МЫСЛИТЬ БУДУЩИМ

ПОЛИТЕХ
Санкт-Петербургский политехнический университет Петра Великого

МИНИСТЕРСТВО НАУКИ И ВЫСШЕГО ОБРАЗОВАНИЯ РОССИЙСКОЙ ФЕДЕРАЦИИ

КРИТЕРИИ СИНТЕЗА СЕТЕВЫХ СТРУКТУР, УСТОЙЧИВЫХ К КОМПЬЮТЕРНЫМ АТАКАМ

Павленко Е.Ю., Гололобов Н.В.
Высшая Школа кибербезопасности
Института компьютерных наук и кибербезопасности СПбПУ

2

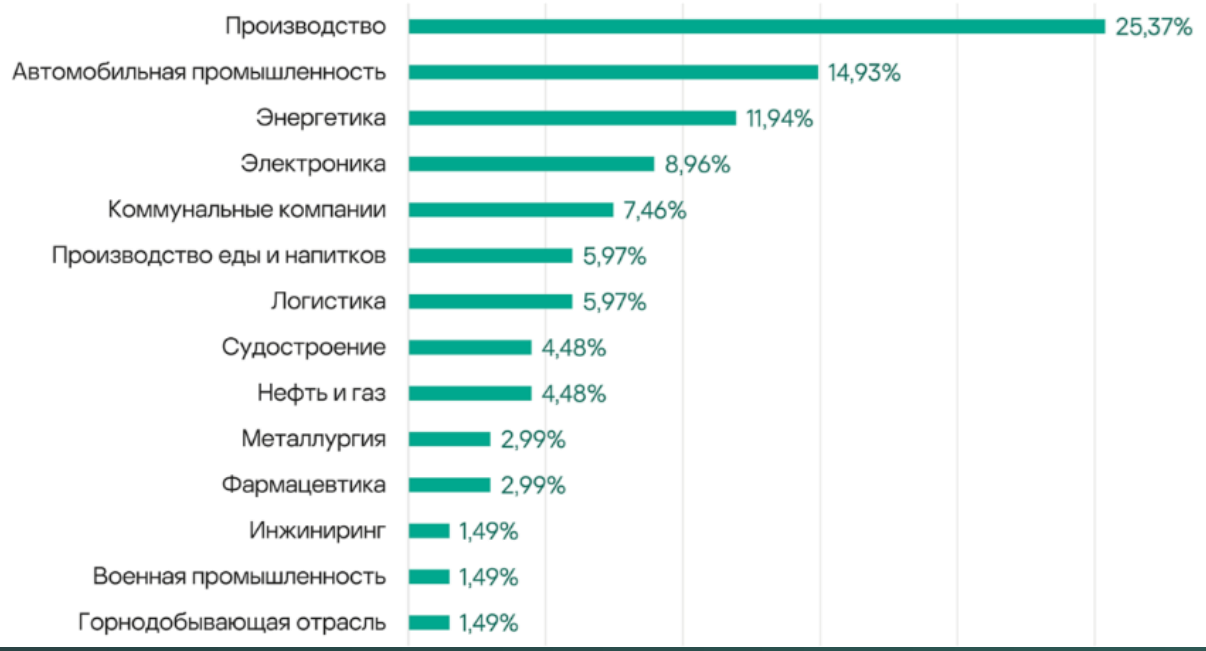
Безопасность киберфизических систем (КФС)

200 000
КИБЕРУГРОЗ
фиксируется в РФ каждую минуту

172 000
КИБЕРАТАК
отразили системы информационной безопасности Петербурга за 2023 год

6,3%
В 2024 ГОДУ
составил рост числа кибератак в РФ по сравнению с IV кварталом 2023 года

Кибератаки на промышленные КФС



Учитывая высокую интенсивность и непрекращающийся рост числа кибератак, необходимо обеспечивать корректное функционирование КФС в условиях кибератак

КИБЕРУСТОЙЧИВОСТЬ

Устойчивая сетевая структура КФС :

1. Способность системы выполнять целевую функцию (ЦФ) с заданным показателем качества и сохранять ее даже в условиях атак.
2. Способность системы к перестроению для противодействия атакам.

Статистика атак на промышленность по данным «Лаборатории Касперского»

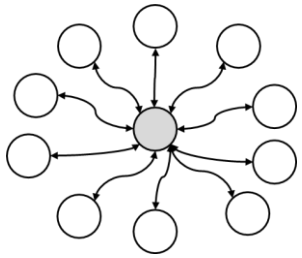
3 Графовая модель сетевой структуры КФС

Сетевая структура КФС моделируется ориентированным графом G, V – множество его вершин, E – множество дуг. Целевая функция (ЦФ) КФС представлена как множество путей на графе, характеризующееся показателем качества Q.

$$Path = A \cdot v_i^{(1)}, B \cdot v_j^{(2)}, \dots, Z \cdot v_n^{(k)}$$

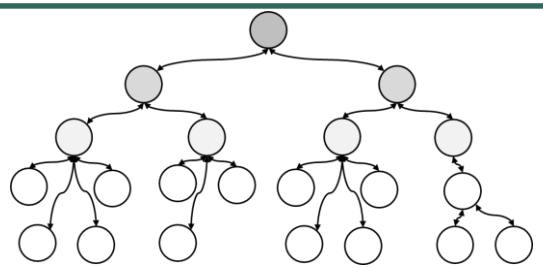
- $A, B, \dots, Z$ – целочисленные коэффициенты, характеризуют число задействованных узлов каждого типа
- $v_i, v_j, \dots, v_n$ – различные узлы заданного типа

Типы сетевых структур КФС и примеры ЦФ для них



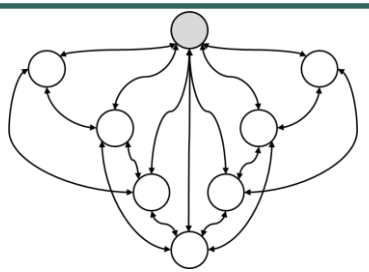
централизованная

$$\begin{cases} Path = N \cdot v_i^{(1)}, 1 \cdot v_j^{(2)} \\ Path = 1 \cdot v_j^{(2)}, N \cdot v_i^{(1)} \end{cases}$$



иерархическая

$$Path = 1 \cdot v_i^{(1)}, 2 \cdot v_j^{(2)}, 4 \cdot v_k^{(3)}, n \cdot v_l^{(4)}$$



распределенная

$$\begin{cases} Path = 1 \cdot v_i^{(1)}, 7 \cdot v_j^{(2)}, k \cdot v_k^{(2)} \\ Path = k \cdot v_k^{(2)}, 7 \cdot v_j^{(2)}, 1 \cdot v_i^{(1)} \end{cases}$$

4

Задача синтеза киберустойчивых сетевых структур

В условиях возрастающего числа кибератак на КФС, актуальна задача синтеза их киберустойчивой структуры. Выделим следующие типы синтеза:

Синтез на этапе проектирования	Синтез-восстановление при кибератаках
синтез в условиях отсутствия наблюдений за системой и знания только формального описания принципов ее работы	синтез структуры КФС путем восстановления известной ЦФ, в которой есть нарушения («разрывы»). ЦФ известна, синтез сводится к получению подграфов, восстанавливающих ЦФ

Возможные априорные ограничения на синтез:

- общее число узлов N_{max}
- число типов узлов k
- число узлов каждого типа $|v^{(i)}|$, $i = \overline{1;k}$
- максимально возможная степень узлов каждого типа $\deg(v^{(i)})$, $i = \overline{1;k}$
- ограничения по типам ребер графа (ограничения по коммуникации)
- ограничения на значения целочисленных коэффициентов $A, B, \dots, Z$

Моделирование воздействия атак на КФС для обеспечения киберустойчивости

Массированные, преимущественно случайные атаки

Простейшая математическая модель повреждения графа G: удаление множества вершин $S \subseteq V$ или ребер $S \subseteq E$.
Результирующий граф: $G'(V', E')$: $V' = V \backslash S$ или $G'(V, E')$: $E' = E \backslash S$.

Пример: DoS-атака

Сильное удаление вершин и ребер.
Результирующий граф: $G' = G \div v = G - |v|$ (в случае удаления вершин)
или $G' = G \div e = G - u - v$, здесь $e = \{u, v\}$.

Пример: атака заражения ВПО

Целенаправленные атаки, ориентированы на перехват управления

Моделирование воздействия таких атак в терминах теории графов заключается в формулировании требований к удаляемым вершинам/ребрам (множеству S).

Например, вершины с наибольшим значением центральности по степени или вершины, входящие в доминирующее множество.
Подмножество $S \subseteq V$ вершин графа называется доминирующим, если
для любой вершины $u \in V \backslash S$ существует вершина $v \in S$, такая, что $e = \{u, v\} \in E$.

6

Критерии синтеза сетевой структуры на этапе проектирования

1. В графе нет изолированных вершин – ни один компонент КФС не утратил связь с другими.
2. Задействован необходимый минимум вершин графа – синтез выполняется с учетом допустимой потери качества.
3. Граф синтезирован так, что существует хотя бы 1 путь, соответствующий ЦФ.
4. Граф синтезирован так, чтобы число вершин, которое необходимо удалить для потери связности, стремилось к максимуму. Это выражается как максимизация числа вершинной целостности $VNI(G)$.
5. Граф синтезирован так, чтобы число ребер, которое необходимо удалить для потери связности, стремилось к максимуму.
6. Граф синтезирован так, что число конфликтов между целями, достигаемыми агентам системы, и ЦФ сведено к нулю. Здесь обозначим локальные цели агентов $\{f_1, f_2, \dots, f_l\}$, а ЦФ как F, тогда оператор $confl$ оперирует f_i и F и принимает значение 0 в случае отсутствия конфликтов.

$$\begin{cases} \nexists\, v_i \in G: \deg(v_i) = 0 \\ |N_{max} - N| \to max \\ Path \neq \emptyset \\ VNI(G) \to max \\ ENI(G) \to \beta_1(G) \\ confl(f_i, F) = 0 \;\forall\, f_i \end{cases}$$

$$VNI(G) = \min_{S \subseteq V}\{|S| + w(G \div S)\}$$

где $w(G \div S)$ – порядок наибольшей компоненты связности графа $G \div S$, который получается из исходного графа G путем сильного удаления всех вершин, входящих в $S \subseteq V$.

$$ENI(G) = \min_{S \subseteq E}\{|S| + w(G \div S)\}$$

где $w(G \div S)$ – порядок наибольшей компоненты связности графа $G \div S$, который получается из исходного графа G путем сильного удаления всех ребер, входящих в $S \subseteq V$.

Критерии синтеза-восстановления сетевой структуры КФС

Если необходимо только восстановить поврежденные участки «пути» на графе, реализующем ЦФ, задача сводится к поиску компонентов КФС, которые способны заменить поврежденные.

подграфы пути $Path_i$ и $Path_j$ функционально изоморфны тогда и только тогда, когда выполняются условия:

- сохраняется заданная последовательность по типам узлов $v^{(i)} - v^{(j)} - v^{(k)} - \cdots - v^{(m)}$ с учетом определенных операций над путями;
- качество реализации ЦФ остается в заданном диапазоне: $Q(Path_i) \in [Q_{min}; Q_{max}], Q(Path_j) \in [Q_{min}; Q_{max}]$.

$$\begin{cases} \exists\, Path' : Path' \sim Path \;\; Q' \in [Q_{min}; Q_{max}] \\ t_r(Path') \rightarrow \\ DI(G) \rightarrow max \\ G_{Cr,i} = \left(V_{Cr}^{(i)}, E_{Cr}\right) \rightarrow K_{N_{Cr}}^{(i)}, i = \overline{1,k} \\ E - I\ index = \dfrac{E - I}{E + I} \rightarrow max \\ action(v_i) \longrightarrow action'(v_i) \Leftrightarrow q(f'_i) \longrightarrow q_{max}\ AND\ q(f'_i) > q_{min} \end{cases}$$

- **Минимизация времени**
- **Максимизация числа ребер между критическими узлами**
- **Максимизация показателя доминирующей целостности $DI(G)$**
- **Максимизация значения коэффициента Кракхардта E/I**

Пример синтеза киберустойчивой иерархической сетевой структуры

ЦФ и параметры синтеза

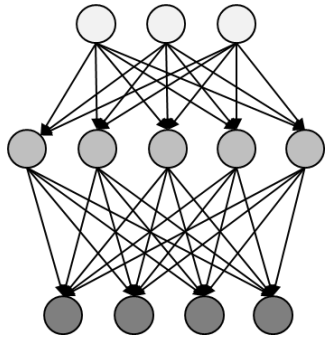
$$Path = \mathrm{A} \cdot v_i^{(1)}, \mathrm{B} \cdot v_j^{(2)}, \mathrm{C} \cdot v_k^{(3)}$$

$$A = \{2,\ 3\}$$
$$B = \{3, 4, 5\}$$
$$C = \{3, 4\}$$

1. Синтез для Q_{max} и Q_{min}

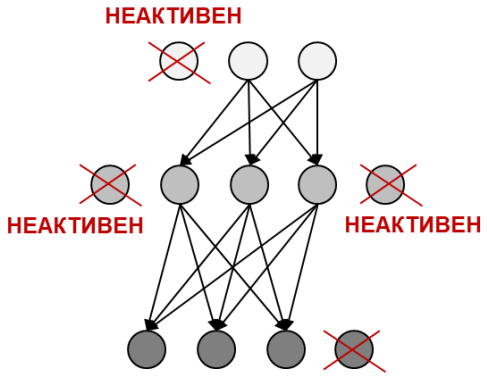
Q_{max}:

$$Path = 3 \cdot v_i^{(1)}, 5 \cdot v_j^{(2)}, 4 \cdot v_k^{(3)}$$

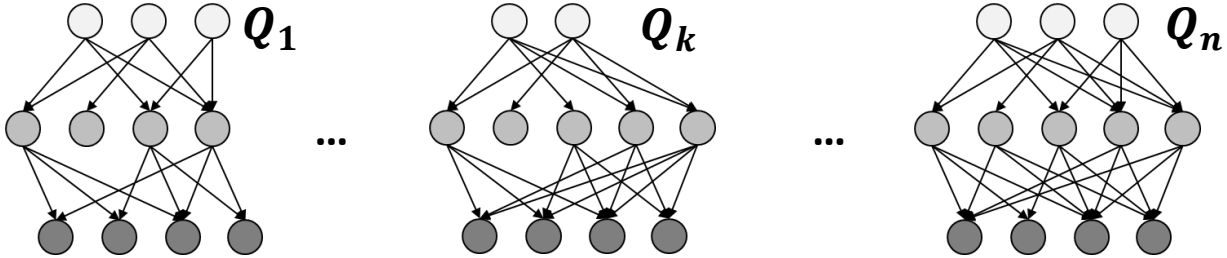


Q_{min}:

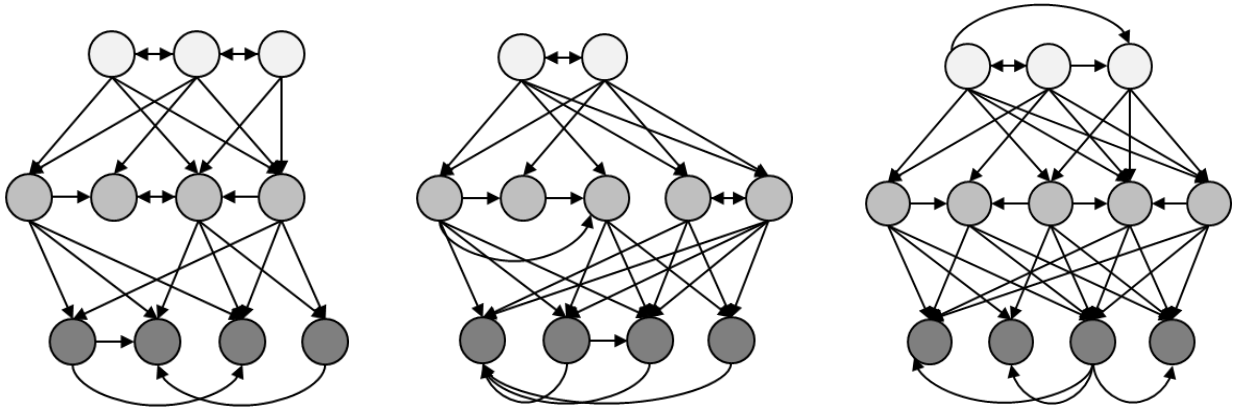
$$Path = 2 \cdot v_i^{(1)}, 3 \cdot v_j^{(2)}, 3 \cdot v_k^{(3)}$$



2. Максимизация числа путей ЦФ



3. Обеспечение киберустойчивости



4. Ранжирование и выбор структуры КФС

Дальнейшие направления исследований

ПОЛИТЕХ

Экспериментальные исследования по синтезу всех типов сетевых структур КФС

Решение оптимизационной задачи ранжирования синтезированных вариантов структуры сети с использованием искусственных нейронных сетей

Разработка показателей киберустойчивости, связанных с предельными параметрами синтеза в части вершинной и реберной связности

Решение задачи синтеза киберустойчивых сетевых структур обеспечит:

Повышение уровня защищенности критической информационной структуры РФ	Создание новых, киберустойчивых систем для различных отраслей деятельности	Расширение научно-практической базы обеспечения кибербезопасности

Санкт-Петербургский политехнический университет Петра Великого

Контакты:

kafedra@ibks.spbstu.ru
Тел.: 552-76-32