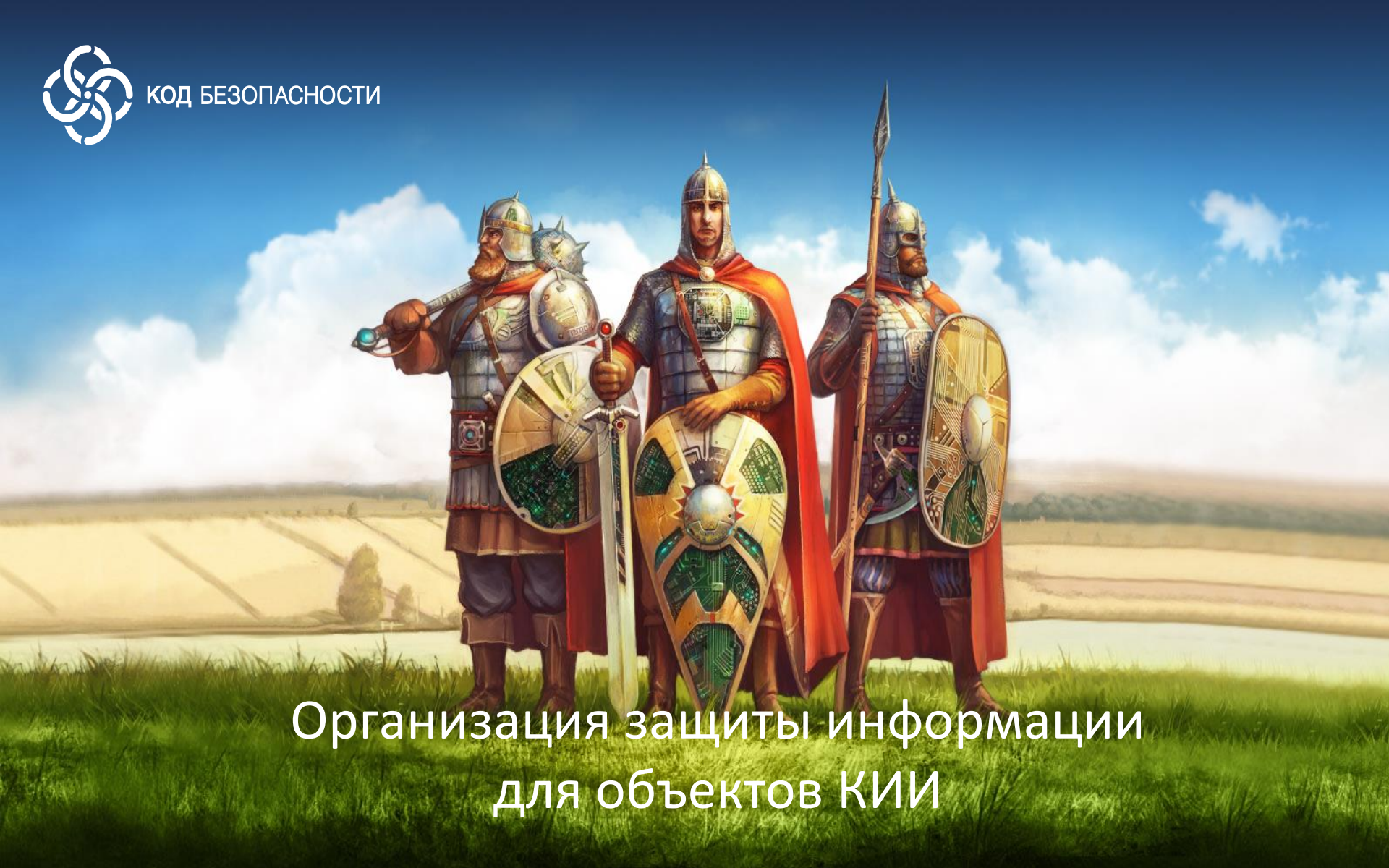
КОД БЕЗОПАСНОСТИ



Организация защиты информации для объектов КИИ

Поговорим о…

- Про что будем говорить
  - Почему КИИ именно сейчас
  - Плюсы/минусы
  - Создание системы защиты объектов КИИ
  - Использование продуктов «Кода Безопасности» в рамках системы защиты объектов КИИ
  - Что же дальше

ФЗ-187 «КИИ»

Подписан Закон о безопасности критической информационной инфраструктуры России.
Он регулирует отношения в области обеспечения безопасности критической информационной инфраструктуры в целях ее устойчивого функционирования при проведении в отношении ее компьютерных атак.

Документ определяет основные понятия в этой сфере: «автоматизированная система управления», «безопасность критической информационной инфраструктуры», «значимый объект критической информационной инфраструктуры», «компьютерная атака», «компьютерный инцидент», «критическая информационная инфраструктура», «объекты критической информационной инфраструктуры» и «субъекты критической информационной инфраструктуры».

ФЕДЕРАЛЬНЫЙ ЗАКОН ОТ 26 ИЮЛЯ 2017 Г. N 187-ФЗ "О БЕЗОПАСНОСТИ КРИТИЧЕСКОЙ ИНФОРМАЦИОННОЙ ИНФРАСТРУКТУРЫ РОССИЙСКОЙ ФЕДЕРАЦИИ"

КОД БЕЗОПАСНОСТИ

Перечень нормативных актов

Уже есть:

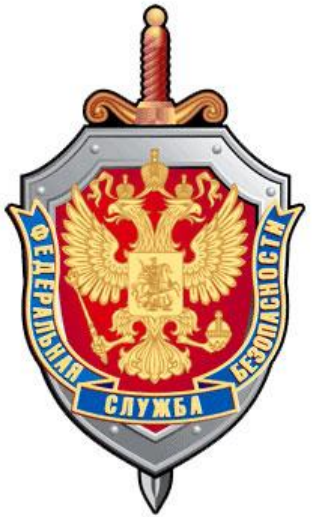
- Закон №187-ФЗ от 26.07.2017 «О безопасности критической информационной инфраструктуры Российской Федерации»
- УК РФ ст. 274.1 «Неправомерное воздействие на критическую информационную инфраструктуру Российской Федерации»
    - Ч.3 Нарушение правил эксплуатации…
- Постановление правительства №127-ПП от 08.02.2018 «Об утверждении правил категорирования…»
- Приказы ФСТЭК
    - Приказ № 235 от 21.12.2017 «Об утверждении требований к созданию систем безопасности значимых объектов КИИ и обеспечению их функционирования»
    - Приказ №236 от 22.12.2017 «Об утверждении формы направления сведений…»
    - Приказ №239 от 25.12.2017 «Об утверждении требований по обеспечению безопасности значимых объектов КИИ РФ»

ВЕРХНЕУРОВНЕВО

Определяются полномочия государственных органов РФ в области обеспечения ее безопасности, а также права и обязанности субъектов критической информационной инфраструктуры.

Федеральный орган исполнительной власти, уполномоченный в области обеспечения безопасности критической информационной инфраструктуры Российской Федерации

Федеральный орган исполнительной власти, уполномоченный в области обеспечения функционирования государственной системы обнаружения, предупреждения и ликвидации последствий компьютерных атак на информационные ресурсы Российской Федерации.



КОД БЕЗОПАСНОСТИ

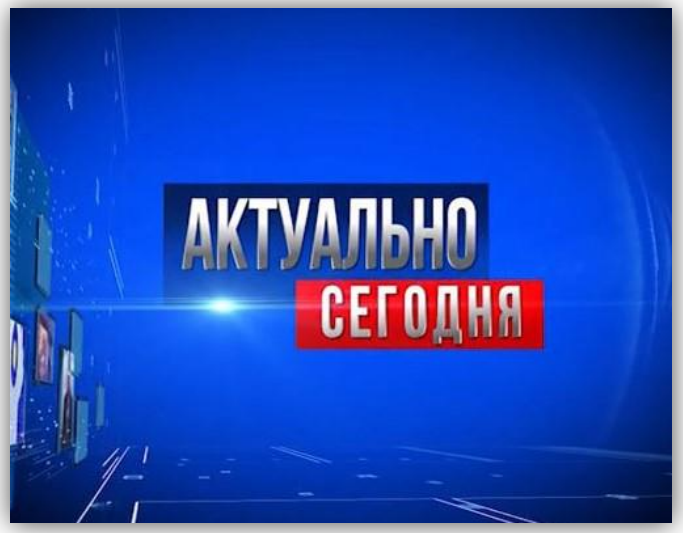
ОБ ОТВЕТСТВЕННОСТИ...

Действия субъекта КИИ	Результат действий атакующего	Ответственность
Не защитили объект КИИ	Не жахнуло	Если попадает по критериям – обязанность защитить объект
Не защитили объект КИИ	Жахнуло	274.1 ч.3 «Нарушение правил эксплуатации средств хранения», **до 6 лет лишения свободы** ответственному должностному лицу субъекта КИИ
Защитили объект КИИ	Не жахнуло	
Защитили объект КИИ	Жахнуло	274.1 ч.1 «Создание вредоносного ПО для неправомерного воздействия на КИИ», **до 5 лет лишения свободы** злоумышленнику 274.1 ч.2 «Несанкционированный доступ к информации в КИИ, если он повлек причинение вреда КИИ РФ», **до 6 лет лишения свободы** злоумышленнику

КОД БЕЗОПАСНОСТИ

Что нового?

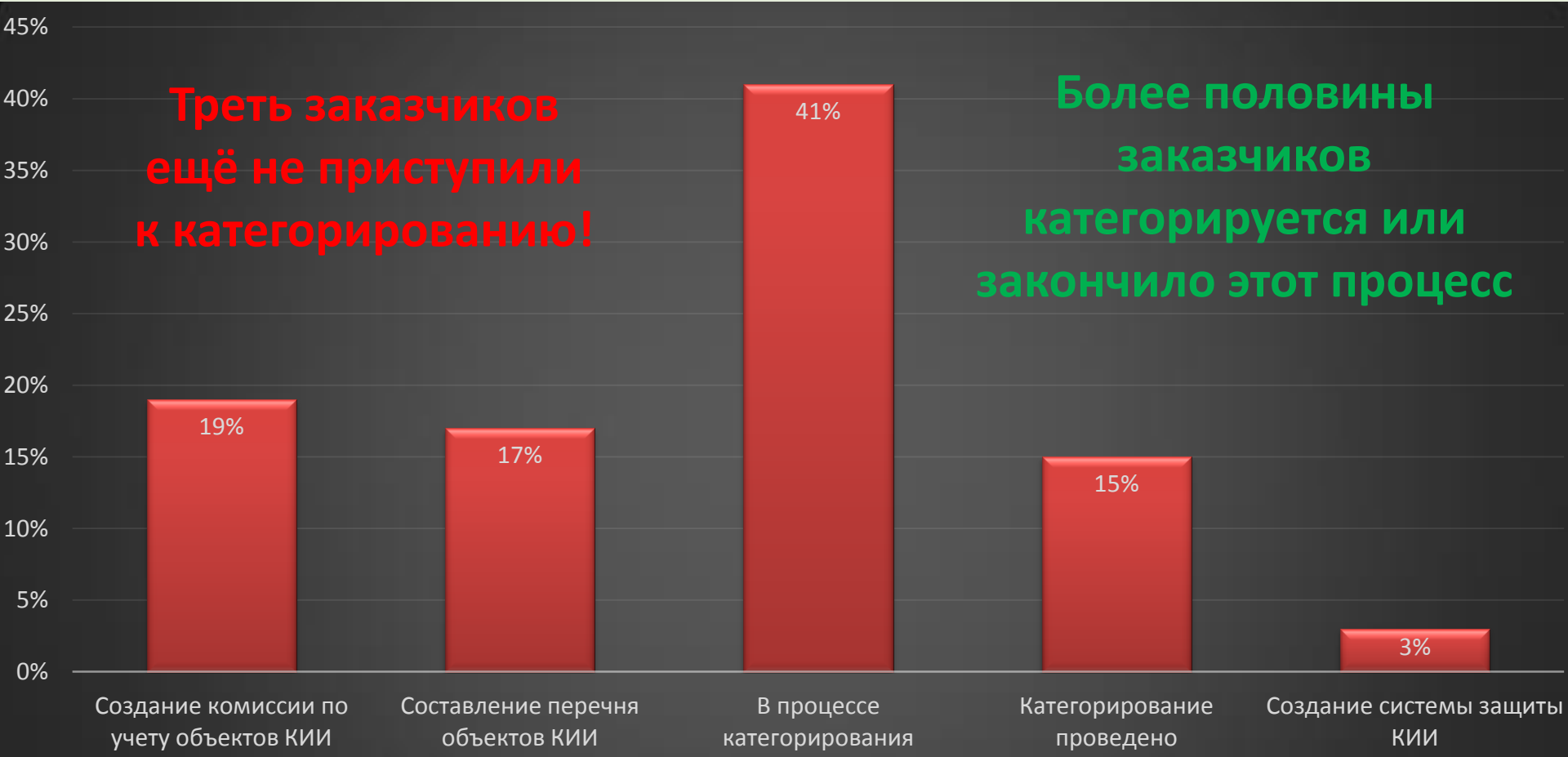
- В декабре 2018 ФСТЭК представил проект поправок в постановление №127-ПП (регулирует процесс категорирования:
  - Новый дедлайн по направлению перечня объектов КИИ – 1 июня 2019 года
  - Снижение порога значимости:
    - Для объектов жизнедеятельности, транспорта или объектов негативно влияющих на окружающую среду **с 50-ти до 2-х тысяч человек**, задетых инцидентом
    - Для объектов связи **с 50-ти до 3-х тысяч человек**, задетых инцидентом
    - Для государственных организаций и компаний госучастием **с 5% до 1% ущерба от годовой выручки**
  - **Необходимость проводить категорирование заново при изменении критериев**



- Ожидаем новых административных наказаний за несвоевременное категорирование и невыполнение других требований законодательства по КИИ

КОД БЕЗОПАСНОСТИ

Стадии выполнения законодательства в области защиты КИИ



Субъекты КИИ

КОД БЕЗОПАСНОСТИ

КОД БЕЗОПАСНОСТИ

Субъект КИИ

Организация с информационной системой, которая относится к одной из этих отраслей

или

Организация из этих отраслей

или

Организация обеспечивающая взаимодействие этих систем или сетей

- Промышленность:
  - Атомная
  - Ракетно-космическая
  - Горнодобывающая
  - Металлургическая
  - Химическая промышленность
  - Оборонная промышленность
- Предприятия ТЭК
- Энергетика
- Учреждения здравоохранения
- Научные организации
- Транспортные организации
- Связь
- Финансовые организации

№187-ФЗ ст. 2 п.8

Критичные процессы и объекты

Объекты КИИ

- Обрабатывают информацию для обеспечения критических процессов
- Осуществляют управление и контроль критических процессов
- Осуществляют мониторинг критических процессов

Категорирование

- Сведения об объекте
- Критичные процессы
- Состав обрабатываемой информации
- Декларация безопасности и паспорт объекта ТЭК (если применимо)
- Сведения о взаимодействии с другими объектами КИИ или зависимости от других объектов КИИ
- Угрозы безопасности информации и статистика по инцидентам на объектах этого типа

КОД БЕЗОПАСНОСТИ

Процесс категорирования

- Определение критических процессов
- Выявление процессов попадающих на критерии значимости
- Определение объектов КИИ реализующих эти процессы **> Отраслевой регулятор (возможно) -> ФСТЭК**
- Определение категорий объектов КИИ **-> ФСТЭК**

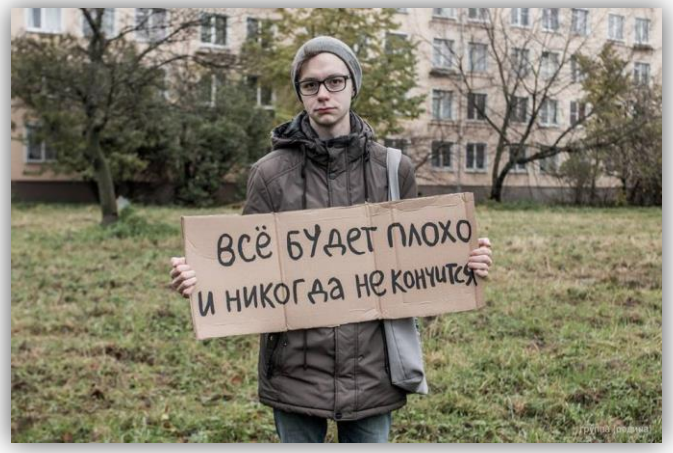
Системы безопасности КИИ

- Силы
  - Подразделение по защите ОКИИ
    - Могут защищать и другую инфраструктуру
    - Совмещать защиту и ИТ – нет!
  - Подразделение эксплуатирующее ОКИИ
  - Подразделение обслуживающее ОКИИ
- Средства
  - Межсетевые экраны
  - СЗИ от НСД
  - Средства обнаружения вторжений
  - Средства антивирусной защиты
  - Средства защиты каналов связи
  - Средства контроля защищенности
  - Средства управления событиями безопасности

Приказ ФСТЭК №235

КОД БЕЗОПАСНОСТИ

А ВСЁ ЛИ ТАК ПЛОХО?



Сам закон, как и его выполнение, очень обеспокоили российские организации в части его исполнения.

Есть понимание того, что надо потратить много денег без видимости реальной ценности мер по защите данных инфраструктур…

Введена уголовная ответственность за действия, направленные против субъекта КИИ. Но пострадать может и сам субъект. Если не защитится…

КОД БЕЗОПАСНОСТИ

Выбор мер защиты

Определение базового набора мер защиты на основе категории значимости

Адаптация с учетом особенностей работы объекта КИИ

Дополнение мерами для выполнения других документов (17/21/31 приказ)

Приказ ФСТЭК №239

Средства защиты

КОД БЕЗОПАСНОСТИ

КОД БЕЗОПАСНОСТИ

Что точно потребуется для защиты КИИ

Что потребуется для защиты	Что мы можем предложить
СЗИ от НСД	**Secret Net Studio (АРМ), vGate (виртуализация), Secret MDM (мобильные устройства)**
Межсетевой экран	**АПКШ «Континент» (сеть), Secret Net Studio (АРМ)**
Средство обнаружения вторжений	**АПКШ «Континент» (сеть), Secret Net Studio (АРМ)**
Средства антивирусной защиты	**Secret Net Studio**
Средства контроля защищенности	---
Средства управления событиями безопасности	---
Средства защиты каналов передачи данных	**АПКШ «Континент»**

Ст .17 приказа ФСТЭК России №235 «Об утверждении Требований к созданию систем безопасности значимых объектов КИИ РФ и обеспечению их функционирования»

Спасибо за внимание!

Горохов Леонид
Тел: +7 (495) 980-2345 доб. 580
l.gorokhov@securitycode.ru

info@securitycode.ru
http://securitycode.ru

КОД БЕЗОПАСНОСТИ