Российский государственный университет нефти и газа (НИУ) имени И.М. Губкина
ФАКУЛЬТЕТ КОМПЛЕКСНОЙ БЕЗОПАСНОСТИ ТЭК

# МОДЕЛЬ УГРОЗ ФСТЭК РОССИИ: ПЕРВЫЕ ВПЕЧАТЛЕНИЯ

Директор Научно-образовательного центра
новых информационно-аналитических технологий
факультета комплексной безопасности ТЭК
РГУ нефти и газа (НИУ) им. И.М.Губкина
к.т.н. Д.И.Правиков

# УТВЕРЖДЕННЫЙ ДОКУМЕНТ

5 февраля 2021 г. Федеральной службой по техническому и экспортному контролю Российской Федерации утвержден методический документ «Методика оценки угроз безопасности информации»

# ЗАДАЧИ ОЦЕНКИ УГРОЗ БЕЗОПАСНОСТИ

2.2. Основными задачами, решаемыми в ходе оценки угроз безопасности информации, являются:

а) *определение негативных последствий, которые могут наступить от реализации (возникновения) угроз безопасности информации;*

б) *инвентаризация систем и сетей и определение возможных объектов воздействия угроз безопасности информации;*

в) *определение источников угроз безопасности информации и оценка возможностей нарушителей по реализаций угроз безопасности информации;*

г) оценка способов реализации (возникновения) угроз безопасности информации;

д) оценка возможности реализации (возникновения) угроз безопасности информации и определение актуальности угроз безопасности информации;

е) оценка сценариев реализации угроз безопасности информации в системах и сетях.

# ВОПРОС 1

Сведения о результатах присвоения объекту критической информационной инфраструктуры одной из категорий значимости либо об отсутствии необходимости присвоения ему одной из таких категорий (форма утверждена приказом ФСТЭК России от 22 декабря 2017 г. № 236).

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

6.2. Основные угрозы безопасности информации или обоснование их неактуальности

7.1. Типы компьютерных инцидентов, которые могут произойти в результате реализации угроз безопасности информации…

**Акты категорирования уже отвечают на основные вопросы модели угроз. Как разделить по назначению указанные два документа?**

# ДИЛЕММА «ЯЙЦА» И «КУРИЦЫ»

**Сначала модель угроз**

- модель может составляться не для всех объектов КИИ;
- может ли быть продуктивной модель на этапе проектирования объекта КИИ?

**Сначала акт категорирования**

- значимые объекты – от 15% до 30% от общего количества;
- угрозы описываются, но защита реализуется компенсирующими мерами.

# ВОПРОС 2

2.7. Оценка угроз безопасности информации проводится подразделением по защите информации… Для оценки угроз безопасности информации по решению обладателя информации или оператора в соответствии с законодательством Российской Федерации могут привлекаться специалисты сторонних организаций.

**Способны ли специалисты, например, промышленных предприятий, проводить моделирование угроз с учетом всех требований методического документа?**

**Если использовать консалтинг, то каким образом необходимо обосновывать выделение бюджета?**

**«Оценка угроз безопасности информации должна носить систематический характер» - насколько затратными в случае внешнего консалтинга могут быть затраты на обновление моделей угроз?**

# ВОПРОС 3

«На текущий момент российские промышленные предприятия в качестве уязвимых каналов информационного обмена рассматривают:

- несанкционированное подключение персоналом защищаемых систем внешних носителей;
- заражение систем вредоносным программным обеспечением при подключении внешних носителей в рамках сервисного обслуживания».

Релейщик № 2 – 2000, стр. 6-7.

**Имеет ли смысл более подробная детализация сценария, связанного с работой запущенного с носителя вредоносного программного обеспечения?**

# ВОПРОС 4

«Коммерсант»
22.01.2021, 10:58

Центр кибербезопасности России предупредил о возможных кибератаках из США

Газета "Коммерсантъ" №39/В от 09.03.2021, стр. 6

США расчехляют стратегический сбоезапас

В Белом доме заговорили о кибератаках против Москвы

Основными видами нарушителей, подлежащих оценке, являются:

специальные службы иностранных государств;

террористические, экстремистские группировки;

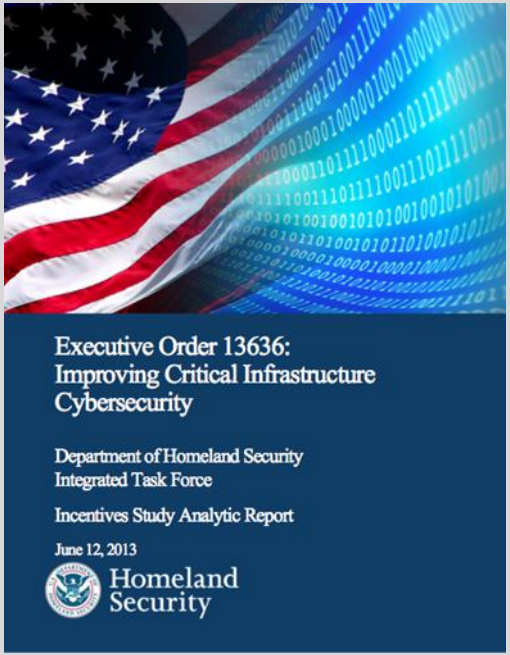
преступные группы (криминальные структуры);

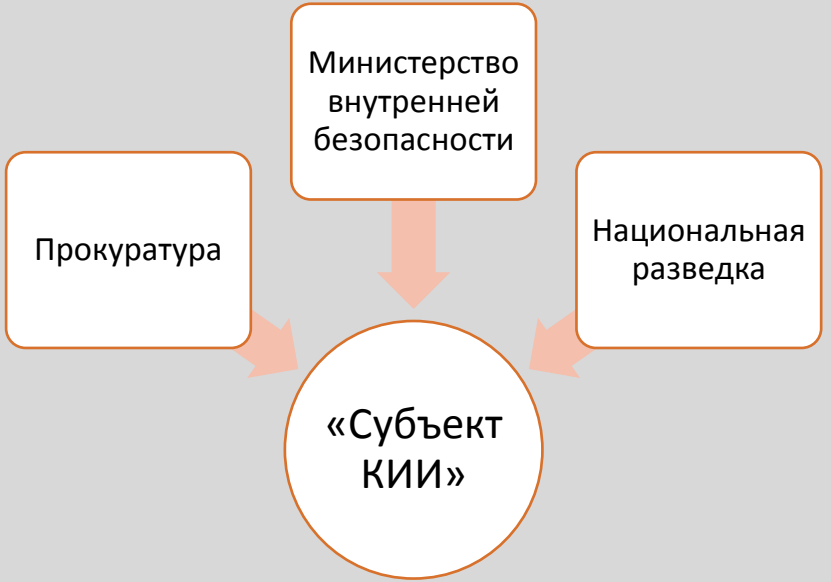
отдельные физические лица (хакеры);

конкурирующие организации;

…..

# ИНФОРМИРОВАНИЕ ПРИ ЗАЩИТЕ КИИ В США

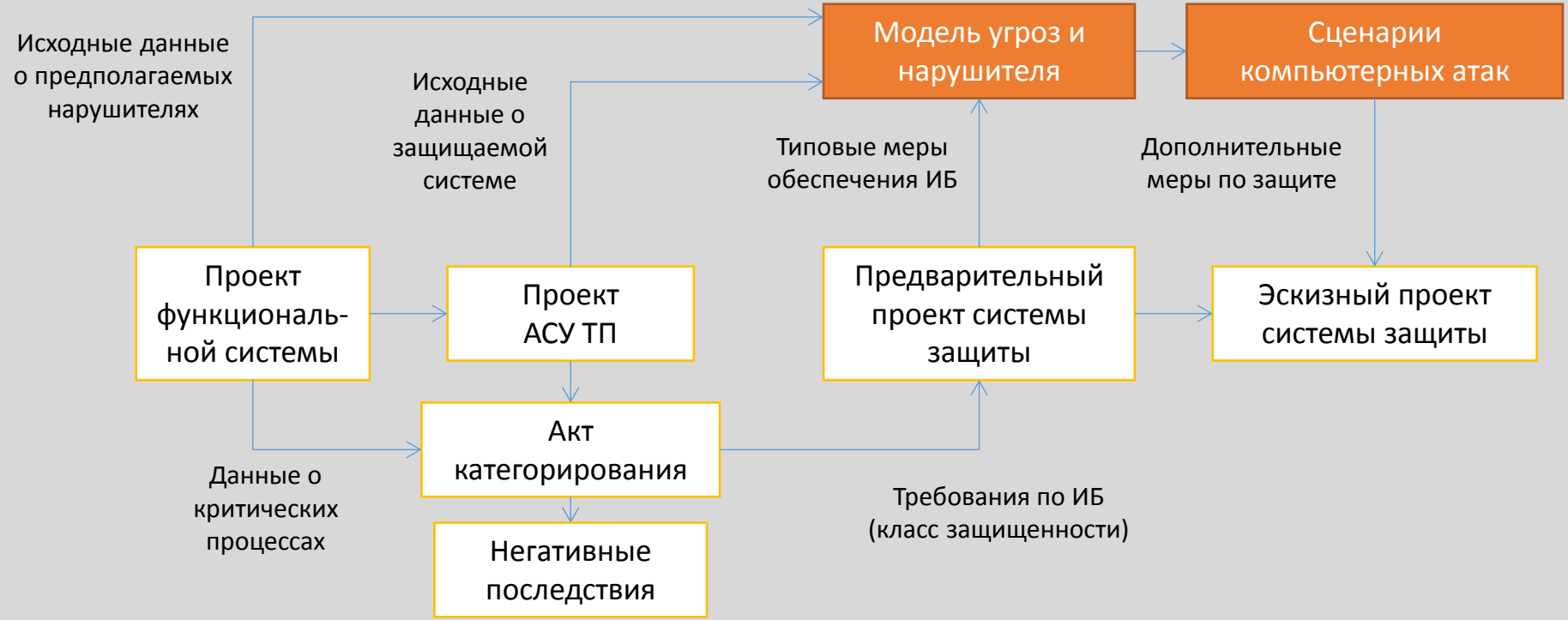


# ВОПРОС 5

Можно ли на основании перечисленных и, возможно, иных вопросов предложить продуктивное использование для защищаемой системы Модели угроз безопасности информации?

# ВОЗМОЖНАЯ СХЕМА РАЗРАБОТКИ СИСТЕМЫ ИБ



# СПАСИБО ЗА ВНИМАНИЕ

dip@gubkin.pro