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

Комплексная безопасность предприятий ТЭК: проблемы обеспечения защищенности и импортозамещения»

Тагиров Айдар Рафаилевич

доцент кафедры комплексной безопасности критически важных объектов

Современные угрозы предприятиям ТЭК носят гибридный характер.

Подход к обеспечению отдельных видов безопасности просматривается через принятие соответствующих федеральных законов.

Наиболее ярким примером является Федеральный закон "О безопасности объектов топливно-энергетического комплекса" от 21.07.2011 № 256-ФЗ, направленный на антитеррористическую защищенность объектов конкретной сферы.

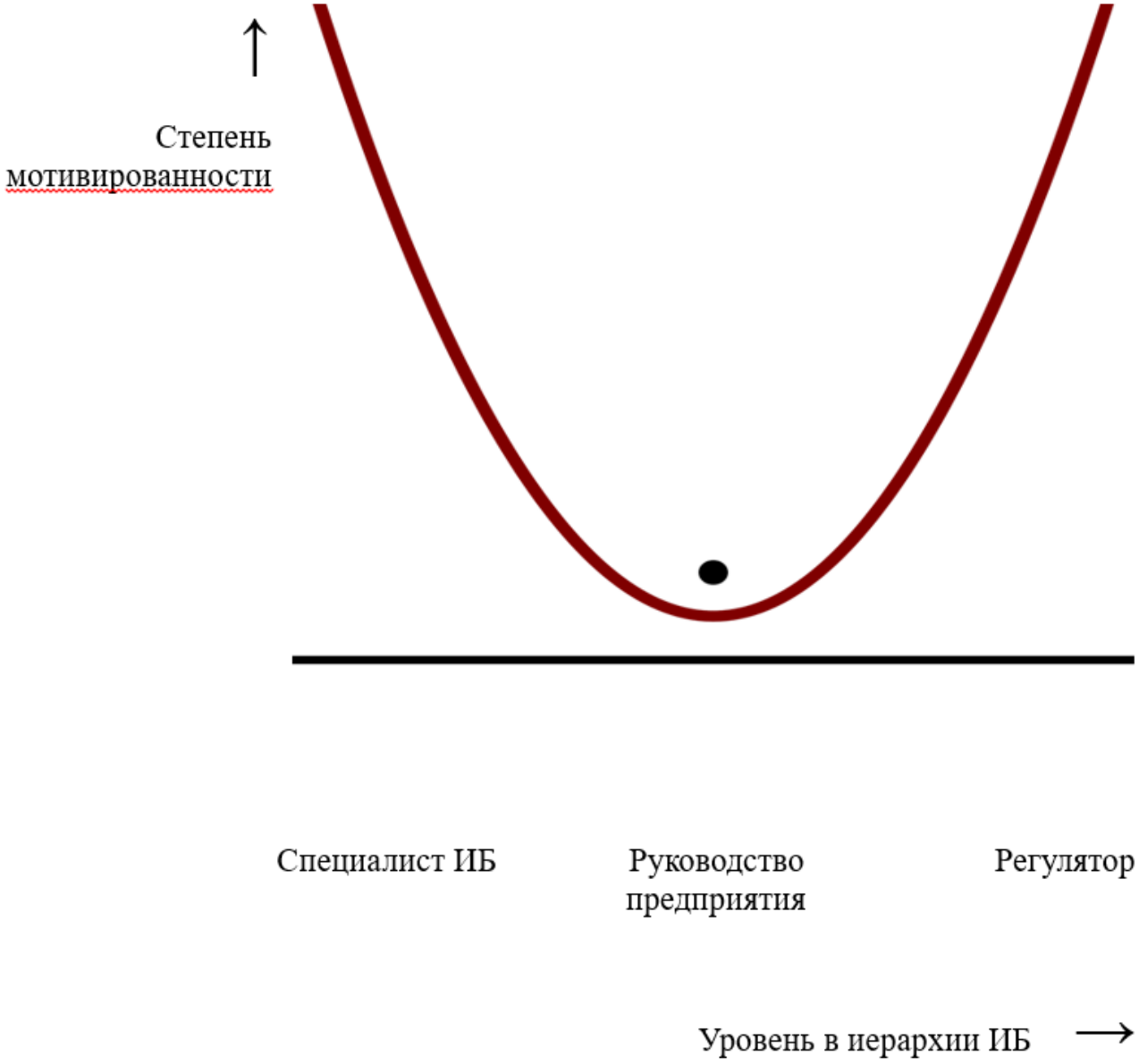


Рис. 1. Зависимость степени мотивированности по обеспечению ИБ от уровня в глобальной иерархии

"Методический документ. Методика оценки угроз безопасности информации" (утв. ФСТЭК России 05.02.2021)

Методика

1. Общие положения
2. Порядок оценки угроз безопасности информации
3. Определение негативных последствий от реализации (возникновения) угроз безопасности информации
4. Определение возможных объектов воздействия угроз безопасности информации
5. Оценка возможности реализации (возникновения) угроз безопасности информации и определение их актуальности
   5.1 Определение источников угроз безопасности информации
   5.2 Оценка способов реализации (возникновения) угроз безопасности информации
   5.3 Оценка актуальности угроз безопасности информации

26 апреля 2022 г. в рамках XV Всероссийской научно-технической конференции «Актуальные проблемы развития нефтегазового комплекса», организованной РГУ нефти и газа (НИУ) имени И.М. Губкина, была проведена панельная секция «Комплексная безопасность предприятий ТЭК: проблемы обеспечения защищенности и импортозамещения».

Комплексная безопасность в понимании **регулятора**

Включает в себя отделы по следующим направлениям:

- противодействие террористическим угрозам;
- противодействие киберугрозам;
- обеспечение правовой защиты предприятий;
- мобилизационная подготовка;
- антикоррупционная деятельность.

Все перечисленные направления обеспечения безопасности предприятий связаны между собой. Так, например, одним из негативных последствий компьютерных атак может быть снижение мобилизационной готовности.

Комплексная безопасность в понимании **регулятора**

Изменение геополитической обстановки привело к тому, что использование решений и средств обеспечения информационной безопасности импортного производства для критической информационной инфраструктуры уже не рассматривается. Как следствие возникает вопрос не просто поиска аналога российского производства, но, возможно, смены парадигмы при обеспечении безопасности предприятий промышленности

Комплексная безопасность в понимании

разработчиков систем моделирования

Все угрозы делятся на две группы:

1. Частые угрозы, для которых можно составить статистику.

2. Редкие явления с катастрофическими последствиями.

Так, например, террористическая атака на объект ТЭК – это редкое явление, для которого невозможно составить статистику, а значит провести обоснованный расчет рисков.

Комплексная безопасность в понимании

разработчиков систем моделирования

Комплексность – понятие о нескольких компонентах безопасности с учётом их влияния друг на друга.

Аксиома об угрозах: объективно существует бесконечное число угроз любому субъекту безопасности, в т. ч. которые невозможно предположить.

Следствия из аксиомы:

1. Абсолютной безопасности не существует.
2. В любой момент может возникнуть любое количество угроз, в т. ч. ранее не известных.
3. Невозможно создать идеальную систему безопасности.
4. Система безопасности должна развиваться.
5. Для реагирования необходим резерв средств за счёт избыточности системы безопасности.

Комплексная безопасность в понимании

разработчиков систем моделирования

Понятие комплексной безопасности начинается с комплексного подхода. Прежде чем создать систему защиты, нужно дать ответы на вопросы:

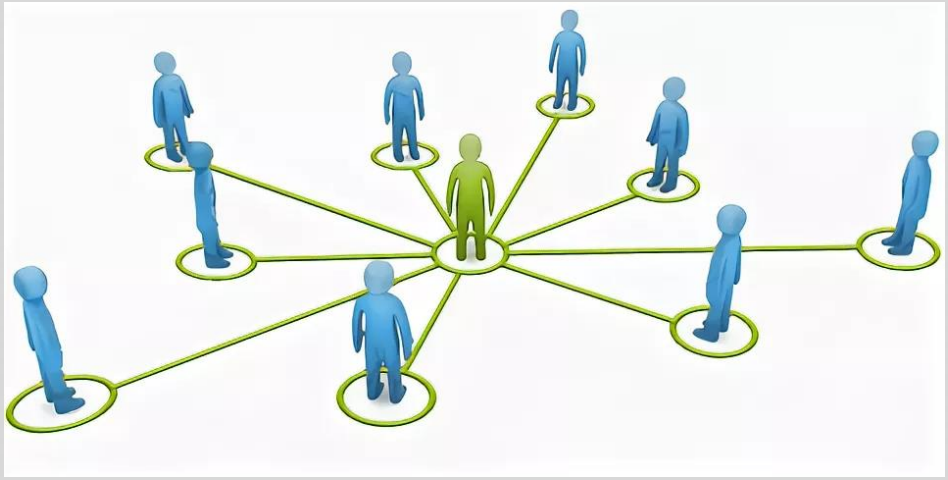
Что защищать?

От кого защищать?

Сколько времени понадобится злоумышленнику на совершение несанкционированного действия?

Как и какими силами обеспечить создание рубежей защиты?

Комплексная безопасность в понимании **вендора**



Вместо классического процесса проектирования: сбора данных, их анализа, разработки рабочей документации, которые сопровождаются проблемами устаревания и потерей информации, в настоящее время внедряется продукт, способный обеспечить возможность быстрого и качественного создания системы безопасности с консолидацией данных и возможностью оперативно менять данную цифровую модель.

Комплексная безопасность в понимании **интегратора**

Большой уровень абстракции при моделирования угроз. Затрагивает разные сферы – промышленную, антитеррористическую и информационную. Обеспечение КБ должно производиться быстро, что приводит к декомпозиции проектов на три базовых уровня:

1. Стратегический, на котором осуществляется анализ состояния безопасности АСУ ТП на уровне исполнительных аппаратов, материнских компаний, общая систематизация подходов к защите, связанная с разработкой стратегии и дорожной карты, формирование целевой модели безопасности.
2. Оперативный, на котором проводится анализ состояния безопасности АСУ ТП на уровне филиалов, тестов на проникновение для оценки реального уровня защищенности и инвентаризация типовых объектов, а также формируются контуры систем защиты.
3. Тактический, на котором повышается осведомленность на местах персонала, проведение обучения, киберучений, в рамках этого уровня также может производиться аутсорсинг реализации основных функций безопасности для быстрого парирования потенциальных угроз.

Описание комплексной безопасности в системе трех координат

Первая координата – уровень рассмотрения проблемы:

= геополитический,
= национального государства,
= отрасли,
= предприятия,
= объекта критической информационной инфраструктуры,
= отдельной системы,
= уровень хоста,
= уровень микросхемы.

Описание комплексной безопасности в системе трех координат

Вторая координата – аспекты безопасности:

= экономическая,

= физическая,

= экологическая,

= пожарная,

= промышленная,

= информационная.

При этом, например, пожарную безопасность нельзя отделить от информационной, т.к. современные противопожарные системы включают в себя программно-аппаратные комплексы.

Описание комплексной безопасности в системе трех координат

Третья координата – цели обеспечения безопасности, включая информационную безопасность:

= государство (описано достаточно внятно и подробно),

= предприятия (как избежать наказания ответственных лиц в соответствии с изменениями в кодексах Российской Федерации), т.е. цели носят условно отрицательный характер,

= отдельные информационные системы (хорошо разработано, даже на уровне пресловутой триады «конфиденциальность — целостность — доступность»).

СПАСИБО ЗА ВНИМАНИЕ!