НПП “Гамма”

Защита критической информационной инфраструктуры и персональных данных в медицинских учреждениях

Марков Сергей

Начальник отдела системных проектов

Санкт-Петербургский НТЦ ФГУП «НПП «Гамма»

Тел.: +7 (921)3724674

e-mail: markov@spb.nppgamma.ru

10.03.2020

НПП “Гамма”

1. Зачем защищать?
2. Что защищать?
3. Как защищать?

Зачем защищать

НПП “Гамма”

Каждый год пополняется перечень уязвимостей в различных ИТ. Вместе с ним растёт и количество методов атак на информационные системы.

Эти уязвимости напрямую влияют на защищённость информационных активов: злоумышленники могут нанести ощутимый вред организации, похитить критичные данные. Современная и правильно сконструированная ИБ позволит оценить эффективность применяемых средств и мер защиты информации и выработать рекомендации по их модернизации, если будут обнаружены уязвимости или недостаточность защитных функций. Позволит предотвратить ущерб.

SANS 2019 Threat Landscape Survey

Угроза реальна!

НПП "Гамма"

U.S. Revives Secret Program to Sabotage Iranian Missiles and Rockets - The New York Times - Mozilla Firefox

WebMail :: Входящие | Colonel Cassad | Новая вкладка | New York Times feb iran ba | U.S. Revives Secret Progran | Google | Google Переводчик

https://www.nytimes.com/2019/02/13/us/politics/iran-missile-launch-failures.html

переводчик

The New York Times

POLITICS | U.S. Revives Secret Program to Sabotage Iranian Missiles and Rockets

192

Long-range missiles on display this month in Tehran. This year marks the 40th anniversary of the Islamic Revolution.
Arash Khamooshi for The New York Times

By David E. Sanger and William J. Broad

Feb. 13, 2019

192

WARSAW — The Trump White House has accelerated a secret American program to sabotage Iran's missiles and rockets, according to current and former administration officials, who described it as part of an expanding campaign by the United States to undercut Tehran's military and isolate its economy.

Officials said it was impossible to measure precisely the success of the classified program, which has never been publicly acknowledged. But in the past month alone, two Iranian attempts to launch satellites have failed within minutes.

Those two rocket failures — one that Iran announced on Jan. 15 and the other, an unacknowledged attempt, on Feb. 5 — were part of a pattern over the past 11 years. In that time, 67 percent of Iranian orbital launches have failed, an astonishingly high number compared to a 5 percent failure rate worldwide for similar space launches.

The setbacks have not deterred Iran. This week, President Hassan Rouhani singled out Tehran's missile fleets as he vowed to "continue our path and our military power."

11-ти летняя работа ЦРУ и АНБ по внедрению в управление и технологические процессы ракетных программ Ирана. Результат – 67% неудачных пусков

U.S. Revives S...

EN 10:24 Ср, 29 май

Baltimore government held hostage by hackers' ransomware

23 May 2019 Share

ALEX WROBLEWSKI/GETTY IMAGES

Baltimore's government servers have been attacked by ransomware

The US city of Baltimore's government, long plagued by dysfunction, is now battling a ransomware attack that has crippled its systems for more than two weeks and counting.

Hackers breached the Maryland city's servers on 7 May and demanded $100,000 (£79,000) worth of Bitcoin.

The ransomware has blocked government email accounts and disabled online payments to city departments.

Baltimore city officials have so far refused to pay the ransom.

It is the second cyber-attack to strike the city in as many years - the last one knocked out its emergency dispatch system for about a day.

НПП "Гамма"

Информационная система Балтимора в результате атаки хакеров полностью выведена из строя.
Не принимаются местные платежи, не могут работать городские службы, не выплачиваются пенсии и пособия.
Злоумышленники требуют выплаты 100000$ криптовалютой. Поиски преступников пока безуспешны.
На протяжении месяца системы полностью восстановить не удалось.

The City of Baltimore is currently unable to send or receive email. If you need assistance, please call the department you wish to contact.

Click here for information on Baltimore city services / contact numbers.

Click here for Lien Affidavit For Payment of Outstanding Charges

Инциденты в сфере здравоохранения

- **Известный госпиталь в городе Мумбаи, Индия, стал жертвой нападения хакеров-вымогателей. Киберпреступники зашифровали данные больницы и для возврата контроля над документами требуют выкуп в биткойнах.**
- Представители больницы Махатма Ганди (MGM) в Мумбаи подтвердили, что госпиталь стал жертвой вируса-шифровальщика и потерял контроль над своей компьютерной системой управления 15 июля. Атака была зафиксирована системным администратором MGM, после попытки подключения к базе данных медицинской системы с помощью удаленного доступа.

НПП “Гамма”

Инциденты в сфере здравоохранения

- **Хакеры организовали атаку на компьютерные системы Федерального центра нейрохирургии в Тюмени в момент серьезной операции. Об этом в ходе международного конгресса по кибербезопасности рассказал глава Сбербанка Герман Греф, сообщает ТАСС.**

Злоумышленники взломали компьютеры и приборы с помощью вируса-вымогателя под названием Пурген. По личной просьбе Суфианова специалисты по кибербезопасности посетили центр нейрохирургии и восстановили данные, вернув компьютерные системы к жизни.

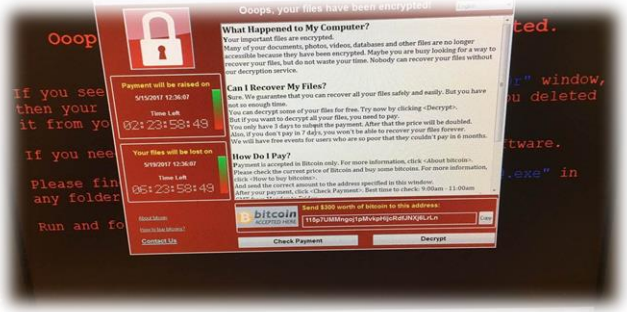
По его словам, инцидент произошел во время сложной операции на головном мозге 13-летней пациентки. В процессе оперативного вмешательства медицинские приборы оказались отключены из-за взлома. Главный врач центра Альберт Суфианов сумел закончить операцию, не опираясь на электронные показатели.

НПП “Гамма”

Инциденты в сфере здравоохранения

Больницы в Англии пострадали от крупномасштабной хакерской атаки. Вирус атаковал внутренние компьютерные системы медицинских учреждений, а за восстановление работы злоумышленники потребовали заплатить выкуп.

Доктора практически в одно и то же время сообщили в соцсетях о техническом сбое в ряде больниц. По словам врачей, они массово получили сообщения о переходе компьютеров под контроль хакеров и с требованием выкупа в размере 300 долларов в обмен на восстановление доступа.



В Департаменте здравоохранения Великобритании подтвердили факт атаки хакеров и пообещали детально рассказать о проблеме позже. Врачи сообщили, что вместе с отсутствием доступа к компьютерам потеряли возможность узнать о записях пациентов, рецептах и результатах анализов.

Больницы временно перестали принимать пациентов, сделав исключение только для неотложных случаев.

НПП “Гамма”

Что защищать

Субъекты КИИ и объекты КИИ

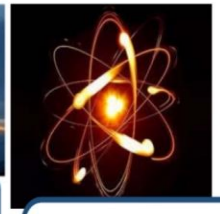
субъект


Сфера здравоохранения


Сфера науки


Сфера транспорта


Сфера связи


Область атомной энергии


Область оборонной промышленности


Область ракетно-космической промышленности


Область горнодобывающей промышленности


Сфера энергетики

Банковская и иные сферы финансового рынка


Сфера ТЭК


Область химической промышленности


Область металлургической промышленности

объекты КИИ –
[ВСЕ!] ИС, ИТКС, АСУ субъектов КИИ

НПП “Гамма”

Информационная система как объект КИИ в сфере здравоохранения?

В соответствии с п.1 ст.91 Федерального закона от 21.11.2011 № 323-ФЗ «Об основах охраны здоровья граждан в Российской Федерации» под информационными системами в сфере здравоохранения понимается:

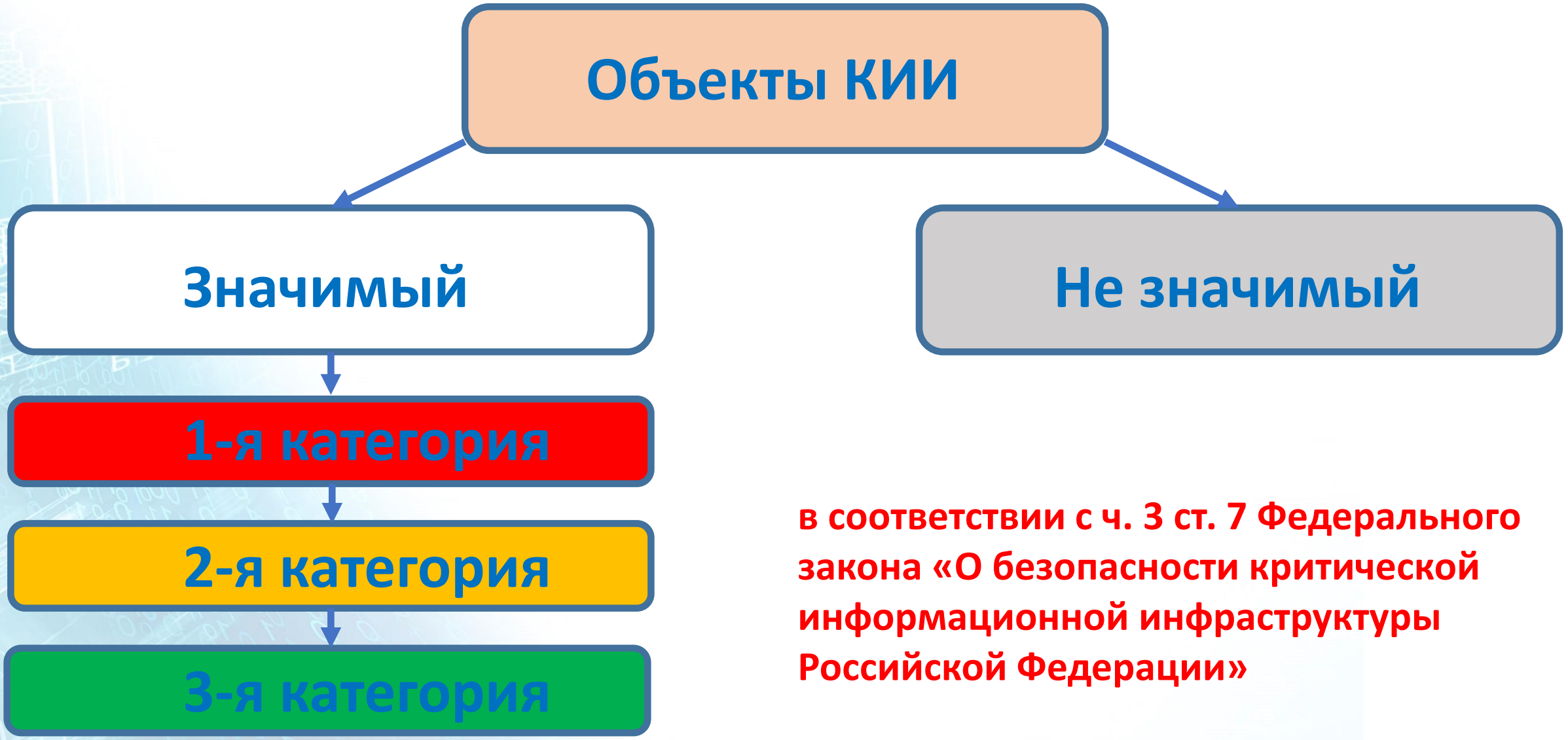
- федеральные государственные информационные системы в сфере здравоохранения;
- информационные системы в сфере здравоохранения Федерального фонда обязательного медицинского страхования и территориальных фондов обязательного медицинского страхования;
- государственные информационные системы в сфере здравоохранения субъектов Российской Федерации;
- медицинские информационные системы медицинских организаций;
- информационные системы фармацевтических организаций.
- Согласно определению, данному в методических рекомендациях по обеспечению функциональных возможностей медицинских информационных систем медицинских организаций (МИС МО) (утв. Министерством здравоохранения РФ 1 февраля 2016 г.) медицинская информационная система медицинской организации обозначается как «интегрированная или комплексная информационная система, предназначенная для автоматизации лечебно-диагностического процесса и сопутствующей медицинской деятельности медицинской организации».

Дорожная карта

НПП "Гамма"

Есть ли значимые?

НПП “Гамма”



в соответствии с ч. 3 ст. 7 Федерального закона «О безопасности критической информационной инфраструктуры Российской Федерации»

НПП “Гамма”

Содержание процедуры категорирования ОКИИ

- **1 шаг**: Определение процессов в рамках выполнения функций (полномочий) или осуществления видов деятельности субъекта КИИ
- **2 шаг**: Выявление критических процессов
- **3 шаг**: Определение ОКИИ
- **4 шаг**: Формирование перечня ОКИИ
- **5 шаг**: Оценка в соответствии с перечнем показателей критериев значимости масштаба возможных последствий в случае возникновения компьютерных инцидентов на ОКИИ
- **6 шаг**: Присвоение или не присвоение категории ОКИИ (*оформление акта и заполнение 236формы*):
- Значимые ОКИИ: I категории, II категории, III категории
- Незначимые ОКИИ

НПП “Гамма”

Участники процедуры категорирования ОКИИ

- Постоянно действующая комиссия по категорированию (п.11 Правил, утв. ПП РФ № 127):
- руководитель субъекта КИИ или уполномоченное им лицо
- специалисты в области выполняемых функций или осуществляемых видов деятельности
- специалисты в области информационных технологий и связи
- специалисты по эксплуатации основного технологического оборудования
- специалисты по технологической (промышленной) безопасности
- специалисты по контролю за опасными веществами и материалами, учету опасных веществ и материалов
- специалисты, на которых возложены функции обеспечения безопасности (ИБ) ОКИИ
- специалисты подразделения по защите государственной тайны субъекта КИИ*
- работники структурного подразделения по гражданской обороне и защите от чрезвычайных ситуаций или работники, уполномоченные на решение задач в области гражданской обороны и защиты от чрезвычайных ситуаций (*согласно Положению, утв. ПП РФ № 782*)

* Если ОКИИ обрабатывает информацию, составляющую государственную тайну

НПП “Гамма”

- «*По решению руководителя субъекта критической информационной инфраструктуры в состав комиссии могут быть включены работники не указанных в пункте 11 настоящих Правил подразделений, в том числе финансово-экономического подразделения*» (п.11(1) Правил, утв. ПП РФ № 127)
- «*В состав комиссии по категорированию могут включаться представители государственных органов и российских юридических лиц, выполняющих функции по разработке, проведению или реализации государственной политики и (или) нормативно-правовому регулированию в установленной сфере деятельности, по согласованию с государственными органами и российскими юридическими лицами*» (п.2 Правил, утв. ПП РФ № 127)

- Иные специалисты в постоянно действующей комиссии по категорированию:
- специалисты в области экономического учета
- специалисты в области налогового учета
- специалисты в области юриспруденции

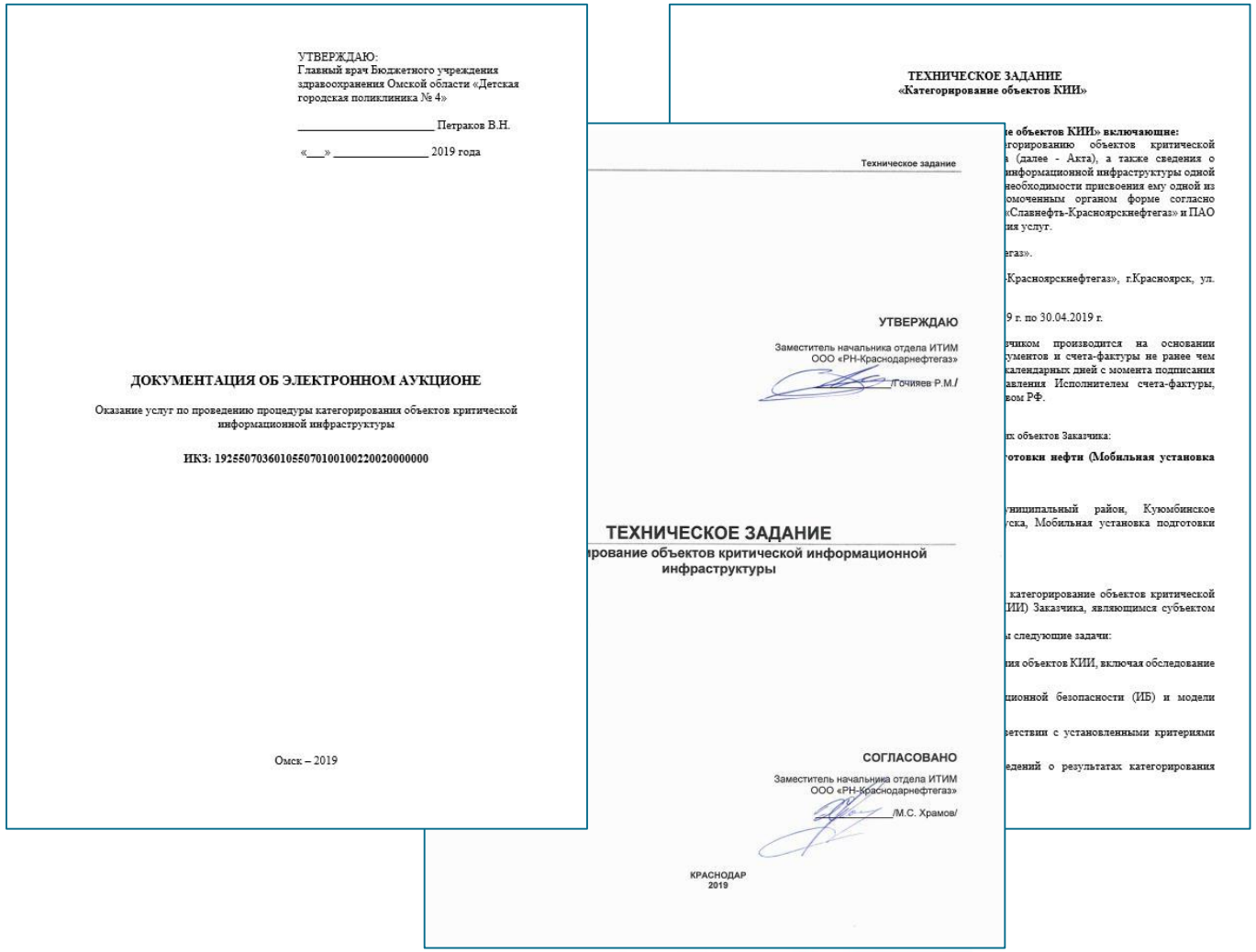
НПП “Гамма”

Конкурсы на категорирование ОКИИ, уместны ли?

Категорирование ОКИИ осуществляется самостоятельно субъектом КИИ (п.2 Правил, утв. ПП РФ № 127)

- **Оказание услуг по категорированию ОКИИ …**
- **Категорирование ОКИИ …**

- **Консультационные услуги в рамках категорирования ОКИИ …**
- **Услуги по сопровождению процедуры категорирования ОКИИ …**
- **Услуги по методическому обеспечению процедуры категорирования ОКИИ …**



УТВЕРЖДАЮ:
Главный врач Бюджетного учреждения здравоохранения Омской области «Детская городская поликлиника № 4»

_____ Петраков В.Н.

«___» _____ 2019 года

ДОКУМЕНТАЦИЯ ОБ ЭЛЕКТРОННОМ АУКЦИОНЕ

Оказание услуг по проведению процедуры категорирования объектов критической информационной инфраструктуры

ИКЗ: 192550703601055070100100220020000000

Омск – 2019

ТЕХНИЧЕСКОЕ ЗАДАНИЕ
«Категорирование объектов КИИ»

Техническое задание

УТВЕРЖДАЮ
Заместитель начальника отдела ИТИМ
ООО «РН-Краснодарнефтегаз»
_____ /Гочияев Р.М./

ТЕХНИЧЕСКОЕ ЗАДАНИЕ
рование объектов критической информационной инфраструктуры

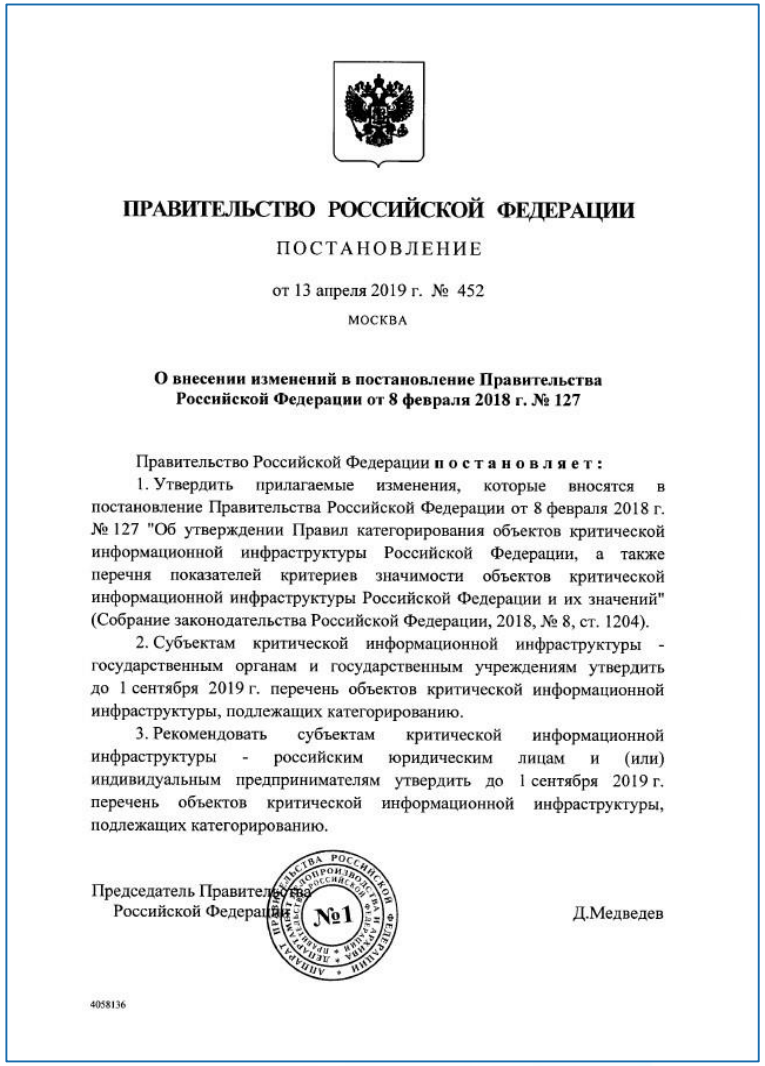
СОГЛАСОВАНО
Заместитель начальника отдела ИТИМ
ООО «РН-Краснодарнефтегаз»
_____ /М.С. Храмов/

КРАСНОДАР
2019

НПП “Гамма”

«*Субъектам критической информационной инфраструктуры - государственным органам и государственным учреждениям* ***утвердить до 1 сентября 2019 г. перечень объектов*** *критической информационной инфраструктуры, подлежащих категорированию*» (п.2 ПП РФ № 452)

- «***Рекомендовать*** *субъектам критической информационной инфраструктуры - российским юридическим лицам и (или) индивидуальным предпринимателям* ***утвердить до 1 сентября 2019 г. перечень объектов*** *критической информационной инфраструктуры, подлежащих категорированию*» (п.3 ПП РФ № 452)



ПРАВИТЕЛЬСТВО РОССИЙСКОЙ ФЕДЕРАЦИИ

ПОСТАНОВЛЕНИЕ

от 13 апреля 2019 г. № 452

МОСКВА

О внесении изменений в постановление Правительства Российской Федерации от 8 февраля 2018 г. № 127

Правительство Российской Федерации **п о с т а н о в л я е т :**

1. Утвердить прилагаемые изменения, которые вносятся в постановление Правительства Российской Федерации от 8 февраля 2018 г. № 127 "Об утверждении Правил категорирования объектов критической информационной инфраструктуры Российской Федерации, а также перечня показателей критериев значимости объектов критической информационной инфраструктуры Российской Федерации и их значений" (Собрание законодательства Российской Федерации, 2018, № 8, ст. 1204).

2. Субъектам критической информационной инфраструктуры - государственным органам и государственным учреждениям утвердить до 1 сентября 2019 г. перечень объектов критической информационной инфраструктуры, подлежащих категорированию.

3. Рекомендовать субъектам критической информационной инфраструктуры - российским юридическим лицам и (или) индивидуальным предпринимателям утвердить до 1 сентября 2019 г. перечень объектов критической информационной инфраструктуры, подлежащих категорированию.

Председатель Правительства Российской Федерации Д.Медведев

4058136

Для кого есть конкретные сроки проведения категорирования ОКИИ?

НПП “Гамма”

- *Государственные органы:*
- Федеральные министерства (*МВД, МЧС, МИД, МО, Минэнерго, Минюст и др.*)
- Федеральные службы (*ФМС, ФСВТС, ФСТЭК, ФСИН, ФСР, ФССП и др.*)
- Федеральные агентства (*Спецстрой, Росстандарт, Росспорт, Росархив, Роспечать и др.*)
- Конституционный и верховный суды
- Другие органы власти (*Совбез, Генпрокуратура, ЦБ, ПФР, ФСС, РФПР, ТПП и др.*)

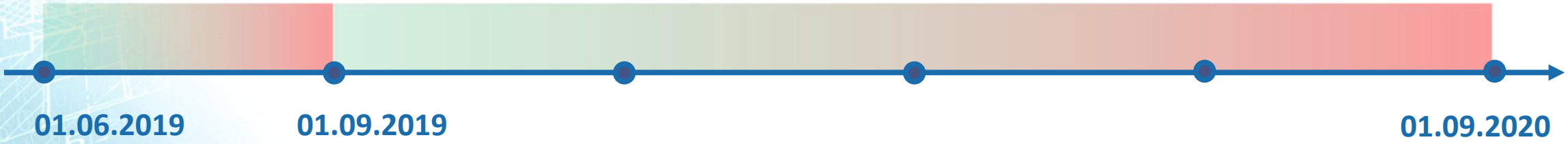
- *Государственные учреждениям:*
- Казенный (*ФГКУ «Росвоенипотека», ФГКУ »Росгранстрой» и др.*)
- Бюджетные (*ФГБУ «ФКП Росреестра», ФГБУ«ЦЖКУ» МО РФ и др.*)
- Автономные (*ФГАУ «НЦЗД» Минздрава России, ФГАУ «УИСП» МО РФ и др.*)

Сроки проведения категорирования ОКИИ

НПП “Гамма”

- «***Максимальный срок категорирования не должен превышать одного года со дня утверждения субъектом критической информационной инфраструктуры перечня объектов (внесения изменений в перечень объектов)***» (п.15 ПП РФ № 127)

Для государственных органов и государственных учреждений



Для российских юридических лиц и (или) индивидуальных предпринимателей

А если мы не в сроках то, что?

НПП “Гамма”

- *Обсуждаемые изменения в КоАП:*
- Нарушение порядка категорирования ОКИИ: до 100 000 руб.
- Нарушение требований к созданию систем безопасности значимых ОКИИ: до 100 000 руб.
- Нарушение требований по обеспечению безопасности значимых ОКИИ: до 100 000 руб.
- Нарушение порядка информирования о компьютерных инцидентах, реагирования на них, принятия мер по ликвидации последствий компьютерных атак, проведенных в отношении значимых ОКИИ: до 200 000 руб.
- Нарушение порядка обмена информацией о компьютерных инцидентах: до 200 000 руб.
- Непредставление или нарушение сроков представления сведений о результатах присвоения ОКИИ …: до 100 000 руб.
- Непредставление или нарушение порядка либо сроков представления в ГосСОПКА информации, предусмотренной законодательством: до 500 000 руб.

Оценка ущерба как основа категорирования ОКИИ

НПП “Гамма”

Значимость (негативные последствия)

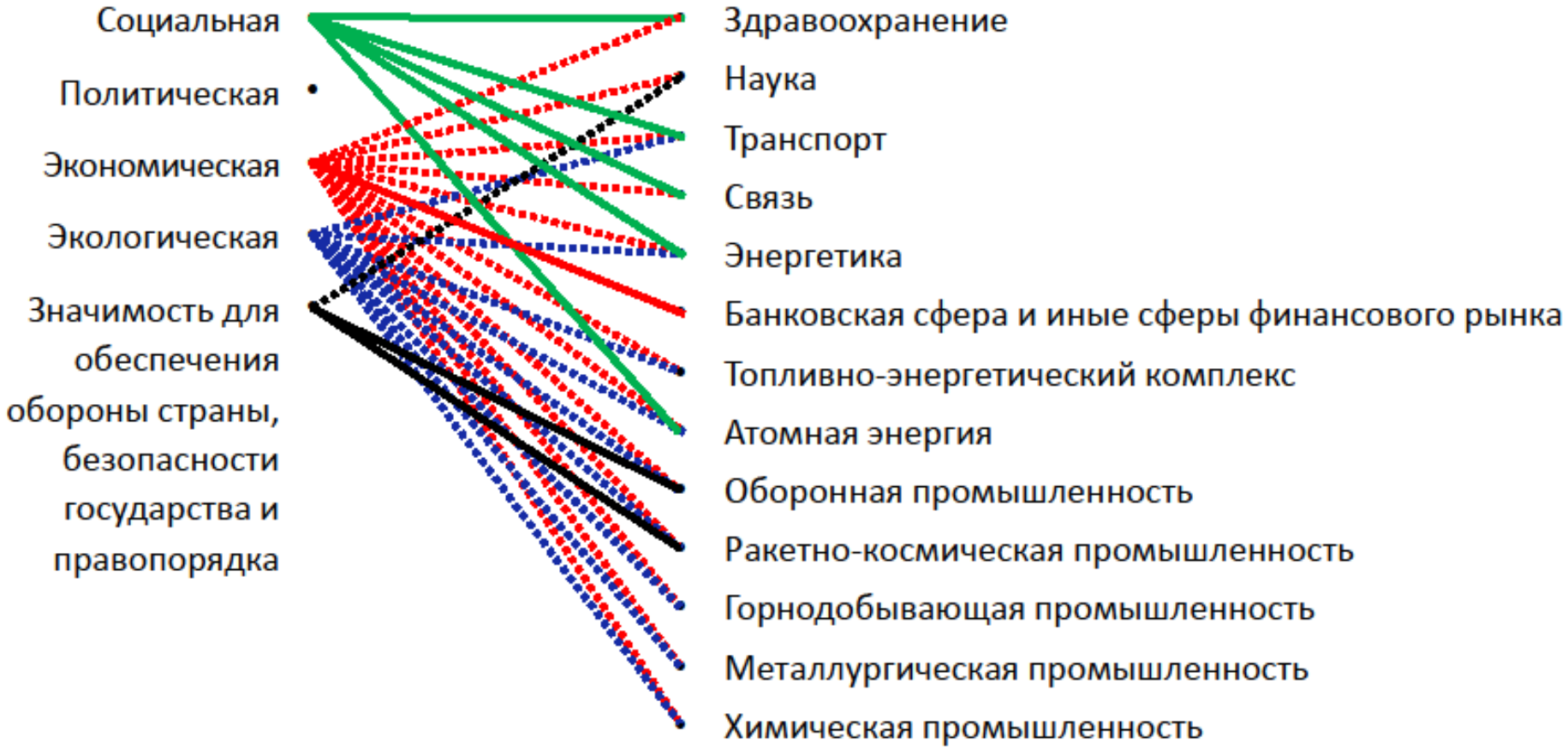
НПП "Гамма"

- **Социальная**: выражается в оценке **возможного ущерба**, причиняемого **жизни** или **здоровью** людей, возможности прекращения или нарушения функционирования **объектов обеспечения жизнедеятельности населения***, **транспортной инфраструктуры**, **сетей связи**, а также максимальном времени отсутствия **доступа к государственной услуге** для получателей такой услуги
- **Политическая**: выражается в оценке **возможного** причинения **ущерба интересам Российской Федерации** в вопросах внутренней и внешней политики
- **Экономическая**: выражается в оценке **возможного** причинения **прямого и косвенного ущерба субъектам** критической информационной инфраструктуры и/или **бюджетам Российской Федерации**
- **Экологическая**: выражается в оценке **уровня воздействия** на **окружающую среду**
- Значимость ОКИИ **для обеспечения обороны страны, безопасности государства и правопорядка** (ч.2, ст.7 ФЗ № 187-ФЗ)

- «… ***негативным*** ***социальным, политическим, экономическим, экологическим*** *последствиям,* ***последствиям*** *для* ***обеспечения обороны страны, безопасности государства и правопорядка*** …» (пп. «б», п.5 Правил, утв. ПП РФ № 127)

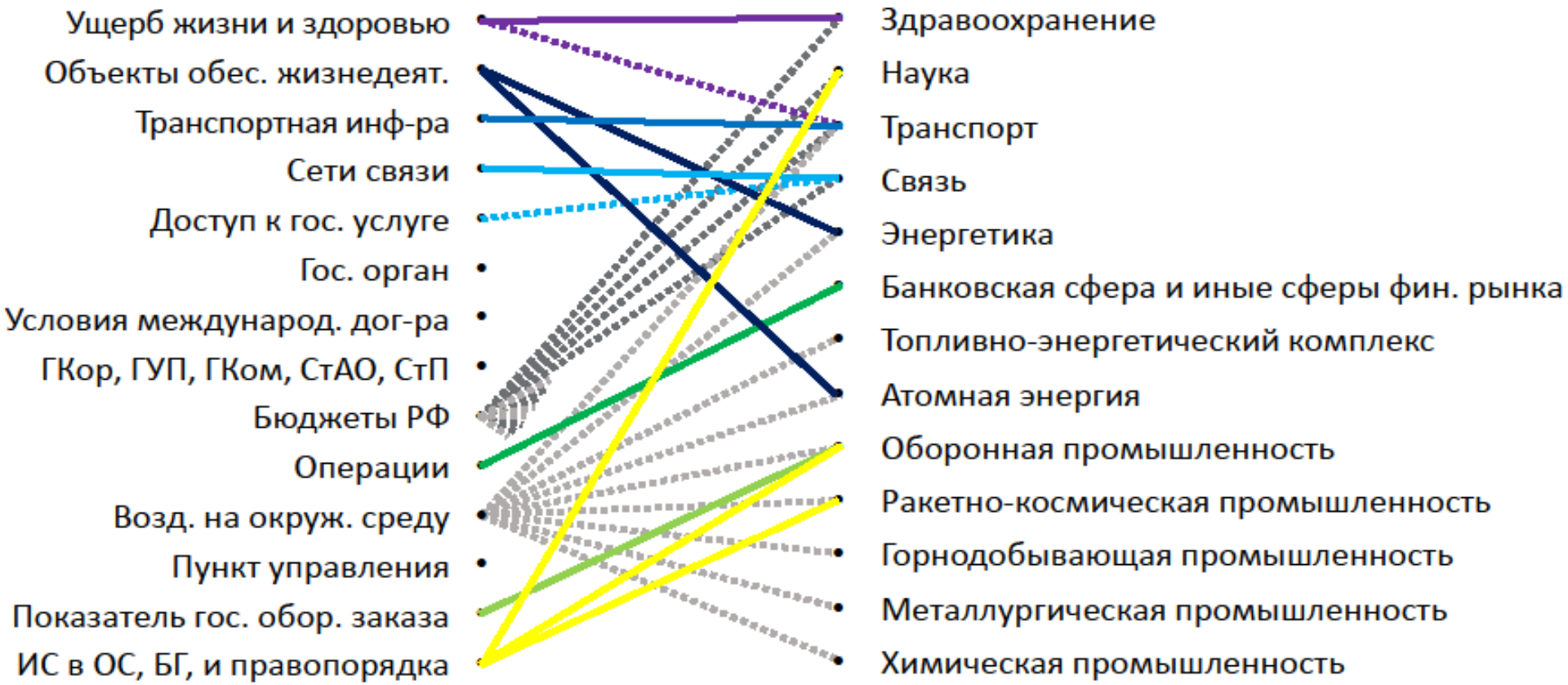
* Объекты, обеспечивающие водо-, тепло-, газо- и электроснабжение населения

Значимость по ФЗ и сферы по ФЗ



НПП “Гамма”

Значимость по ПП(ущерб) и сферы по ФЗ



Значимость (негативные последствия) и сферы, есть ли прямая связь?

НПП “Гамма”

- **К сожалению, субъект КИИ не может оперировать только «своими» негативными последствиями (*отдельными показателями критериев значимости*), исходя из сферы деятельности**

- ***«Оценивает в соответствии с перечнем показателей критериев значимости масштаб возможных последствий в случае возникновения компьютерных инцидентов на объектах критической информационной инфраструктуры, определяет значения каждого из показателей критериев значимости или обосновывает их неприменимость»*** **(пп. «е», п.14 Правил, утв. ПП РФ № 127)**

0 шаг: Определение видов деятельности

НПП “Гамма”

- Установлены Ваши виды деятельности:
- Вид деятельности 1
- Вид деятельности 2 в сфере(ах) согласно ФЗ № 187-ФЗ:

- Здравоохранение
- Наука
- Транспорт
- Связь
- Энергетика
- Банковская сфера и иные сферы финансового рынка
- Топливно-энергетический комплекс
- Атомная энергия
- Оборонная промышленность
- Ракетно-космическая промышленность
- Горнодобывающая промышленность
- Металлургическая промышленность
- Химическая промышленность

НПП “Гамма”

1 шаг: Определены процессы

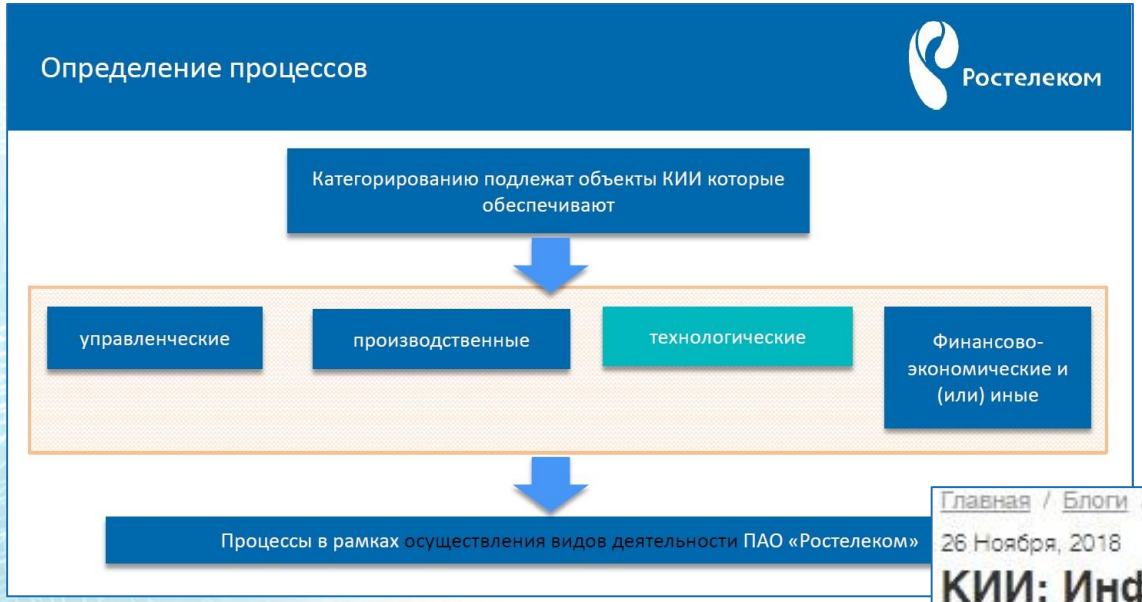
***«Определяет процессы*, указанные в пункте 3 настоящих Правил, в рамках выполнения функций (полномочий) или осуществления видов деятельности субъекта критической информационной инфраструктуры»* (пп. «а», п.14 Правил, утв. ПП РФ № 127)**

***«Категорированию подлежат объекты критической информационной инфраструктуры, которые обеспечивают управленческие, технологические, производственные, финансово экономические и (или) иные процессы в рамках выполнения функций (полномочий) или осуществления видов деятельности субъектов критической информационной инфраструктуры в областях (сферах) …»* (п.3 Правил, утв. ПП РФ № 127)**

*Процесс: Совокупность взаимосвязанных и (или) взаимодействующих видов деятельности, использующих входы для получения намеченного результата

А нужны ли нам эти «типы» процессов?

НПП “Гамма”



Главная / Блоги / Личные блоги / eБлокнот

26 Ноября, 2018

КИИ: Информация от ФСТЭК России: Системные вопросы

Александр Кузнецов

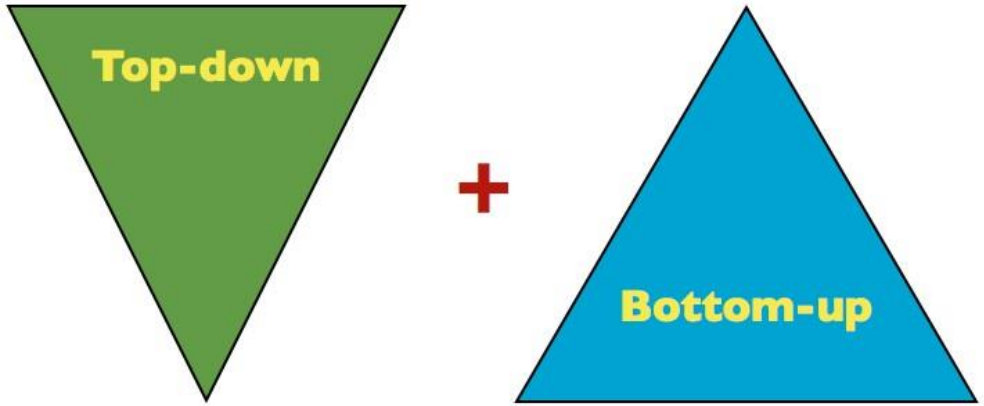
2. **Допускается** ли в рамках категорирования (выполнение пп. «б», п. 5 Правил, утв. ПП РФ № 127) оперировать понятием «Процесс», не разделяя его на «Управленческие», «Технологические», «Производственные», «Финансово-экономические» и «Иные»?
Вопрос связан с тем, что в федеральных законах отсутствуют определения для данных процессов, а в ГОСТ присутствуют определения только для терминов «Производственный процесс» (*ГОСТ 14.004-83*) и «Технологический процесс» (*ГОСТ 3.1109-82*), причем последний позиционируется как часть предшествующего.
Использование одного понятия упростило бы процедуру категорирования.
Позиция по вопросу: **да, допускается**.

НПП “Гамма”

Где взять Ваши процессы?

- В Вашем существующем реестре процессы
- Идентифицировать Ваши существующие процессы
- Взять из отраслевых стандартов

А если негде взять?



Идти от систем

2 шаг: Выявление критических процессов

НПП “Гамма”

- ***«Выявление управленческих, технологических, производственных, финансово-экономических и (или) иных процессов в рамках выполнения функций (полномочий) или осуществления видов деятельности субъектов критической информационной инфраструктуры, нарушение и (или) прекращение которых может привести к негативным социальным, политическим, экономическим, экологическим последствиям, последствиям для обеспечения обороны страны, безопасности государства и правопорядка»*** **(пп. «б», п.5 Правил, утв. ПП РФ № 127)**

Наим. процесса	Нарушение может привести к негативным последствиям?	Прекращение может привести к негативным последствиям?	Критический процесс
Процесс А	Нет	Нет	Нет
Процесс Б	Нет	Нет	Нет
Процесс В	Нет	Да	Да
Процесс Г	Да	Да	Да

Определение (выявление) ОКИИ

НПП "Гамма"

- «*Определение объектов критической информационной инфраструктуры, которые* ***обрабатывают информацию****, необходимую для обеспечения критических процессов, и (или) осуществляют* ***управление****,* ***контроль*** *или* ***мониторинг критических процессов***» (пп. «в», п.5 Правил, утв. ПП РФ № 127)

- «*Выявляет объекты критической информационной инфраструктуры, которые* ***обрабатывают информацию****, необходимую для обеспечения выполнения критических процессов, и (или) осуществляют* ***управление****,* ***контроль*** *или* ***мониторинг критических процессов****, готовит предложения для включения в перечень объектов, а также оценивает необходимость категорирования вновь создаваемых информационных систем, автоматизированных систем управления, информационно-телекоммуникационных сетей*» (пп. «в», п.14 Правил, утв. ПП РФ № 127)

Автоматизация в рамках критического процесса

НПП "Гамма"

- **Обработка** – систематическое выполнение операций над данными, необходимыми для обеспечения критического процесса
- **Управление** – поддержание критического процесса в рабочем состоянии в рамках заданных значений характеристик критического процесса
- **Контроль** – сравнение (сопоставление) фактических (текущих) значений характеристик критического процесса с заданными значениями этих характеристик
- **Мониторинг** – постоянное (регулярное) наблюдение за значениями характеристик критического процесса

10 Ноября, 2018

КИИ: Информация от ФСТЭК России

3. Если ИС, ИТС или АСУ не автоматизируют (*не участвует в обработке информации, управлении, контроле или мониторинге*) критический процесс, «завязанный» на выполнение функций (*полномочий*) или осуществление видов деятельности субъекта КИИ, то они не рассматриваются как объект КИИ (*например, у учреждения, функционирующего* ***не*** *в сфере энергетики (т.е. нет в Уставе деятельности по производству, передаче и сбыту электроэнергии), есть АСУ своей электроподстанции, то эта АСУ* ***не*** *объект КИИ*).

Автоматизация в рамках критического процесса

НПП "Гамма"

- **ИС** – совокупность содержащейся в базах данных информации и обеспечивающих ее обработку информационных технологий и технических средств
- **ИТС** – технологическая система, предназначенная для передачи по линиям связи информации, доступ к которой осуществляется с использованием средств вычислительной техники
- **АСУ** – комплекс программных и программно-аппаратных средств, предназначенных для контроля за технологическим и (или) производственным оборудованием (исполнительными устройствами) и производимыми ими процессами, а также для управления такими оборудованием и процессами

Наим. ИС, АСУ, ИТКС	Обработка в процессе В	Управление процессом В	Контроль процесса В	Мониторинг процесса В
ИС № 1	Да	Нет	Нет	Нет
ИС № 2	Да	Нет	Нет	Нет
Наим. ИС, АСУ, ИТКС	Обработка в процессе Г	Управление процессом Г	Контроль процесса Г	Мониторинг процесса Г
АСУ № 1	Нет	Да	Да	Да
АСУ № 2	Нет	Нет	Да	Да

Определение (выявление) ОКИИ – Пример

НПП "Гамма"

Наим. критического процесса	Обработка	Управление	Контроль	Мониторинг
Процесс В	ИС № 1 ИС № 2	-	-	-
Процесс Г	-	АСУ № 1	АСУ № 1 АСУ № 2	АСУ № 1 АСУ № 2

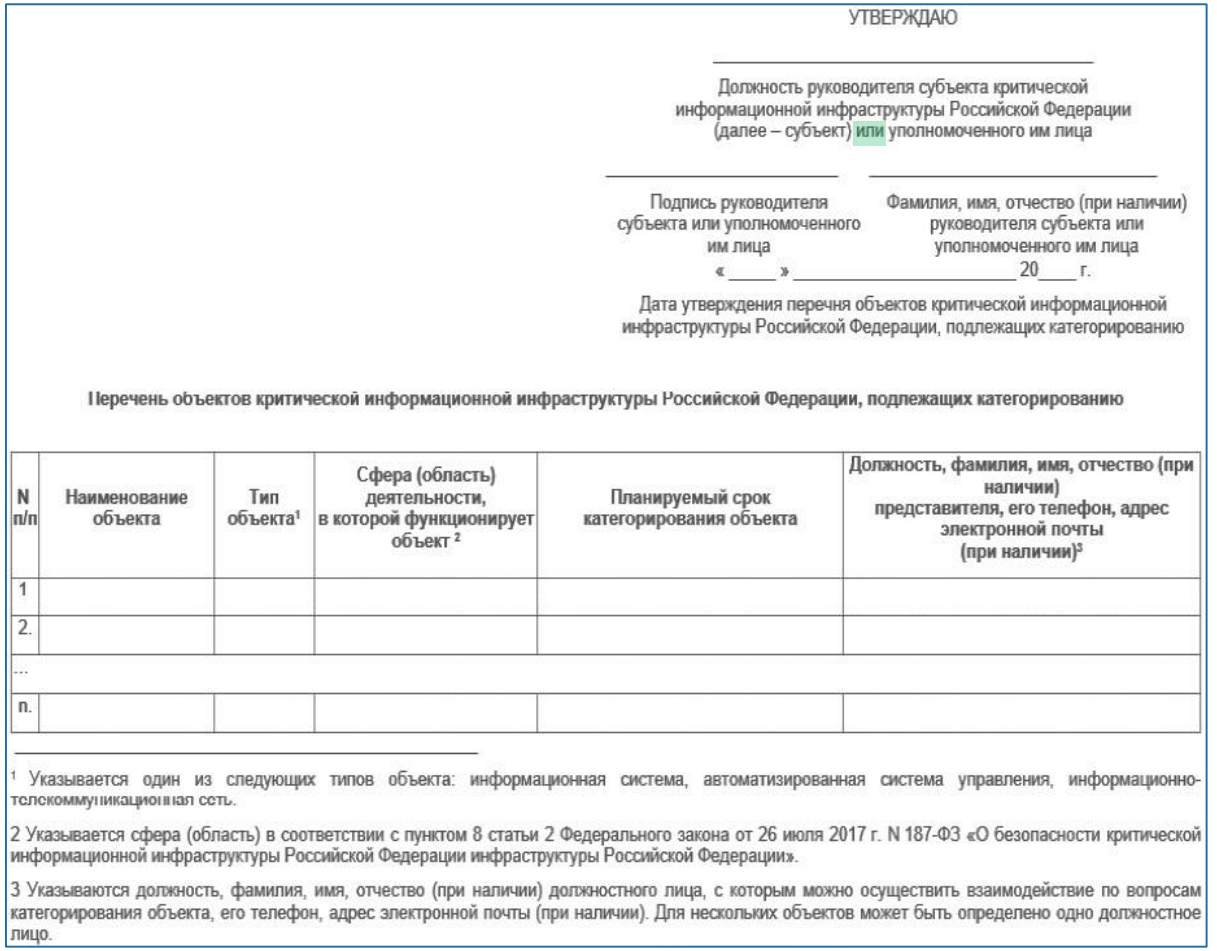
- Определены Ваши ОКИИ:
- ИС № 1 (Процесс В)
- ИС № 2 (Процесс В)
- АСУ № 1 (Процесс Г) • АСУ № 2 (Процесс Г) которые используются в критических процессах, выявленных на 2 шаге:
- Процесс В (Вид деятельности 2)
- Процесс Г (Вид деятельности 2)

4 шаг: Формирование перечня ОКИИ

НПП "Гамма"

- В качестве **наименования ОКИИ** указывается наименование из:
- акта ввода в эксплуатацию системы
- паспорт системы
- сертификат соответствия (если есть)
- эксплуатационная документации от производителя или наименование производителя (например, Система от «Наименование производителя»)

- **Адрес отправки**: Москва, ул. Старая Басманная, д. 17, на бумажном носителе и на электронном носителе информации в DOC(X)/XLS(S)-формате



УТВЕРЖДАЮ

_____

Должность руководителя субъекта критической информационной инфраструктуры Российской Федерации (далее – субъект) или уполномоченного им лица

_____ _____

Подпись руководителя субъекта или уполномоченного им лица | Фамилия, имя, отчество (при наличии) руководителя субъекта или уполномоченного им лица

«____» _____ 20____ г.

Дата утверждения перечня объектов критической информационной инфраструктуры Российской Федерации, подлежащих категорированию

Перечень объектов критической информационной инфраструктуры Российской Федерации, подлежащих категорированию

N п/п	Наименование объекта	Тип объекта[1]	Сфера (область) деятельности, в которой функционирует объект [2]	Планируемый срок категорирования объекта	Должность, фамилия, имя, отчество (при наличии) представителя, его телефон, адрес электронной почты (при наличии)[3]
1					
2.					
...					
n.					

[1] Указывается один из следующих типов объекта: информационная система, автоматизированная система управления, информационно-телекоммуникационная сеть.

2 Указывается сфера (область) в соответствии с пунктом 8 статьи 2 Федерального закона от 26 июля 2017 г. N 187-ФЗ «О безопасности критической информационной инфраструктуры Российской Федерации инфраструктуры Российской Федерации».

3 Указываются должность, фамилия, имя, отчество (при наличии) должностного лица, с которым можно осуществить взаимодействие по вопросам категорирования объекта, его телефон, адрес электронной почты (при наличии). Для нескольких объектов может быть определено одно должностное лицо.

Инф. сообщение ФСТЭК России № 240/25/3752

5 шаг : Оценка в соответствии с Перечнем, утв. ПП РФ № 127

НПП “Гамма”

- «***рассматривает возможные действия нарушителей*** *в отношении объектов критической информационной инфраструктуры, а также иные* ***источники угроз*** *безопасности информации*» (пп. «г», п.5 Правил, утв. ПП РФ № 127)

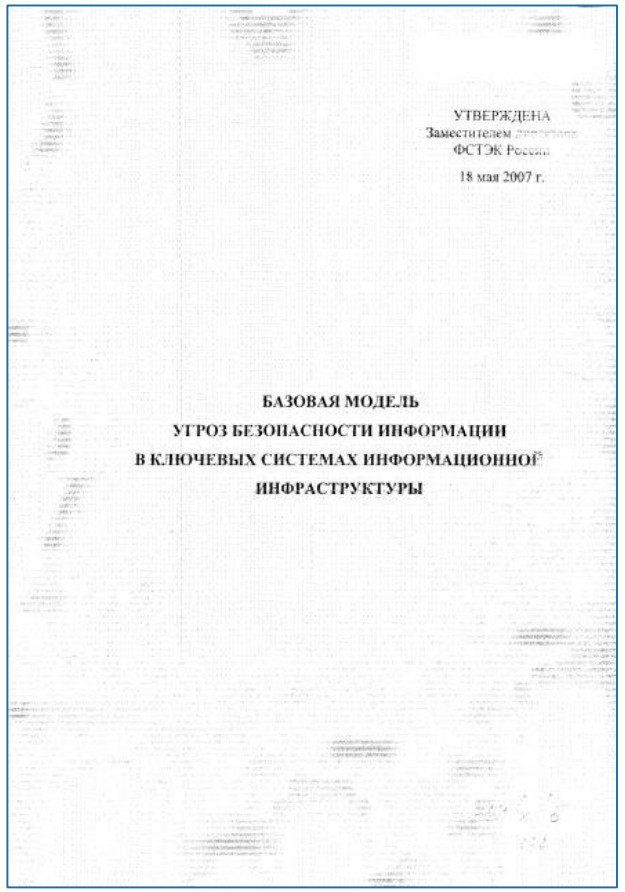
- **Источники угроз**:
  - нарушитель
  - носитель вредоносной программы
  - аппаратная закладка

6.1.	Категория нарушителя (внешний или внутренний), краткая характеристика основных возможностей нарушителя по реализации угроз безопасности информации в части его оснащенности, знаний, мотивации или краткое обоснование невозможности нарушителем реализовать угрозы безопасности информации

НПП "Гамма"

- «***анализирует угрозы*** *безопасности информации, которые могут привести к возникновению компьютерных инцидентов на объектах критической информационной инфраструктуры*» (пп. «д», п.5 Правил, утв. ПП РФ № 127)

«***Базовая модель угроз*** *безопасности информации в* ***ключевых системах информационной инфраструктуры****, утвержденная ФСТЭК России 18 мая 2007 г., а также* ***Методика определения актуальных угроз*** *безопасности информации в* ***ключевых системах информационной инфраструктуры****, утвержденная ФСТЭК России 18 мая 2007 г.,* ***могут применяться для моделирования угроз*** *безопасности информации на* ***значимых объектах*** *критической информационной инфраструктуры Российской Федерации до утверждения ФСТЭК России соответствующих методических документов*


УТВЕРЖДЕНА
Заместителем
ФСТЭК России
18 мая 2007 г.

БАЗОВАЯ МОДЕЛЬ
УГРОЗ БЕЗОПАСНОСТИ ИНФОРМАЦИИ
В КЛЮЧЕВЫХ СИСТЕМАХ ИНФОРМАЦИОННОЙ
ИНФРАСТРУКТУРЫ

- «… *должны быть рассмотрены* ***наихудшие сценарии****, учитывающие проведение* ***целенаправленных компьютерных атак*** …» (п.14(1) Правил, утв. ПП РФ № 127)

Оцениваем ущерб (ПП РФ №127 от 08.02.2018 г.)

НПП "Гамма"

I. Социальная значимость

Показатель		Значение показателя		
		III категория	II категория	I категория
5.	Отсутствие доступа к государственной услуге, оцениваемое в максимальном допустимом времени, в течение которого государственная услуга может быть недоступна для получателей такой услуги (часов)	менее или равно 24, но более 12	менее или равно 12, но более 6	менее или равно 6

6 шаг: Присвоение категории значимости объекта

НПП "Гамма"

- **Пример:**
- Если по показателю 1 – категория III, по показателю 2 – категория II, по остальным – без категории, то итоговая категория ОКИИ – II
- «*Объекту критической информационной инфраструктуры по результатам категорирования присваивается в соответствии с перечнем показателей критериев значимости категория значимости с наивысшим значением*» (п.6 Правил, утв. ПП РФ № 127)

«*В случае если объект критической информационной инфраструктуры* ***по одному*** *из показателей критериев значимости* ***отнесен к первой категории***, ***расчет по остальным показателям критериев значимости не проводится***» (п.6 Правил, утв. ПП РФ № 127)

- В каком порядке?
- Противоречит пп. «е», п.14 Правил, утв. ПП РФ № 127:

Определяет значения каждого из показателей критериев значимости или обосновывает их неприменимость!

НПП “Гамма”

6 шаг: Присвоение категории значимости объекта

- Решение комиссии по каждому объекту КИИ оформляется актом (**допускается оформление единого акта** по результатам категорирования нескольких ОКИИ)
- Все акты могут быть утверждены одним приказом руководителя оператора связи (акты будут выступать приложениями к соответствующему приказу), или каждый акт может быть утвержден по отдельности
- Субъект КИИ обеспечивает хранение акта (приказа об утверждении акта, в случае его наличия) до вывода из эксплуатации объекта КИИ или до изменения его категории значимости согласно части 12 статьи 7 Федерального закона N 187-ФЗ

Субъект КИИ не реже чем один раз в 5 лет, а также в случае изменения показателей критериев значимости ОКИИ или их значений осуществляет пересмотр установленных категорий значимости или решений об отсутствии необходимости присвоения указанным объектам таких категорий, т.е. **нужно перекатегорировать ОКИИ, если не учтено ПП РФ № 452**

Откатегорировались, что дальше?

НПП “Гамма”

Защищаться!

Как защищать?

НПП "Гамма"

Основные нормативно-правовые акты, устанавливающие меры защиты ОКИИ

Не значимый						Значимый					
АСУ	149-ФЗ		31			149-ФЗ		31	235	239	
ИТКС	149-ФЗ		351			149-ФЗ		351	235	239	
ИС											
ГИС	149-ФЗ		17			149-ФЗ	17	235	239		
МИС	149-ФЗ		17			149-ФЗ	17	235	239		
Иные ИС	149-ФЗ	98-ФЗ	НК РФ	395-1	382-П	149-ФЗ	98-ФЗ	НК РФ	395-1	382-П	235	239
ГИС ПДн	149-ФЗ	152-ФЗ	1119	17	378	149-ФЗ	152-ФЗ	1119	17	378	235	239
МИС ПДн	149-ФЗ	152-ФЗ	1119	17	378	149-ФЗ	152-ФЗ	1119	17	378	235	239
ИС ПДн	149-ФЗ	152-ФЗ	1119	21	378	149-ФЗ	152-ФЗ	1119	21	378	235	239

НПП “Гамма”

Пояснение к таблице:

1. НК РФ - Налоговый кодекс Российской Федерации
2. 98-ФЗ - Федеральный закон от 29.07.2004 № 98-ФЗ «О коммерческой тайне».
3. 149-ФЗ - Федеральный закон от 27.07.2006 № 149-ФЗ «Об информации, информационных технологиях и о защите информации».
4. 152-ФЗ - Федеральный закон от 27.07.2006 № 152-ФЗ «О персональных данных».
5. 395-1 - Федеральный закон от 02.12.1990 № 395-1 «О банках и банковской деятельности»
6. 1119 - Постановление Правительства РФ от 01.11.2012 № 1119 «Об утверждении требований к защите персональных данных при их обработке в информационных системах персональных данных».
7. 351 - Указ Президента Российской Федерации от 17.03.2008 № 351 «О мерах по обеспечению информационной безопасности Российской Федерации при использовании информационно-телекоммуникационных сетей международного информационного обмена».
8. 17 - Приказ ФСТЭК России от 11.02.2013 № 17 «Об утверждении Требований о защите информации, не составляющей государственную тайну, содержащейся в государственных информационных системах».
9. 21 - Приказ ФСТЭК России от 18.02.2013 № 21 «Об утверждении Состава и содержания организационных и технических мер по обеспечению безопасности персональных данных при их обработке в информационных системах персональных данных».
10. 31 - Приказ ФСТЭК России от 14.03.2014 № 31 (ред. от 09.08.2018) «Об утверждении Требований к обеспечению защиты информации в автоматизированных системах управления производственными и технологическими процессами на критически важных объектах, потенциально опасных объектах, а также объектах, представляющих повышенную опасность для жизни и здоровья людей и для окружающей природной среды».
11. 235 - Приказ ФСТЭК России от 21.12.2017 № 235 «Об утверждении требований к созданию систем безопасности значимых объектов критической информационной инфраструктуры российской федерации и обеспечению их функционирования»
12. 239 - Приказ ФСТЭК России от 25.12.2017 №239 «Об утверждении Требований по обеспечению безопасности значимых объектов КИИ РФ»
13. 378 - Приказ ФСБ России от 10.07.2014 № 378 «Об утверждении Состава и содержания организационных и технических мер по обеспечению безопасности персональных данных при их обработке в информационных системах персональных данных с использованием средств криптографической защиты информации, необходимых для выполнения установленных Правительством Российской Федерации требований к защите персональных данных для каждого из уровней защищенности».
14. 382-П - Положение Банка России от 9 июня 2012 г. № 382-П «О требованиях к обеспечению защиты информации при осуществлении переводов денежных средств и о порядке осуществления Банком России контроля за соблюдением требований к обеспечению защиты информации при осуществлении переводов денежных средств».

НПП “Гамма”

Особенности КИИ в здравоохранении (Приказ Минздрава №911н от 24 декабря 2018 г.)

1. Обязательность применения сертифицированных СЗИ, даже для защиты незначимых объектов КИИ. Для ЗОКИИ требования Минздрава ужесточают требования 239 Приказа ФСТЭК – только сертифицированные СЗИ.
2. Если по 239 приказу ФСТЭК (проект 2019 года) ограничения по размещению программно-технических средств ЗОКИИ территорией РФ устанавливаются только для 1 категории значимости + предусмотрены исключения для зарубежных филиалов, а также законодательных исключений, то по требованиям Минздрава никаких исключений не предусмотрено и ограничения относятся ко всем ОКИИ, включая незначимые.
3. Установлено требование о бесперебойном круглосуточном функционировании ИС в непрерывном режиме. Если это ИС, с помощью которых оказываются госуслуги населению, то автоматом попадаете под 1 категории значимости КИИ. Смотрим показатели в ПП127, п.5. Даже если брать 4 часа в месяц, отведенные Минздравом на ремонт и обслуживание ИС, это все равно меньше 6 часов (показатель 1 категории). Ну или пытаться доказать при проверках, что расчетный период не указан в ПП127 и его правильно считать годовым.

Критические процессы МО:

1. Процесс управления и планирования потока пациентов при оказании первичной медико-санитарной помощи и специализированной медицинской помощи в стационарных условиях (расписание приема специалистами, учет занятости коечного фонда).

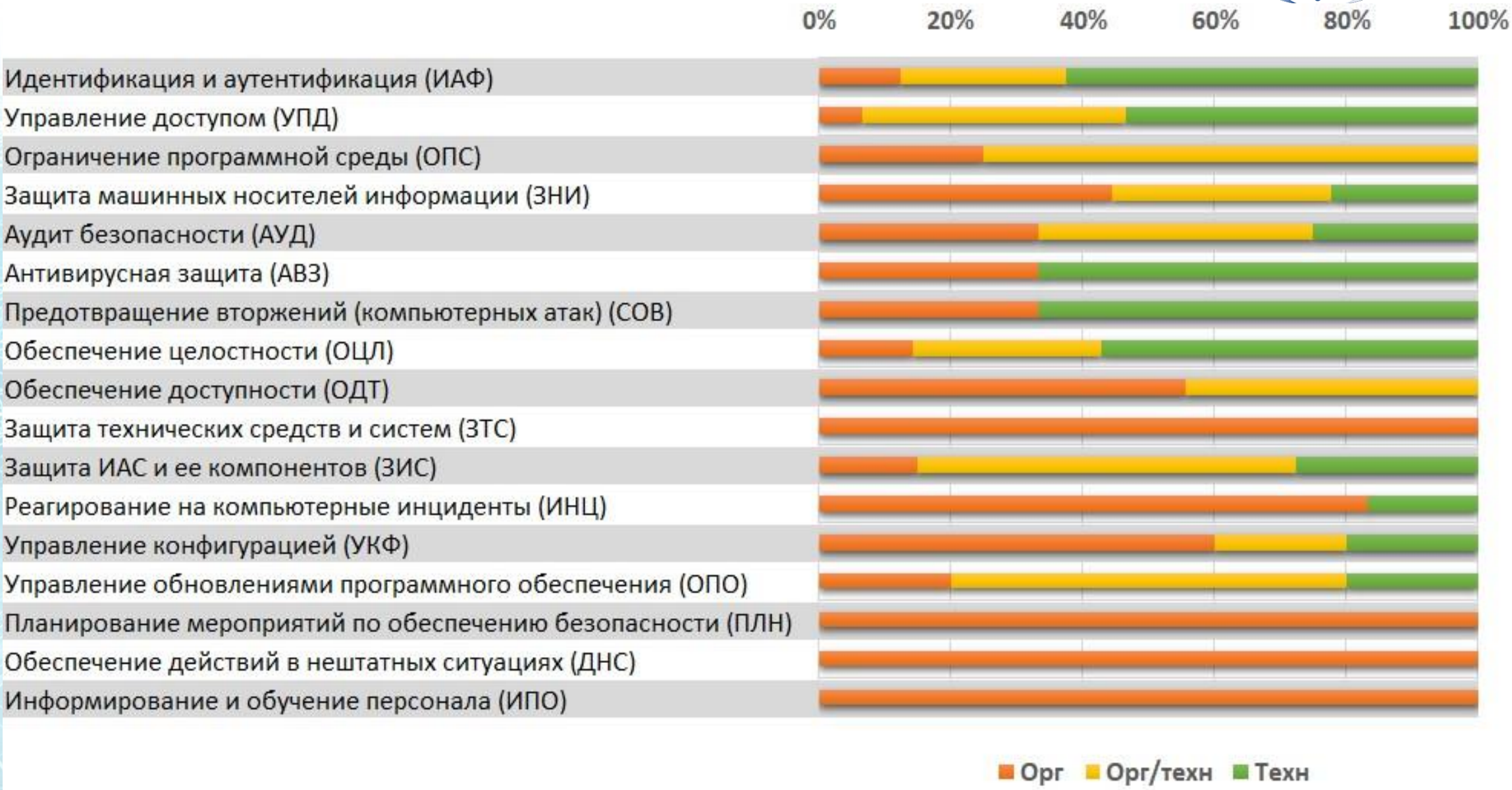
2. Процесс мониторинга доступности записи на прием к врачу (соблюдение установленных сроков).
3. Процесс учета населения, прикрепленного к МО (ФОМС).
4. Процесс мониторинга доступности медицинской помощи.

Порядок выполнения работ по объектам КИИ

НПП "Гамма"

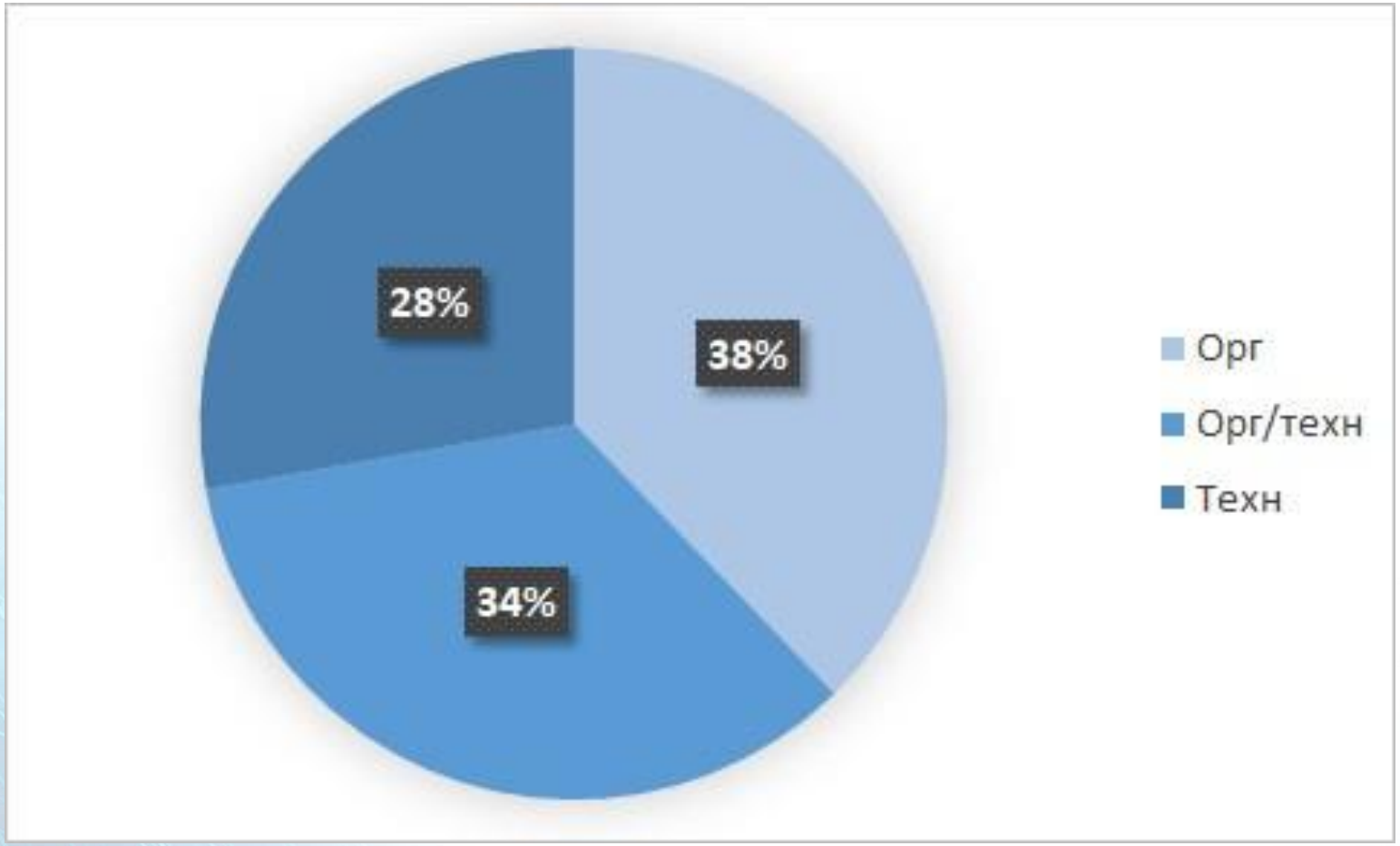
Меры защиты. Классификация ФСТЭК России

НПП "Гамма"



НПП “Гамма”

Соотношение мер защиты различного характера



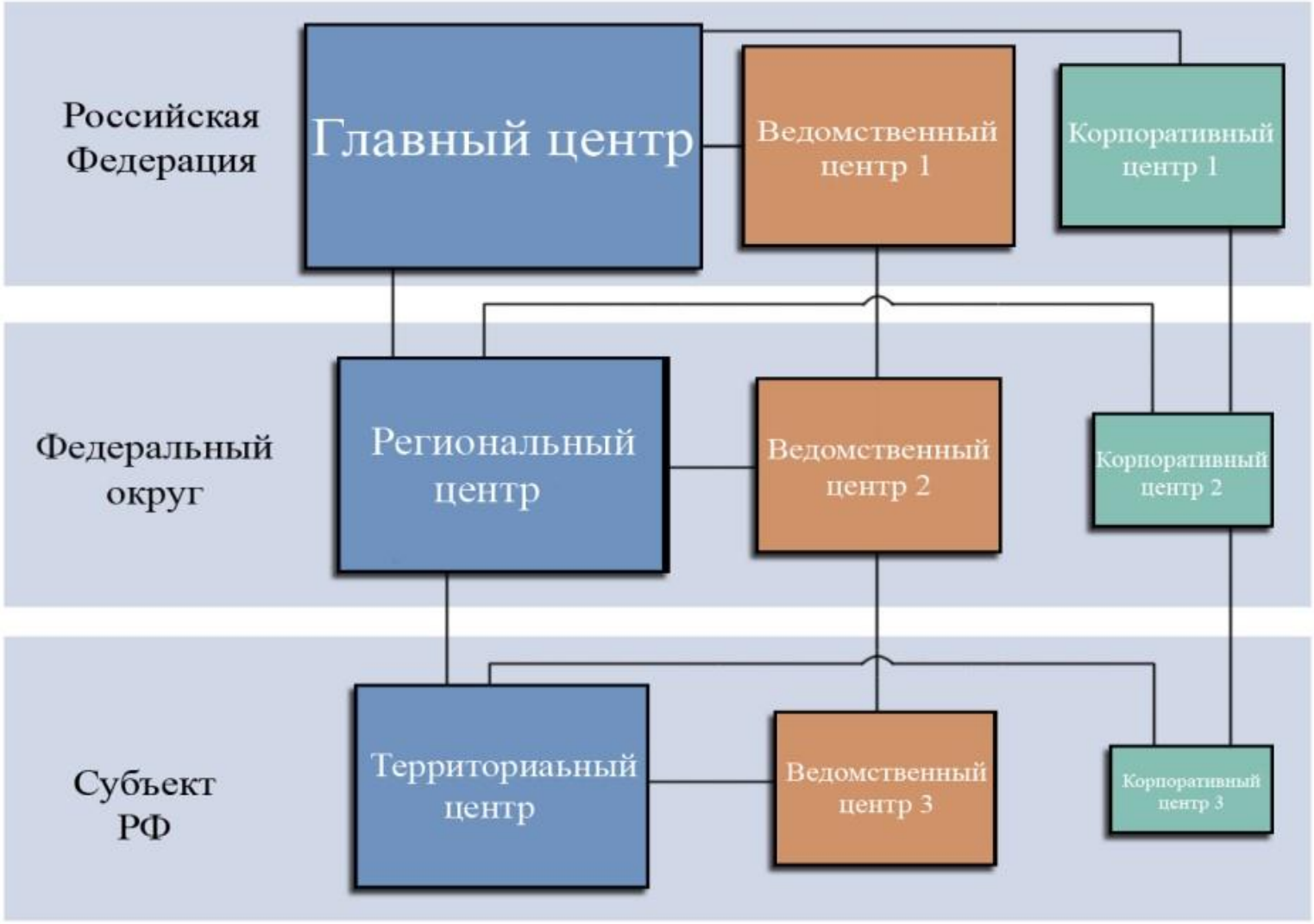
НПП “Гамма”

Состав работ по обеспечению безопасности субъектов КИИ РФ

1. Аудит информационной безопасности
2. Разработка моделей потенциального нарушителя и возможных угроз безопасности информации
3. Определение величины возможного ущерба в случае возникновения инцидентов
4. Категорирование объектов КИИ
5. Формирование требований к системе ЗИ и разработка ТЗ на систему ЗИ
6. Проектирование систем ЗИ, проектирование подключения к сегменту ГосСОПКА
7. Разработка организационно-распорядительной документации
8. Внедрение (в т.ч. Подготовка к вводу в эксплуатацию) средств и систем ЗИ, подключение к сегменту ГосСОПКА
9. Аттестация на соответствие требованиям безопасности информации
10. Сопровождение созданных систем ЗИ, в т.ч. мониторинг событий ИБ

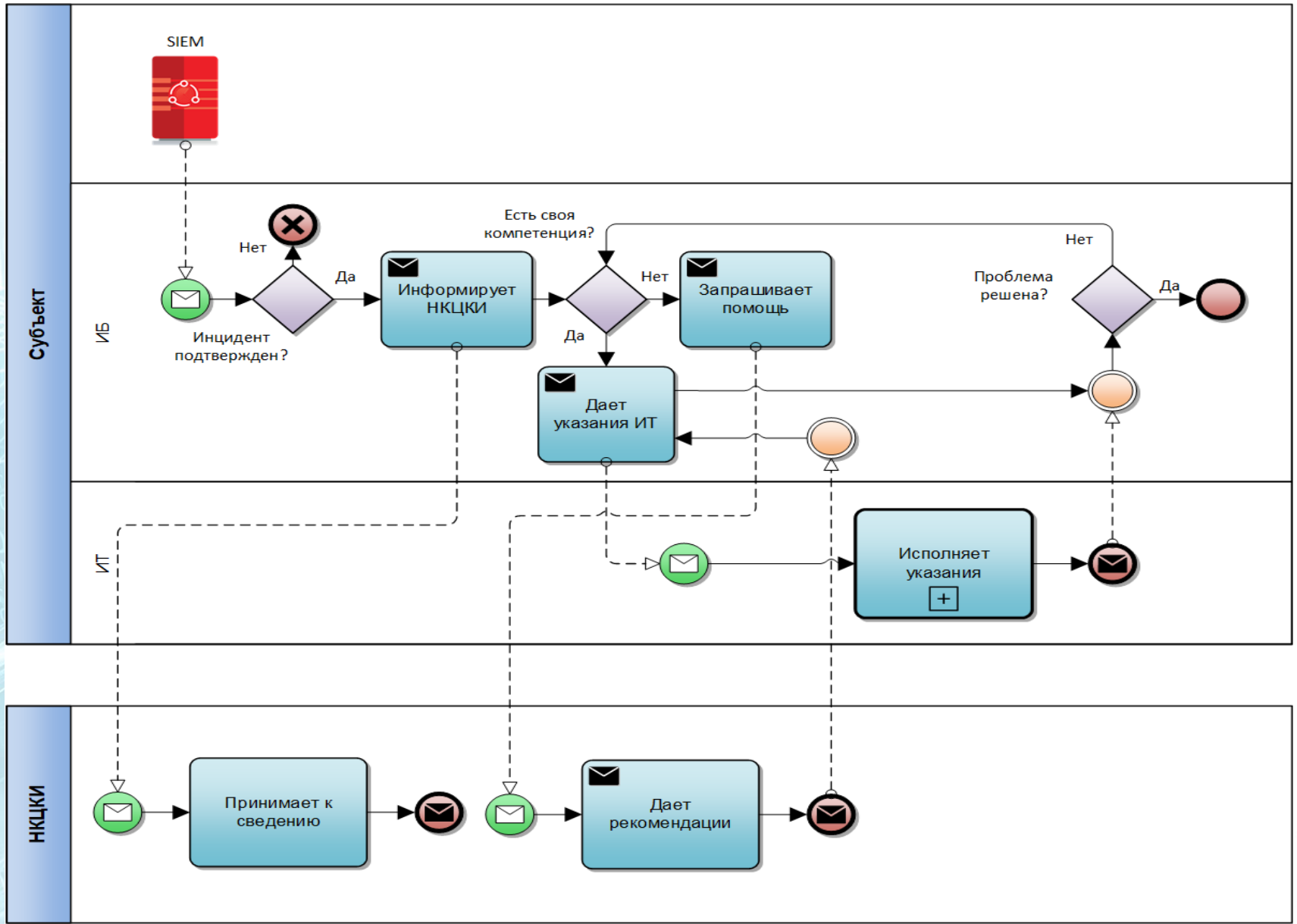
НПП “Гамма”

Взаимодействие субъекта КИИ с сегментом ГосСОПКА не пожелание ,а обязанность в соответствии с п.4 ст.10 187-ФЗ



Как это работает?

НПП "Гамма"



Приказ ФСБ России №367 от 24.07.2018 г. «Об утверждении Перечня Информации представляемой В ГосСОПКА и Порядка пред-ставления информации в ГосСОПКА»

ФГУП
“НПП “Гамма”

Спасибо за внимание!

Сергей Марков

Начальник отдела системных проектов

Санкт-Петербургский НТЦ ФГУП «НПП «Гамма»

Тел.: +7 (921)3724674

e-mail: markov@spb.nppgamma.ru