SAVE group

Код ИБ Воронеж

Критическая информационная инфраструктура Российской Федерации

Как выполнить требования закона о КИИ с минимальным ущербом для компании?

КОД ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ

Технический директор департамента защиты информационных систем, к.т.н. Владимир Минаков

Федеральный закон «О безопасности критической информационной инфраструктуры Российской Федерации»

Автоматизированные системы управления субъектов КИИ

Информационные системы субъектов КИИ

Информационно-телекоммуникационные системы субъектов КИИ

Кто должен выполнить закон?

Субъекты КИИ

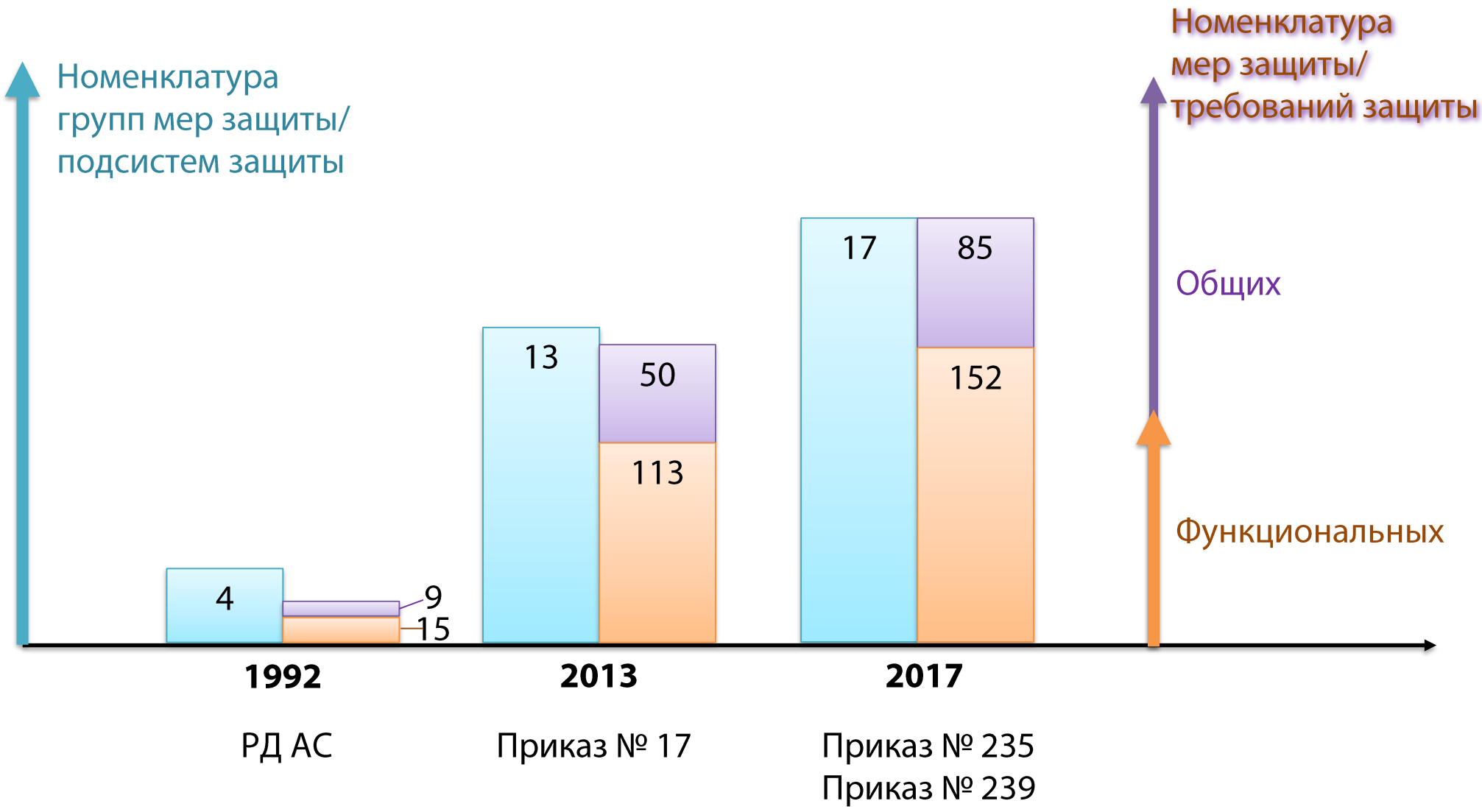
- ✓ государственныеорганы,
- ✓ государственные учреждения,
- ✓ российские ЮЛ,
- ✓ российские ИП

→ которым на праве собственности, аренды или на ином законном основании принадлежат ИС, ИТКС, АСУ, функционирующие в сферах (областях):

- **Металлургия**
- **Горнодобывающая отрасль**
- **Здравоохранение**
- **Топливно-энергетический комплекс**
- **Транспорт**
- **Наука**
- **Финансовая сфера**
- **Оборонная промышленность**
- **Ракетно-космическая область**
- **Химическая промышленность**
- **Связь**

→ которые обеспечивают взаимодействие объектов КИИ

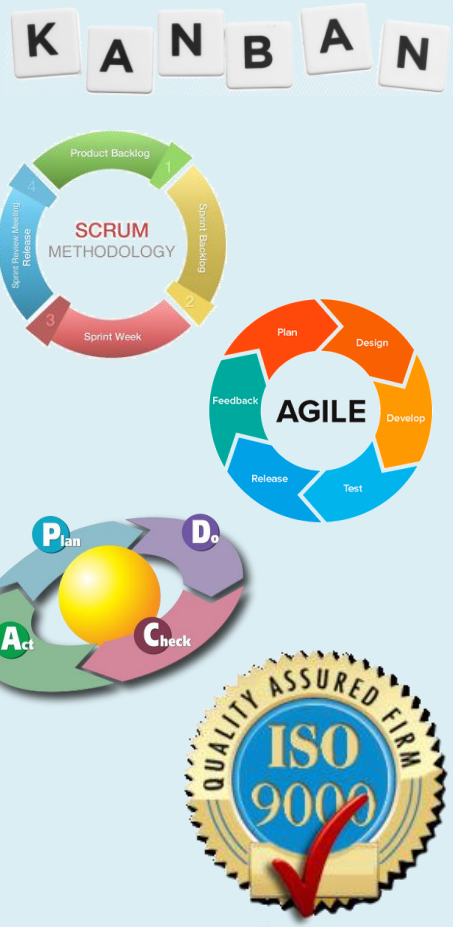
Рост номенклатуры требований безопасности информации



Лучшие практики ≈ Best Practice

Best Practices in…

Качество



Управление проектами

PRINCE2®

PMI®
PMBOK V5

PMAJ P2M

TOGAF®

Информационная безопасность

OSSTMM
www.osstmm.org
Open Source Security Testing Methodology Manual

OWASP
Open Web Application Security Project

ITIL®

PCI DSS COMPLIANT

NIST
National Institute of Standards and Technology
Information Technology Laboratory
800-115

Standard of Good Practice for Information Security

ISSAF
Information Systems Security Assessment Framework
www.oissg.org

Information Security Management System
ISO 27001
Certified

International Organization for Standardization
ISO 20000

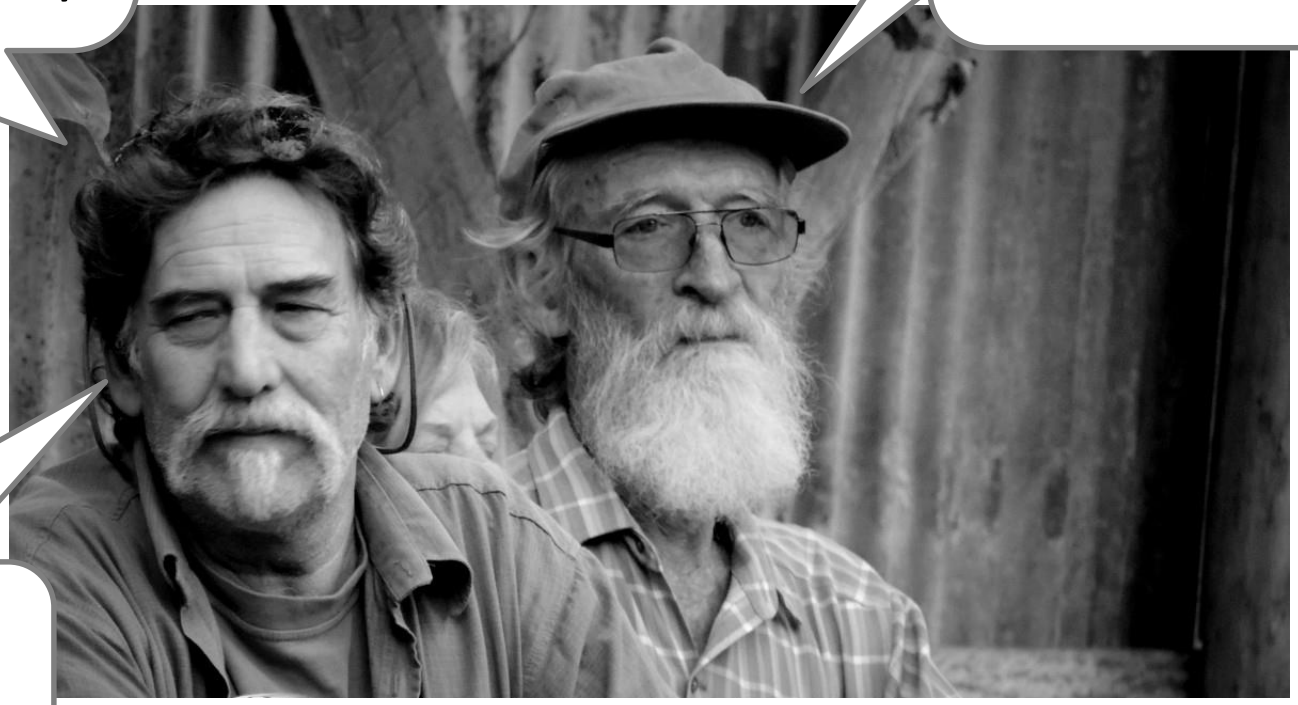
COBIT 5
AN ISACA® FRAMEWORK

PENETRATION TESTING EXECUTION STANDARD
PTES

Лучшие практики в России

У меня 20 лет успешного опыта ИБ – я за 20 минут выдам аттестат с горой доков на любую систему

А хватит ли Заказчику на это денег?



Нормально ж применяли СТР-К, чего началось-то?

Какие инциденты вынудили принять 187-ФЗ

Stuxnet
2010 год
Ядерный проект Ирана.
Более 1000 центрифуг.
Изменение параметров работы – переход в аварийный режим и поломке

NetTraveler
2013 год
Правительственные учреждения, военные организации, компании нефтегазового сектра.
Взлом баз данных. Шпионаж

Wiper
2012 год
Нефтяной терминал Ирана.
Уничтожение данных о всех нефтяных контрактах десятков нефтяных компаний

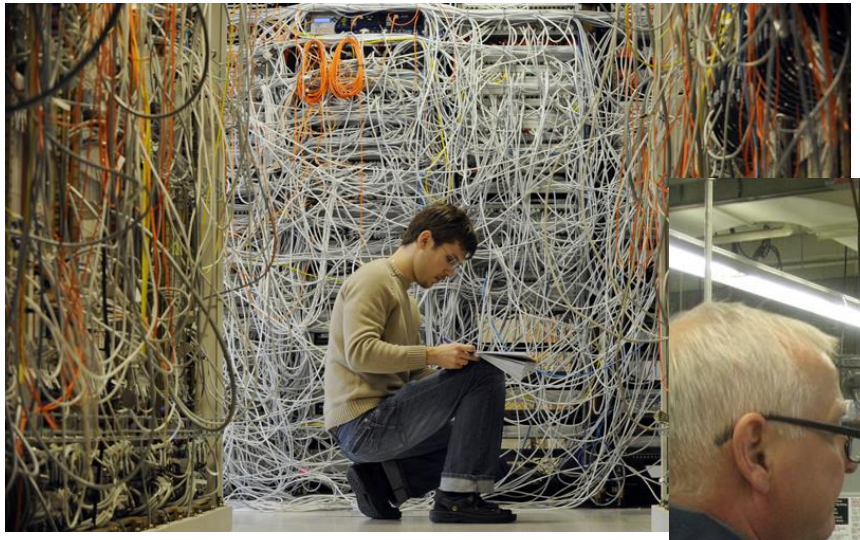
Icefog
2013 год
Правительственные организации, военные ведомства и компании, связанные с созданием вооружений, промышленные компании. Взлом баз данных

Что расследуют на предприятиях сейчас

Компьютерные инциденты на объектах КИИ

Примеры расследуемых инцидентов :

1. Вышел из строя сервер
2. Сломалась АСУ ТП станка с ЧПУ
3. Работник занёс флешку с вирусом-вымогателем



Система документов о КИИ на одном слайде

Указ № 620, 2017
О совершенствовании ГосСОПКА

Указ № 98, 2018
О засекречивании сведений о безопасности КИИ

ФЗ-187
О безопасности КИИ

ФЗ-193
О наделении полномочиями

ФЗ-194
Об определении ответственности

ПРАВИТЕЛЬСТВО РОССИЙСКОЙ ФЕДЕРАЦИИ

ПП-127
Правила категорирования

ПП-162
Правила госконтроля

П-ХХХ
О НКЦКИ

П-ХХХ
Требования к СОА

П-ХХХ
Порядок информирования

Временный порядок включения корпоративных центров в ГосСОПКА

ФСБ России

П-ХХХ
Информация для ГосСОПКА Порядок предоставления

П-ХХХ
Порядок и ТУ установки и эксплуатации СОА

ХХХ
Временный порядок включения в ГосСОПКА

Рекомендации №149/2/7-200 от 24.12.2016
Методические рекомендации по созданию ведомственных и корпоративных центров ГосСОПКА

ФСТЭК России

П-227
Порядок ведения реестра ЗО КИИ

П-229
Форма Акта проверки

П-235
Требования к созданию систем безопасности ЗО КИИ

П-239
Требования по обеспечению безопасности ЗО КИИ

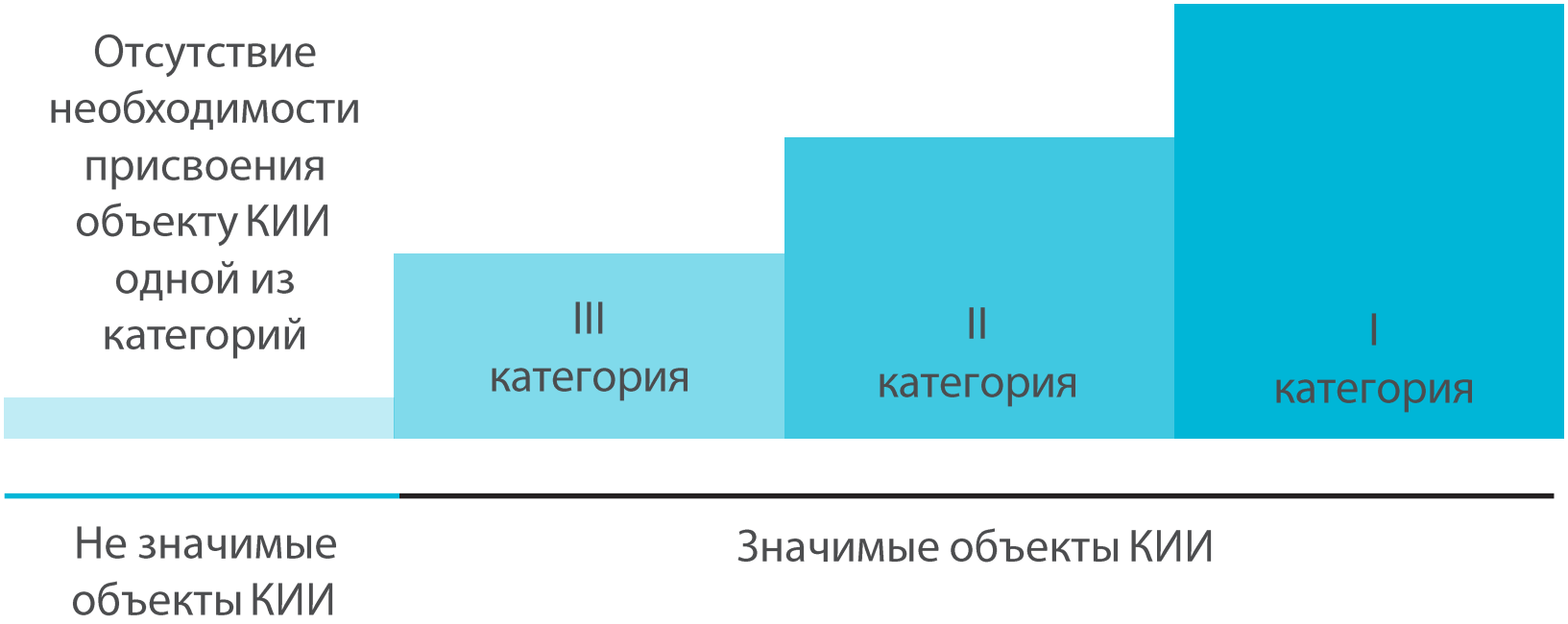
Минкомсвязи России

П-ХХХ
Порядок и ТУ установки и эксплуатации СОА в сетях связи

Значимые и незначимые объекты КИИ

Значимый объект КИИ – объект КИИ:

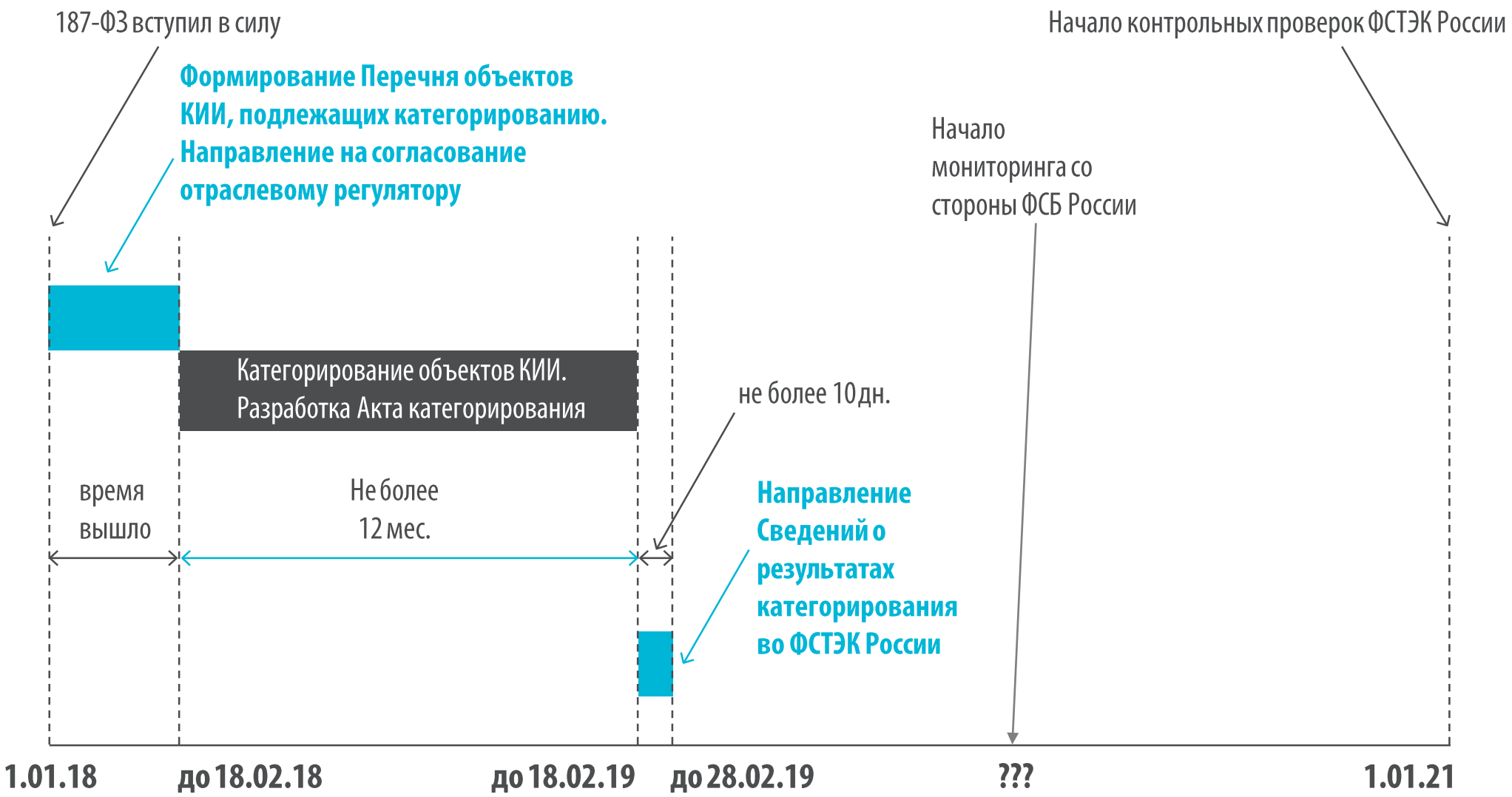
1. которому **присвоена** одна из категорий значимости
   и
2. который **включён** в реестр значимых объектов КИИ



Значимые объекты КИИ. Кто попадает в реестр?

Значимость объекта КИИ для	III категория	II категория	I категория
Социальная	Территория одного муниципального образования	Территория не более одного субъекта РФ	Территория более одного субъекта РФ
Политическая	Орган госвласти субъекта РФ или его договорённости	ФОИВ или его договорённости	Орган государственной власти РФ или его договорённости
Экономическая	Предельно малое недополучение РФ доходов от КИИ	Незначительное недополучение РФ доходов от КИИ	Малое недополучение РФ доходов от КИИ
Экологическая	Территория одного муниципального образования	Территория не более одного субъекта РФ	Территория более одного субъекта РФ
Для обеспечения обороны, безопасности и правопорядка	Предельно малый сдвиг сроков по Гособоронзаказу	Незначительный сдвиг сроков по Гособоронзаказу	Небольшой сдвиг сроков по Гособоронзаказу

Таймлайн по выполнению законодательства в области КИИ



Таймлайн по выполнению законодательства в области КИИ. Уточнения

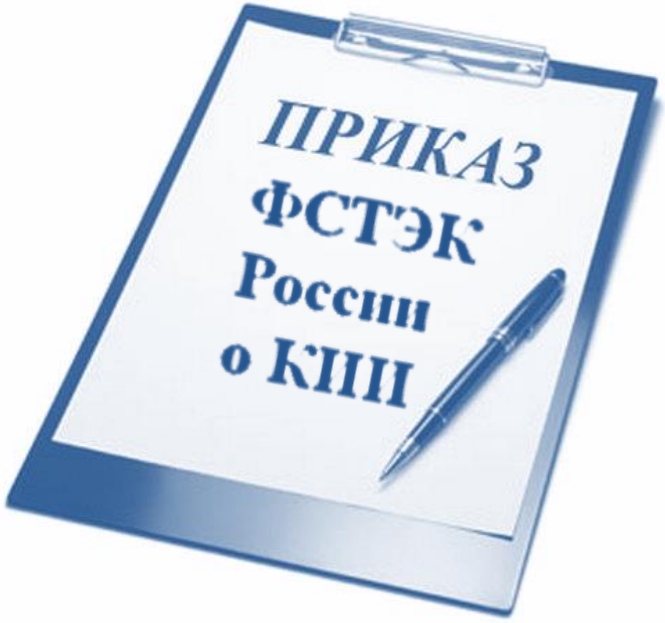
Форма направления сведений во ФСТЭК России:

1.Сведения об объекте КИИ: …, критические процессы, архитектура
2.Сведения о субъекте КИИ: …, лицо, на которое возложены функции обеспечения безопасности объектов, структурное подразделение или штатные специалисты, ответственные за обеспечение безопасности объектов
…
5. **Сведения о программных и программно-аппаратных средствах, используемых на объекте КИИ:** …, средства защиты информации
…

Что требует государство

"Если объект критической информационной инфраструктуры не соответствует критериям значимости, показателям этих критериев и их значениям, ему не присваивается ни одна из таких категорий"

"В качестве средств защиты информации в первую очередь подлежат рассмотрению механизмы защиты (параметры настройки) штатного программного обеспечения значимых объектов при их наличии"



Ответственность за нарушения законодательства о КИИ

Компьютерные инциденты на объектах КИИ

Федеральный закон от 26.07.2017 № 193-ФЗ

Федеральный закон от 26.07.2017 № 194-ФЗ

Сведения о мерах по обеспечению безопасности КИИ РФ и о состоянии ее защищенности от компьютерных атак – теперь ГТ

Разрешение проводить государственный контроль ЮЛ и ИП в области обеспечения безопасности значимых объектов КИИ РФ

Указ Президента РФ от 02.03.2018 N 98

119. Сведения, раскрывающие меры по обеспечению безопасности КИИ РФ. Сведения, раскрывающие состояние защищенности КИИ РФ от компьютерных атак

Ответственность за нарушения законодательства о КИИ

Компьютерные инциденты на объектах КИИ

Федеральный закон от 26.07.2017 № 193-ФЗ

Федеральный закон от 26.07.2017 № 194-ФЗ

Нарушение правил эксплуатации средств хранения/ обработки/ передачи информации, содержащейся в КИИ РФ, либо правил доступа к информации или объектам КИИ, если оно повлекло причинение вреда КИИ РФ,

Предварительное следствие производится следователями органов ФСБ России

«без отягчающих» лишение свободы до 6 лет с лишением права занимать определённые должности

«группой лиц по предварительному сговору/организованной группой/лицом с использованием своего служебного положения» лишение свободы от 3 до 8 лет с лишением права занимать определённые должности

«повлекли тяжкие последствия» лишение свободы от 5 до 10 лет с лишением права занимать определённые должности

Схема #1 «***генеральный директор, год через три***»

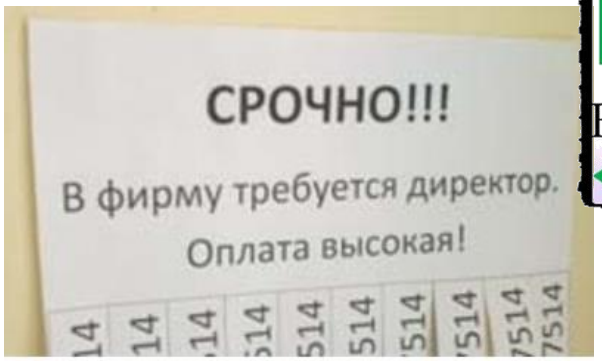


График выхода
директоров на работу

1.01.2020-31.12.2020	Директор #1
1.01.2021-31.12.2021	Директор #2
1.01.2022-31.12.2022	Директор #3
~~1.01.2023-31.12.2023~~	~~Директор #1~~

...

См. 194ФЗ

Схема #2 «Divide et impera»[1]

Значимый объект

Много незначимых объектов

[1] *Разделяй и властвуй*

Схема #3 «*применение лучших практик*»

Качество

Управление проектами

PRINCE2®

PMI®
PMBOK V5

PMAJ P2M

TOGAF®

Информационная безопасность

ITIL®

PCI DSS COMPLIANT

ISF Standard of Good Practice for Information Security

Information Security Management System
ISO 27001 Certified

International Organization for Standardization
ISO 20000

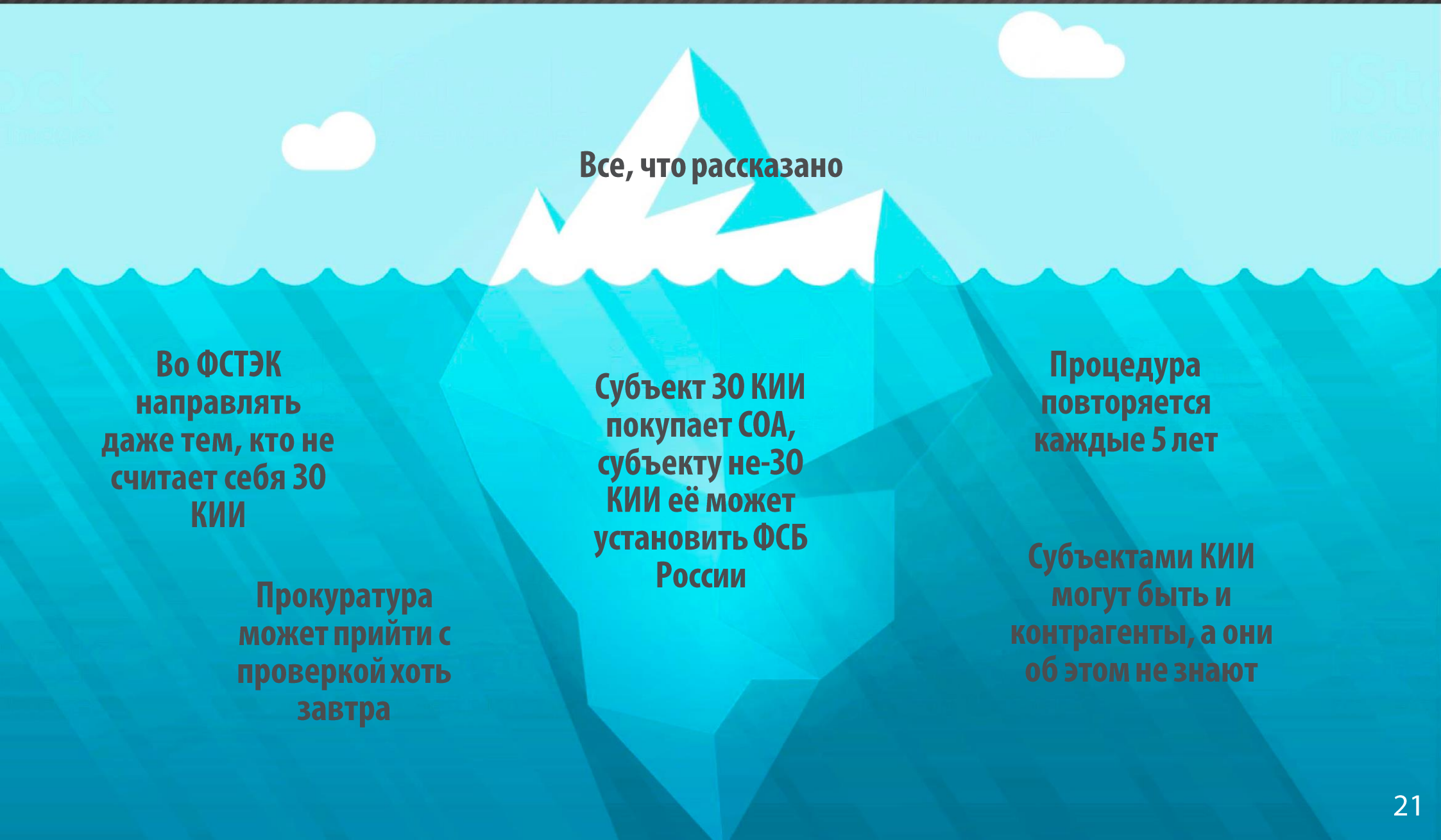
COBIT® 5
AN ISACA® FRAMEWORK

Приказ № 17 + **СМИБ** ≈ **Приказ № 239**

Схема #4 «Vis unita fortior»

[1] *Объединённые силы мощнее*

Что «осталось за кадром»



SAVE IT group

Официальный telegram-канал

CyberSecurityRussia

Мы можем всё

Технический директор

Департамента защиты информационных систем

Владимир Минаков

@Vladimir_Minakov

minakov_v@saveit.pro

@v_a_minakov

+7 (800) 250-87-34

info@saveit.pro