ANGARA SECURITY

Категорирование ОКИИ — разбор на примере «слона»

Александр Хонин
Руководитель Отдела консалтинга и аудита

Основные вопросы при категорировании

Как выделить объекты КИИ?

Что должны включать в себя объекты КИИ?

Как определить категорию значимости?

Как правильно заполнить все пункты 236 формы?

...

Категорирование объектов КИИ

Как задача ◄·····► Как проект

Основные этапы категорирования

Начало работ

- Приказ о создании комиссии
- Положение о комиссии

Сбор исходных данных

- Перечень процессов
- Перечень объектов КИИ
- Информация по объектам КИИ
- Информация по угрозам безопасности
- Состав информации, обрабатываемой на объектах КИИ
- Информация по компьютерным инцидентам

Категорирование

Проекты «Актов категорирования объектов КИИ»

Подготовка и отправка сведений

Заполненные формы подачи сведений о присвоении категории значимости объектам КИИ

Сбор исходных данных

01 Методика категорирования

02 Определение критических процессов

03 Описание ИС / АСУ / ИТКС

04 Формирование перечня объектов КИИ

05 Предварительное определение категории значимости ОКИИ

Сбор исходных данных

01 Методика категорирования

- Общая методика категорирования
- Определение применимых показателей критериев значимости объектов КИИ
- Методика оценки масштаба возможных последствий

02 Определение критических процессов

- Общий перечень процессов
- Перечень критических процессов

Сбор исходных данных

03 Описание ИС / АСУ / ИТКС

- Функциональное назначение системы
- Состав обрабатываемой информации
- Месторасположение компонентов ИС
- Архитектура, состав оборудования и ПО
- Описание взаимодействий
- Меры защиты информации
- Сведения об угрозах безопасности информации и инцидентах ИБ

04 Формирование перечня объектов КИИ

- Описание методики и принципов выделения объектов КИИ
- Предложения по логическому структурированию
- Перечень объектов КИИ

Сбор исходных данных

05 Предварительное категорирование объектов КИИ

- Оценка масштаба последствий
- Определение категории значимости для объекта КИИ

Акт категорирования объекта КИИ

Промежуточные результаты

Сбор исходных данных

1. Описание объектов КИИ
2. Перечень объектов КИИ

Акт категорирования объекта КИИ

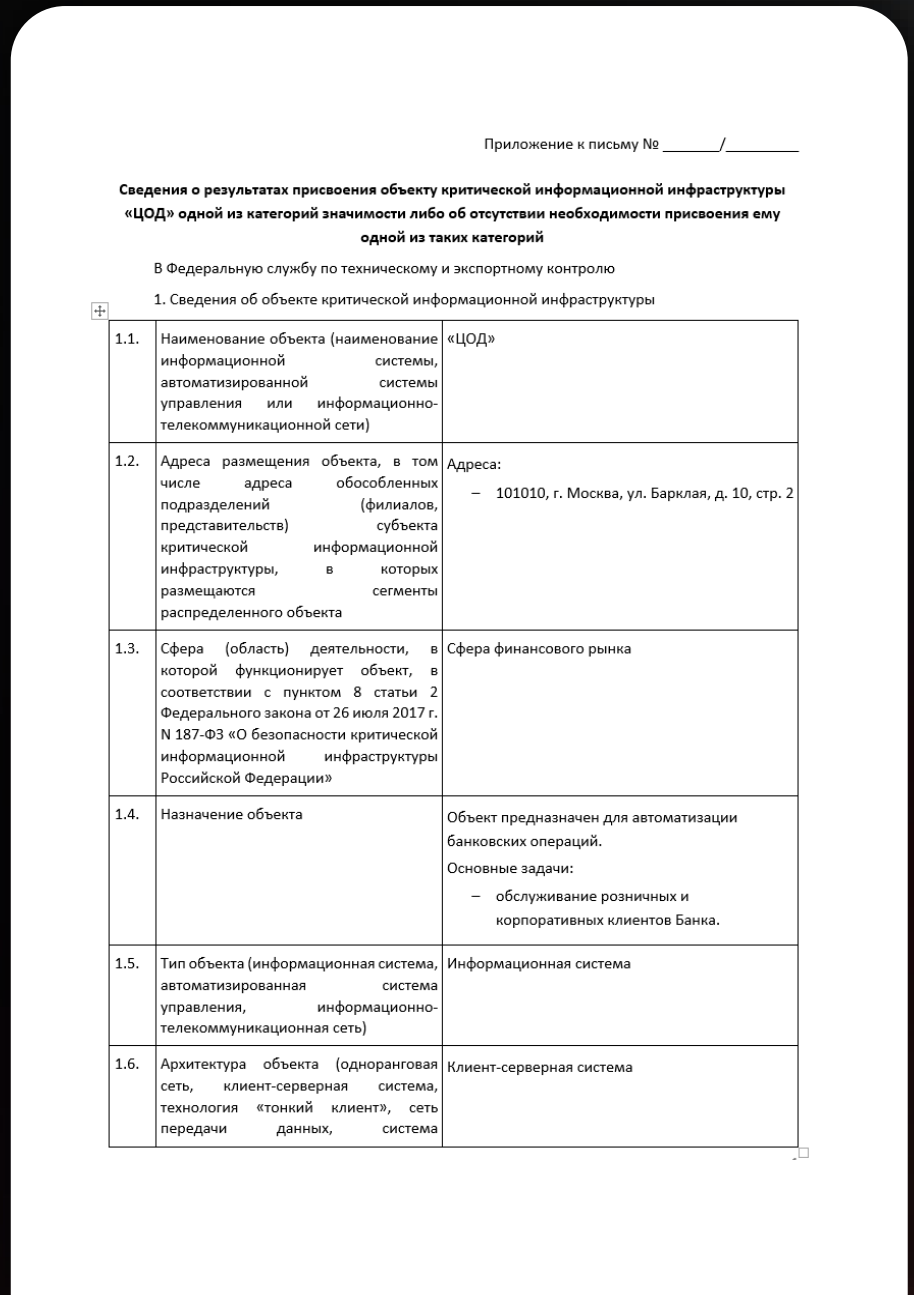
Результаты категорирования

Оценка масштаба последствий

Сведения об объекте КИИ

Сведения по результатам категорирования

- ☑ Бумажный формат
- ☑ Формат .ods



Приложение к письму № _____/_____

Сведения о результатах присвоения объекту критической информационной инфраструктуры «ЦОД» одной из категорий значимости либо об отсутствии необходимости присвоения ему одной из таких категорий

В Федеральную службу по техническому и экспортному контролю

1. Сведения об объекте критической информационной инфраструктуры

1.1.	Наименование объекта (наименование информационной системы, автоматизированной системы управления или информационно-телекоммуникационной сети)	«ЦОД»
1.2.	Адреса размещения объекта, в том числе адреса обособленных подразделений (филиалов, представительств) субъекта критической информационной инфраструктуры, в которых размещаются сегменты распределенного объекта	Адреса: – 101010, г. Москва, ул. Барклая, д. 10, стр. 2
1.3.	Сфера (область) деятельности, в которой функционирует объект, в соответствии с пунктом 8 статьи 2 Федерального закона от 26 июля 2017 г. N 187-ФЗ «О безопасности критической информационной инфраструктуры Российской Федерации»	Сфера финансового рынка
1.4.	Назначение объекта	Объект предназначен для автоматизации банковских операций. Основные задачи: – обслуживание розничных и корпоративных клиентов Банка.
1.5.	Тип объекта (информационная система, автоматизированная система управления, информационно-телекоммуникационная сеть)	Информационная система
1.6.	Архитектура объекта (одноранговая сеть, клиент-серверная система, технология «тонкий клиент», сеть передачи данных, система	Клиент-серверная система

На что обратить внимание

- Оформление акта категорирования и сведений по результатам категорирования
- Обоснование неприменимости показателей критериев значимости
- Оценка масштаба последствий
- Наименование программно-аппаратных средств и ПО
- Перечень угроз безопасности ≠ Модель угроз
- Технические меры по ИБ

Категорирование объектов КИИ

Что выбрать?

- Как задача
- Как проект

ANGARA
SECURITY

Спасибо!
Вопросы?

www.angarasecurity.ru
+7 (495) 269-26-06
121096, г. Москва,
ул. Василисы Кожиной, д.1,к.1
БЦ «Парк Победы»