ПОЛИТЕХ
Институт кибербезопасности
и защиты информации

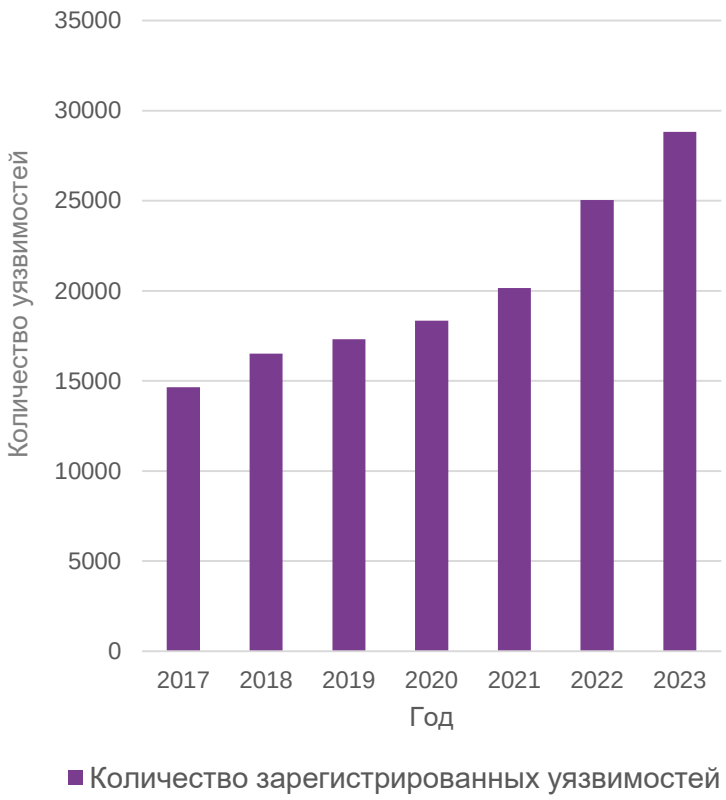
Министерство науки и высшего образования Российской Федерации
Санкт-Петербургский политехнический университет Петра Великого
Институт компьютерных наук и кибербезопасности

ТЕХНОЛОГИЯ ЗАЩИТНОЙ АДАПТИВНОЙ ВИРТУАЛИЗАЦИИ ФУНКЦИОНАЛЬНЫХ СЕТЕЙ КИБЕРФИЗИЧЕСКИХ СИСТЕМ

Докладчик
Е.В. Завадский

Санкт-Петербург – 2024

Актуальность



Увеличение пула эксплуатируемых уязвимостей, в том числе «нулевого дня»

65% компаний по всему миру сталкиваются с целевыми атаками (APT)

40% компаний, столкнувшихся с кибератакой, прервали свою деятельность не менее чем на 8 часов

Межсетевые экраны, IDS / IPS, средства на основе машинного обучения не могут противодействовать новым векторам атак

Необходим новый комплексный подход к обеспечению безопасности объектов КФС

Граф функциональных зависимостей

Узлы графа функциональных зависимостей

$$V = \{v_1, v_2, \dots, v_n\}$$

Функции, поддерживаемые узлом $\boldsymbol{v_i}$

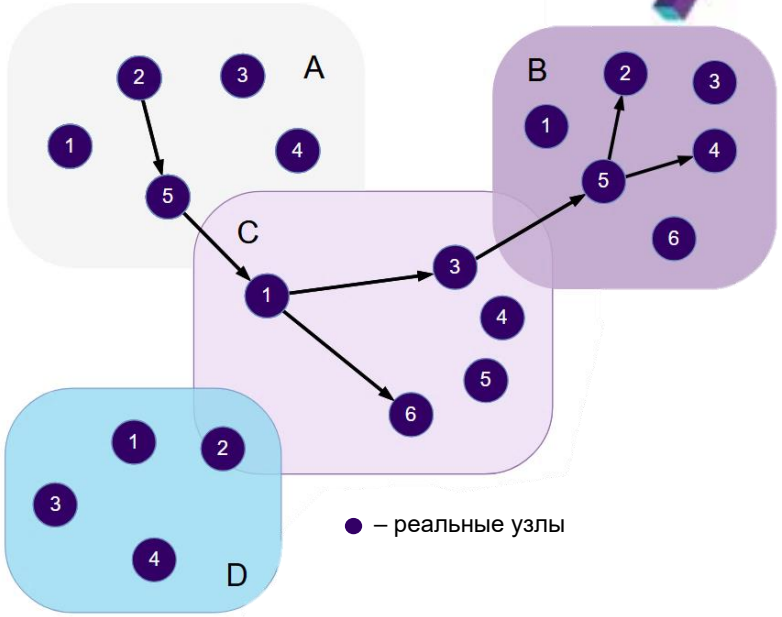
$$F_{v_i} = \left\{ f_1^{(i)}, f_2^{(i)}, \dots \right\}$$

Технологический процесс

$$P_{process}^{(j)} = \left\{ f_1^{(j)}, f_2^{(j)}, \dots, f_n^{(j)} \right\}$$

Реализация технологического процесса

$$R_{process_j} = \left\{ v_1^{(j)}, v_2^{(j)}, \dots, v_n^{(j)} \mid f_{j_1} \in F_{v_1^{(j)}} \,\&\, \dots \,\&\, f_{j_n} \in F_{v_n^{(j)}} \right\}$$



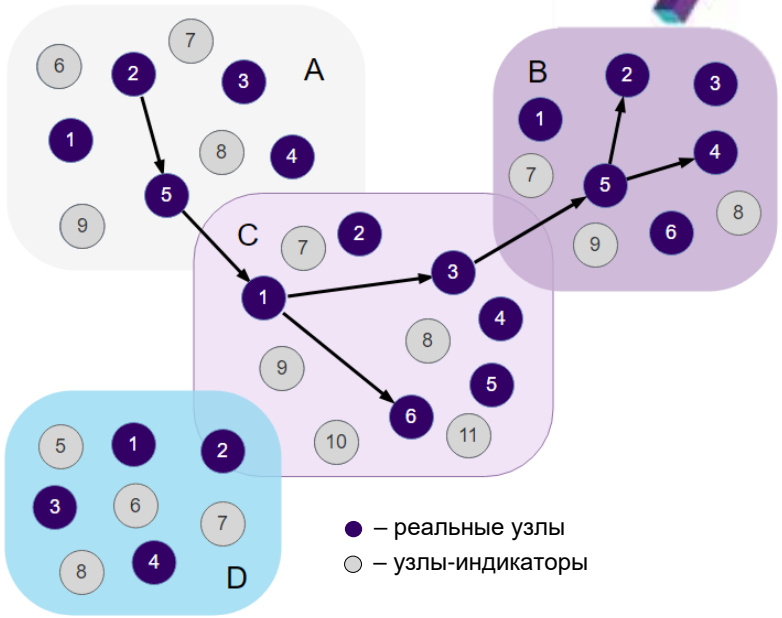
Граф функциональных зависимостей

Выявление наличия вредоносного воздействия

Свойства узлов–индикаторов ($v_{indicator}$)

- Виртуальность
- Неотличимость от узлов реальной сети
- Отсутствие объектов приманок, свойственных Deception-системам
- Полный внешний контроль над операционной системой узла со стороны команды защиты
- Отсутствие штатного сетевого взаимодействия

Обращение к узлу-индикатору → Выявление факта вредоносного воздействия



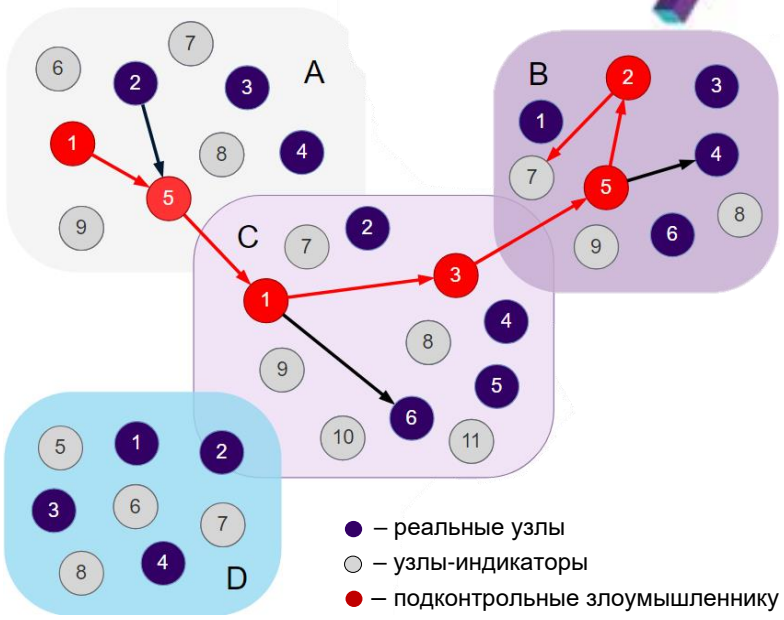
Граф функциональных зависимостей

Выявление наличия вредоносного воздействия

Свойства узлов–индикаторов ($v_{indicator}$)

- Виртуальность
- Неотличимость от узлов реальной сети
- Отсутствие объектов приманок, свойственных Deception-системам
- Полный внешний контроль над операционной системой узла со стороны команды защиты
- Отсутствие штатного сетевого взаимодействия

Обращение к узлу-индикатору → Выявление факта вредоносного воздействия



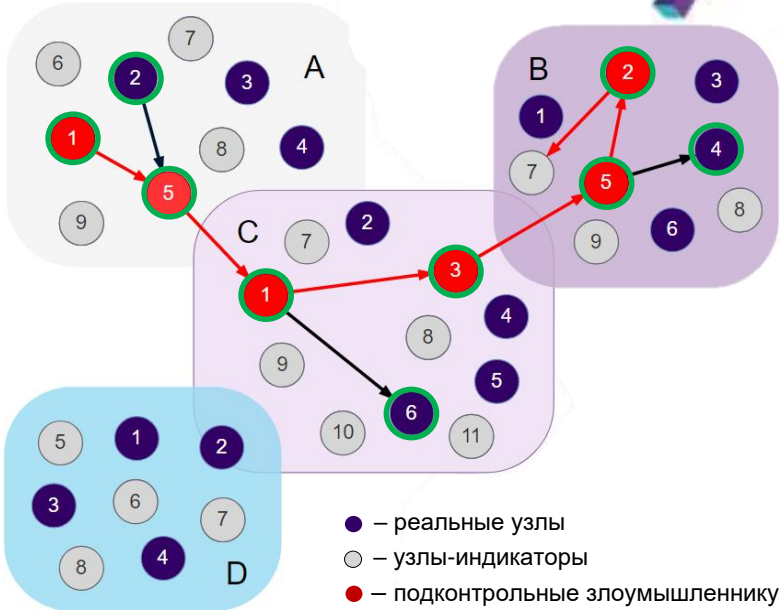
Граф функциональных зависимостей

Определение множества скомпрометированных узлов

Определение №1

Скомпрометированным считается каждый узел, который включен в граф $G_{interaction}$, построенный при помощи способа обратного распространения от узла-индикатора по цепочке сетевых взаимодействий

$$v_i \in V_{compromised}, \text{если } v \in V(G_{interaction})$$



Граф функциональных зависимостей

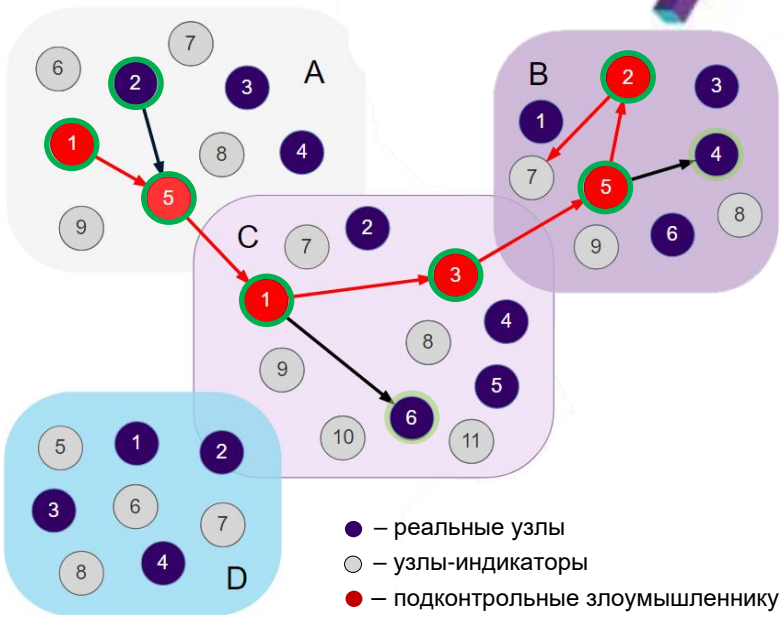
Определение множества скомпрометированных узлов (2)

Определение №2

Узел считается скомпрометированным в том случае, если он включен в граф, полученный в результате пересечения графа потенциальных атак G_{attack} для затронутого узла-индикатора и графа $G_{interaction}$

$$v_i \in V_{compromised}, \text{если } v \in V(G_{interaction} \cap G_{attack}) \cup \{v_{interaction}\}$$

$$V(G_{attack}^{v_{B/7}}) = \{v_{A/1}, v_{A/2}, v_{A/3}, v_{A/5}, v_{C/1}, v_{C/3}, v_{B/5}, v_{B/1}, v_{B/2}, v_{B/3}\}$$



Граф функциональных зависимостей

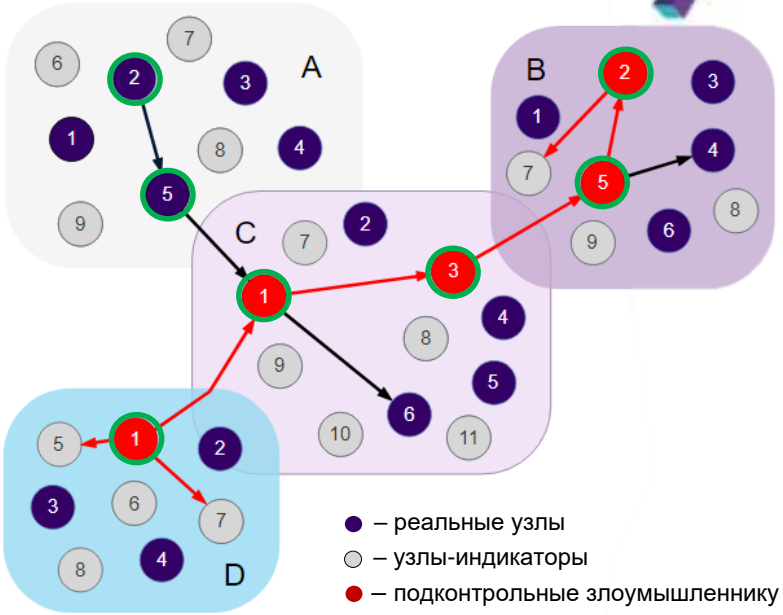
Определение множества скомпрометированных узлов (3)

Определение №2*

Узел считается скомпрометированным в том случае, если он включен в граф, полученный в результате пересечения графа, являющегося объединением графов потенциальных атак G_{attack} затронутых узлов-индикаторов, и графа $G_{interaction}$

$$v_i \in V_{compromised}, \text{если } v \in V(G_{interaction} \cap (G_{attack}^{(1)} \cup G_{attack}^{(2)} \cup \cdots)) \cup \{v_{interaction}\}$$

$$V(G_{attack}^{v_{B/7}}) = \{v_{A/1}, v_{A/2}, v_{A/3}, v_{A/5}, v_{C/1}, v_{C/3}, v_{B/3}, v_{B/1}, v_{B/2}, v_{B/3}\}$$
$$V(G_{attack}^{v_{D/5}}) = \{v_{A/1}, v_{A/2}, v_{A/5}, v_{C/1}, v_{D/1}, v_{D/3}\}$$
$$V(G_{attack}^{v_{D/7}}) = \{v_{D/1}, v_{D/2}, v_{D/3}\}$$



Граф функциональных зависимостей

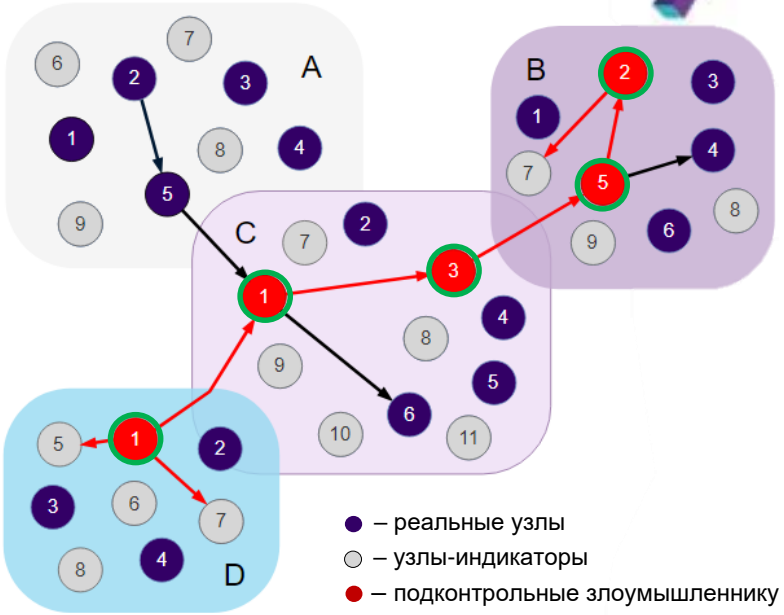
Определение множества скомпрометированных узлов (4)

Определение №3

Узел является нескомпрометированным, если узлы-индикаторы не сигнализируют о вредоносном воздействии с его стороны, и он не входит в трассу, объединяющую затронутые в ходе атаки узлы-индикаторы

$$v_i \notin V_{compromised}, \text{если}$$
$$\left(\forall\, v_{indicator}^{(j)}:\ is_signal\left(v_{indicator}^{(j)}\right) = false\right) \&$$
$$(v_i \notin s_{km} =< v_{indicator}^{(k)}, \dots, v_{indicator}^{(m)} >,$$
$$\forall\, v_{indicator}^{(k)}, v_{indicator}^{(m)}$$
$$is_signal\left(v_{indicator}^{(k)}\right) = true, is_signal\left(v_{indicator}^{(m)}\right) = true\ )$$

$$V(G_{attack}^{v_{B/7}}) = \{v_{A/1}, v_{A/2}, v_{A/3}, v_{A/5}, v_{C/1}, v_{C/3}, v_{B/3}, v_{B/1}, v_{B/2}, v_{B/3}\}$$
$$V(G_{attack}^{v_{D/5}}) = \{v_{A/1}, v_{A/2}, v_{A/5}, v_{C/1}, v_{D/1}, v_{D/3}\}$$
$$V(G_{attack}^{v_{D/7}}) = \{v_{D/1}, v_{D/2}, v_{D/3}\}$$



Граф функциональных зависимостей

Определение множества скомпрометированных узлов (5)

Алгоритм выявления и исключения скомпрометированных узлов

Обнаружение вредоносных воздействий → Выделение скомпрометированных узлов в изолированную сеть → Исключение скомпрометированных узлов из защищенной сети → Изменение маршрута реализации процесса → Выделение поведенческих сигнатур скомпрометированных узлов → Обнаружение оставшихся скомпрометированных узлов в сети с помощью выделенных сигнатур

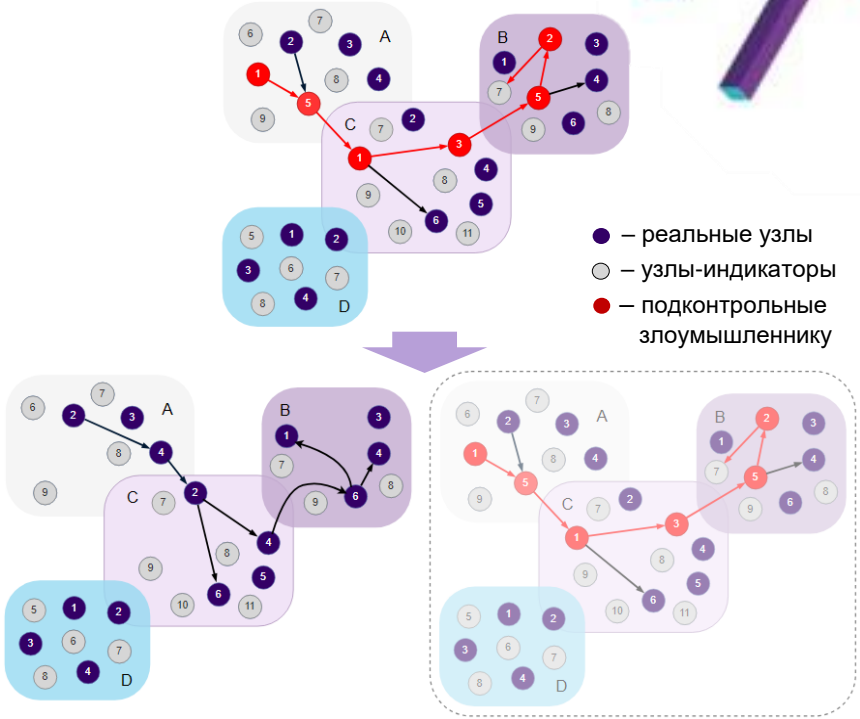


Схема перестроения сетевой инфраструктуры КФС

Тестирование предложенного решения
Атака шифровальщика

Компрометация узлов

Противодействие системы

1 *A/2*

2 *A/1, A/3, A/5, A/6, A/7*

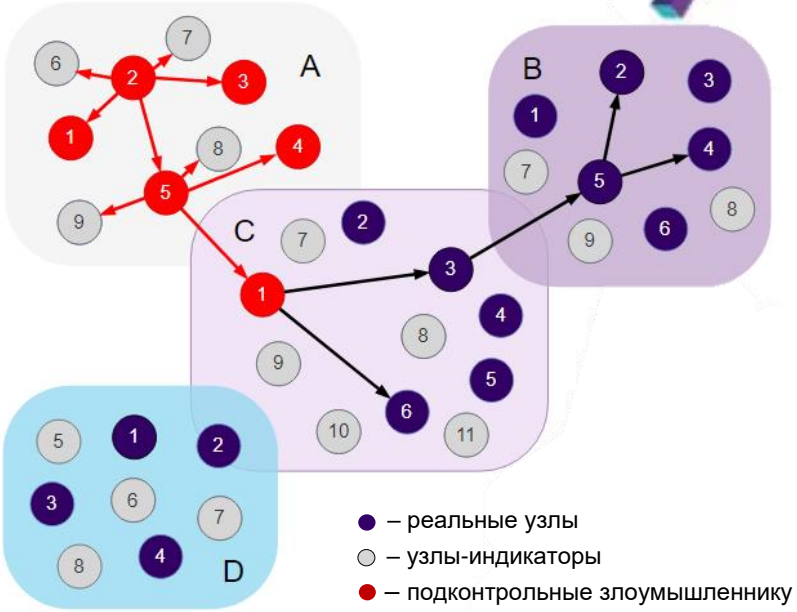
3 *A/1, A/2, A/3*

4 *C/1, A/4, A/8, A/9*

5 *C/1, A/4, A/8, A/9*

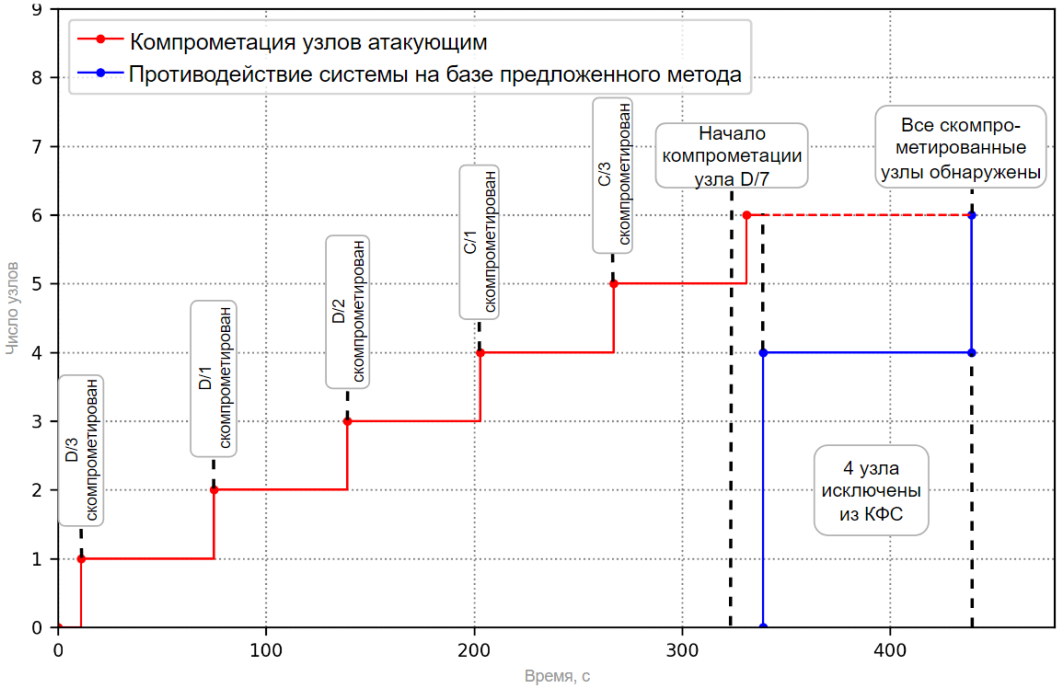
$$V(G_{attack}^{v_{A/6}}) = \{v_{A/1}, v_{A/2}, v_{A/3}\}$$

$$V(G_{attack}^{v_{A/7}}) = \begin{Bmatrix} v_{A/1}, v_{A/2}, v_{A/3}, \\ v_{C/2}, v_{D/1}, v_{D/2} \end{Bmatrix}$$

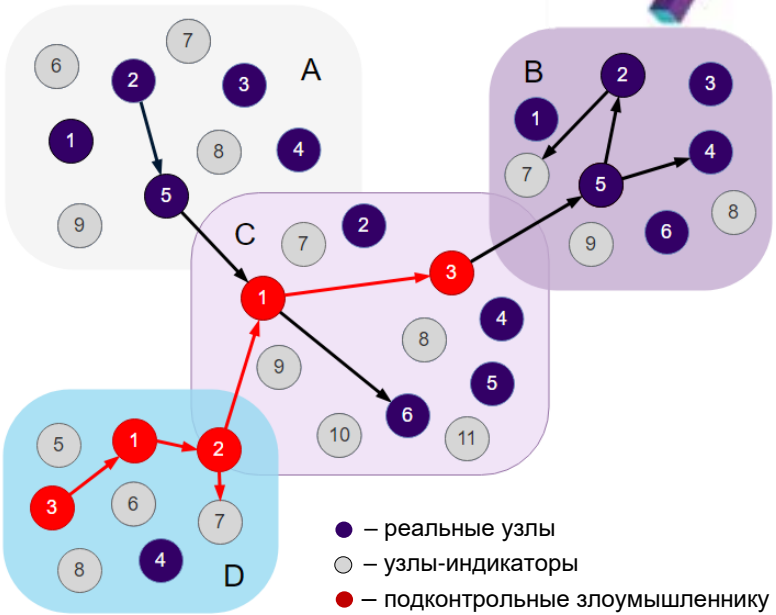


Граф функциональных зависимостей. Атака шифровальщика

Тестирование предложенного решения
APT-атака



$$V(G_{attack}^{v_{D/7}}) = \{v_{D/1}, v_{D/2}, v_{D/3}\}$$



Граф функциональных зависимостей. APT-атака

Сравнение предложенного решения с существующими

Название	Возможность обнаружения неизвестных атак	Автономность	Синтез новых поведенческих сигнатур	Ресурсозатараты
Honeypot / Deception-системы	+	–	–	Низкие
IDS / Методы машинного обучения	–	–	–	Низкие
Биоподобный / Иммунный подход	+	+	–	Низкие
Разработанное решение	+	+	+	Высокие

Результаты

- Предложена новая методика активного обнаружения и противодействия кибервторжениям для усиления защиты функциональной инфраструктуры критических КФС.

- Метод анализа графа функциональных зависимостей обеспечивает идентификацию скомпрометированных узлов в процессе атаки.

- Метод противодействия развивающейся атаке с помощью реконфигурации функциональной инфраструктуры перемещает скомпрометированные узлы в изолированную виртуальную сеть для анализа их поведения, выполнения "работы над ошибками" и повторного построения технологического процесса с незатронутыми узлами.

- Экспериментальное моделирование продемонстрировало корректную работу предложенной методики при атаках APT и программ-вымогателей.