



**ОБ ОЦЕНИВАНИИ УСТОЙЧИВОСТИ ФУНКЦИОНИРОВАНИЯ
ОБЪЕКТОВ КРИТИЧЕСКОЙ ИНФОРМАЦИОННОЙ
ИНФРАСТРУКТУРЫ В УСЛОВИЯХ ВОЗДЕЙСТВИЯ УГРОЗ
ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ**

доцент кафедры «Информационная безопасность» МИЭТ, к. т. н., доцент
Воеводин В.А.



Кафедра «Информационная безопасность»

Цель выступления: доложить о проблеме оценивания устойчивости функционирования объектов КИИ, функционирующих в условиях воздействия угроз ИБ и доложить об основных результатах



Для достижения цели

1. Об актуальности темы
2. О противоречивости ситуации
3. Об ограниченности инструментария
4. О проблеме
5. О полученных результатах

Об актуальности

Нацелен на эффект
административный



Директивный – преобладает
сегодня (фз-149, ст. 16)

Нацелен на эффект
экономический



Рискориентированный – внедряется
в инициативном порядке





Об актуальности

В СИЛУ ЗАКОНА ОБЛАДАТЕЛЬ ИНФОРМАЦИИ И ОПЕРАТОР
ИНФОРМАЦИОННОЙ СИСТЕМЫ ОБЯЗАНЫ, В ТОМ ЧИСЛЕ,
ОБЕСПЕЧИТЬ (ФЗ-149, СТ. 16):

А) предупреждение неблагоприятных последствий нарушения
ДОСТУПА к информации;

Б) недопущение воздействия на технические средства обработки
информации, в результате которого нарушается их
ФУНКЦИОНИРОВАНИЕ;

В) постоянный КОНТРОЛЬ за обеспечением уровня защищенности
информации.

Для чего органам управления
ИБ требуется

методический инструментарий (методы, модели и средства) для
оценивания УСТОЙЧИВОСТИ ФУНКЦИОНИРОВАНИЯ соответствующих
объектов информатизации в различных условиях обстановки



О противоречивости ситуации

Органам управления ИБ при принятии решения по обеспечению безопасности объектов КИИ в условиях воздействия угроз ИБ требуются количественные оценки устойчивости функционирования объектов КИИ



Ограниченность существующих методов, моделей и средств для оценивания устойчивости функционирования объектов КИИ, находящихся под воздействием угроз нарушения их ИБ



О противоречивости ситуации

Существующий инструментарий основан на репрезентативной статистике и допущении о стационарности и эргодичности случайного процесса отказов и восстановлений работоспособности, что позволяет применять приложение теории вероятностей и математической статистики получать своевременно достоверные оценки устойчивости функционирования для штатных условий

Для условий воздействия угроз не может быть репрезентативной статистики, поток событий поражений и восстановлений функциональности объекта не обладает стационарностью и эргодичностью и ему присуща поведенческая неопределенность

Существующего знания уже недостаточно и требуется обобщение приложений классической теории вероятностей, математической статистики для условий когда названные допущения не приемлемы и процесс не является стохастическим в классическом понимании



О противоречивости ситуации

Необходимость обобщения приложений теории вероятностей и математической статистики на случаи когда не представляется добыть репрезентативную статистику (явления весьма редки и обстановку не фиксируется), поток случайных событий поражения и восстановления не представляется принять ни стационарным (вероятностные характеристики изменяются во времени) ни эргодическим и требуется учесть фактор поведенческой неопределенности



Сформулирована научная проблема

Для исходных данных, характеризующих:

структуру объекта КИИ $S=\{A, L\}$;

сценарии воздействия угроз $\langle \{u_a\}, (n^H, n^B), \{\eta^H_j, \eta^B_j\}, (t_0, T) \rangle$;

защищенность элементов КИИ $\{p^H_j, p^B_j\}$;

Восстанавливаемость элементов $\{\tau^H_j(u_a), \tau^B_j(u_a), r_{Tp}(u_a), d_{Tp}(u_a)\}$;

Ресурсоемкость подсистемы восстановления функциональности
объекта КИИ $\Pi_0 = \{R_0, D_0\}$.

при ограничениях:

возможные состояния элементов $\langle \text{«Ф»}, \text{«ПВ»}, \text{«ПР»} \rangle$;

требуемый ресурс не превышает имеющийся $\Pi_0 \geq \Pi(t), t \in (t_0, T]$.

требуется:

разработать взаимоувязанную систему методов, моделей и средств поддержки деятельности по оцениванию устойчивости объектов КИИ функционирующих в условиях угроз $\{u_a\}$, (добывание исходных данных, их обработка и получение и интерпретацию полученных результатов).

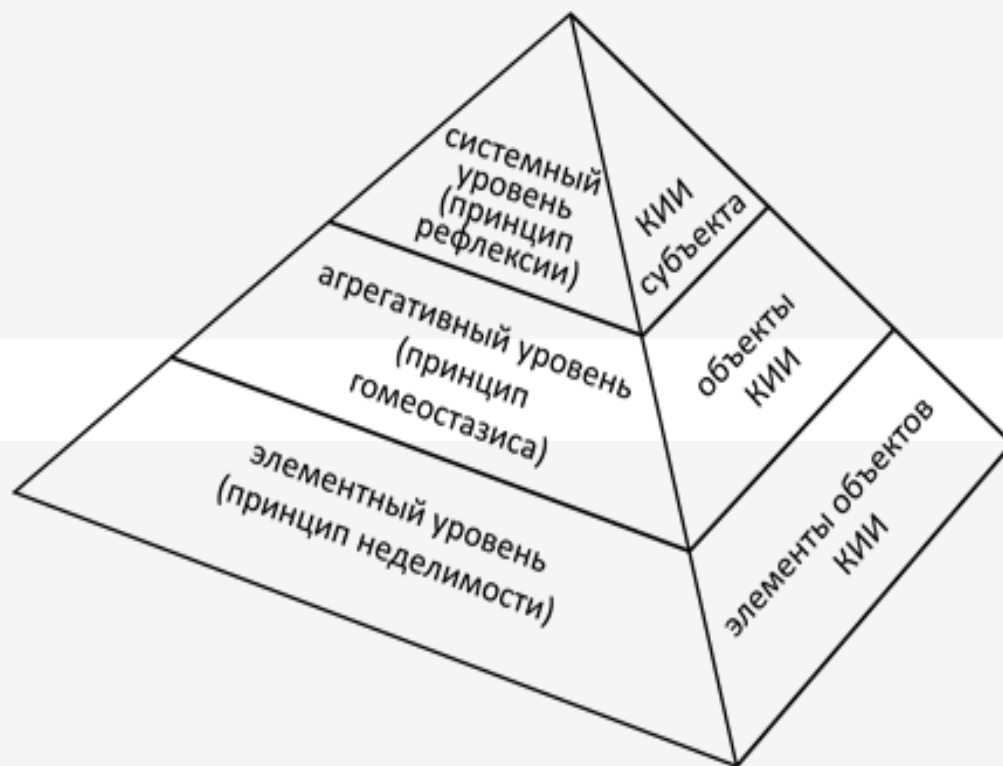


О результатах

Проанализирован существующий научный задел,
обоснована его ограниченность для разрешения проблемы
и сформулирована научная проблема и предложен порядок
ее разрешения



Иерархия методологических уровней оценок





Получены результаты

1. Разработана методология оценивания устойчивости функционирования объектов КИИ, находящиеся под воздействием угроз ИБ

при этом были решены следующие группы задач:

разработаны методы для оценивания устойчивости функционирования:

А) отдельных элементов, входящих в состав объекта КИИ;

Б) объектов КИИ, входящих в состав субъекта КИИ;

разработаны практические приложения для оценивания:

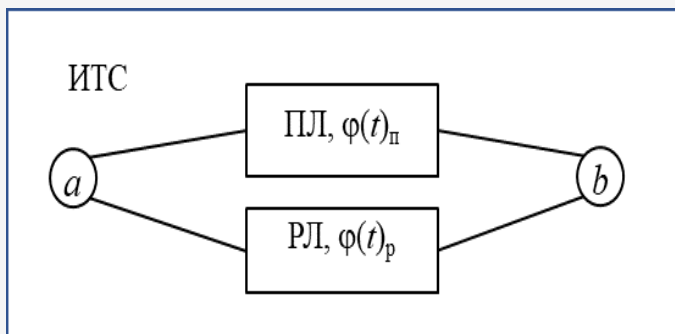
А) устойчивости функционирования объектов КИИ в условиях угроз ИБ;

Б) важности отдельных элементов в структуре объекта КИИ;

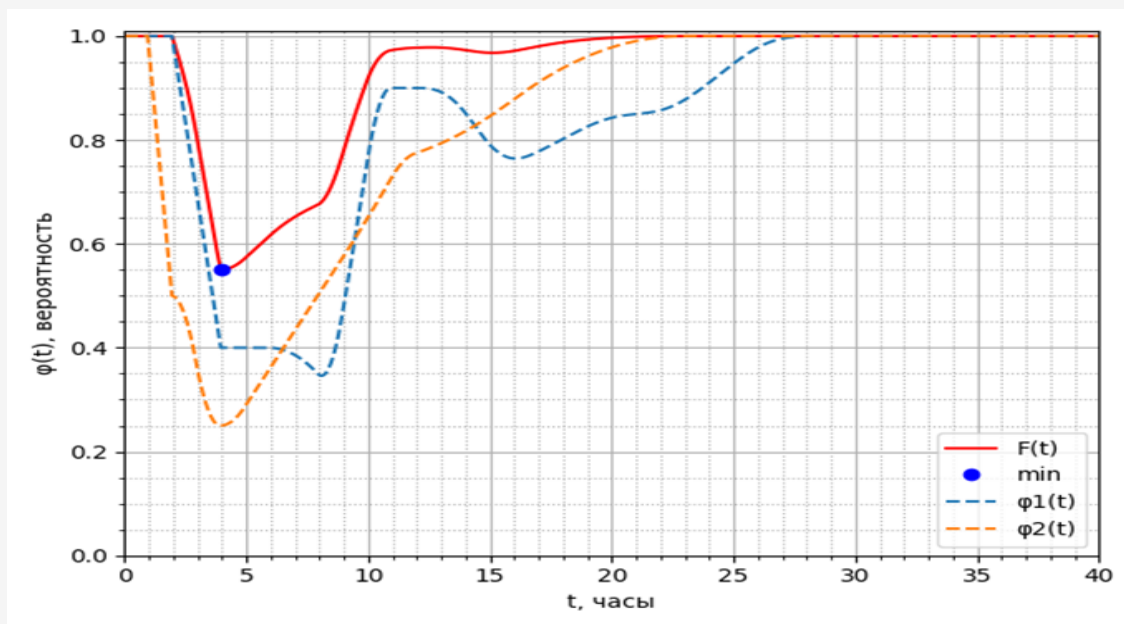
В) планов восстановления функциональности объектов КИИ, элементы которых получили повреждения в результате воздействия угроз;

Г) вариантов распределения ресурса между обеспечением защищенности элементов от воздействия угроз и их восстановления после повреждения.

Результат моделирования (для иллюстрации)



Вил направления связи	Вероятность поражения (нижняя граница)	Вероятность поражения (верхняя граница)	Время начала воздействия угроз	Время окончания воздействия угроз	Время начала восстановления	Время окончания восстановления
1	2	3	4	5	6	7
Проводная линия	0,5	0,7	2	4	6	7
Радиолиния	0,4	0,6	1	2	3	10
Проводная линия	0,2	0,3	4	6	8	12
Радиолиния	0,4	0,6	1	2	3	10





СПАСИБО ЗА ВНИМАНИЕ!

Vva541@mail.ru

<https://miet.ru/person/71166>