

Часть 5

Деяния, предусмотренные частью первой, второй, третьей или четвертой настоящей статьи, если они повлекли тяжкие последствия, - наказываются лишением свободы на срок от пяти до десяти лет с лишением права занимать определенные должности или заниматься определенной деятельностью на срок до пяти лет или без такового. 23

Где получить информацию?

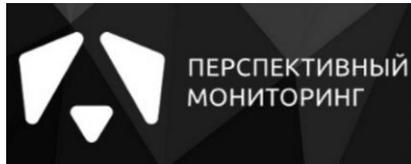


Антон Калинин

Руководитель обособленного подразделения

e-mail: anton.kalinin@infotecs.ru

T: +7 -929 050 14 88



Роман Кобцев

Директор по развитию бизнеса

e-mail: Roman.Kobtsev@amonitoring.ru

T.: +7 (495) 737-6192 доб.5273

Вадим Майшев

Заместитель генерального директора
ООО НПП «Ижинформпроект»

T.: +7 (3412) 918100 mvv@infotrust.ru

A sunset scene with a warm, orange and yellow sky. In the foreground, several wind turbines are silhouetted against the bright light. In the background, a series of high-voltage power lines stretch across the horizon. The overall atmosphere is serene and suggests a focus on renewable energy.

Спасибо за внимание!