«РАЗРАБОТКА ПОДХОДА К СНИЖЕНИЮ РАЗМЕРНОСТИ ПРОСТРАНСТВА ПРИЗНАКОВ УГРОЗ В ИНТЕЛЛЕКТУАЛЬНЫХ СИСТЕМАХ ОБЕСПЕЧИВАНИЯ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ»

Пеливан М.А.
Будников С.А.

Актуальность

Факторы:

- повсеместное внедрение компьютерных технологий;
- постоянное увеличение возможного ущерба от компьютерных атак;
- необходимость оценки эффективности мер защиты;
- большое количество оцениваемых признаков реализации угроз.

Проблема:

большая трудоемкость анализа признаков реализации угроз

Цель и задачи

Цель:

разработка методики снижения размерности пространства возможных условий и последствий реализации угроз безопасности информации.

Задачи:

- формирование групп признаков меньшей размерности;
- определение значимых признаков в сформированных группах.

Базы данных угроз и уязвимостей

Common Vulnerabilities and Exposures

NVD

ATT&CK®

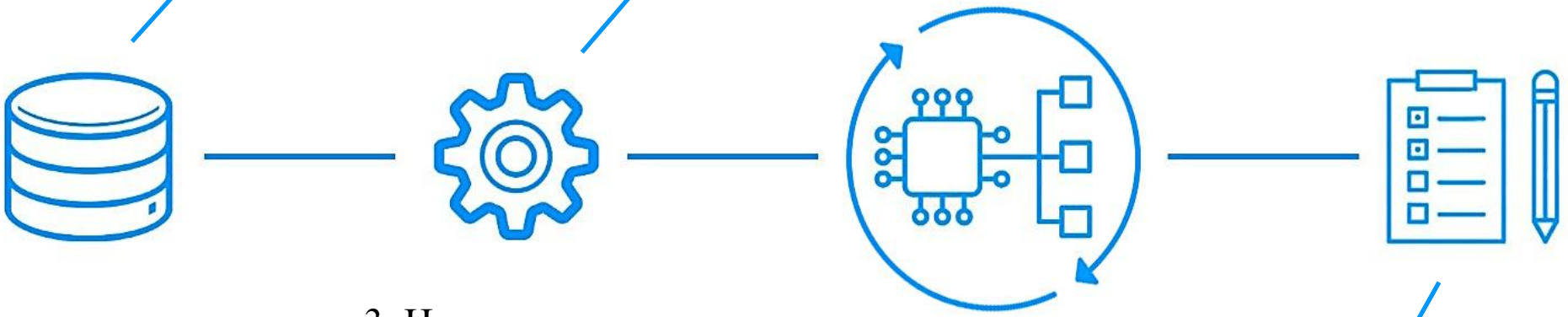
Банк данных угроз безопасности информации (БДУ) ФСТЭК России, функционирует с 2015 года в России. БДУ содержит сведения об основных угрозах безопасности информации и уязвимостях, в первую очередь, характерных для объектов критической информационной инфраструктуры

На текущий момент БДУ содержит 217 угроз и 27843 уязвимости, 135 объектов воздействия, 6 типов нарушителей (источников угрозы), а также 7 видов последствий реализации угрозы

Методика снижения размерности пространства

1. Определение исходных данных

2. Определение количества формируемых кластеров (MATLAB)



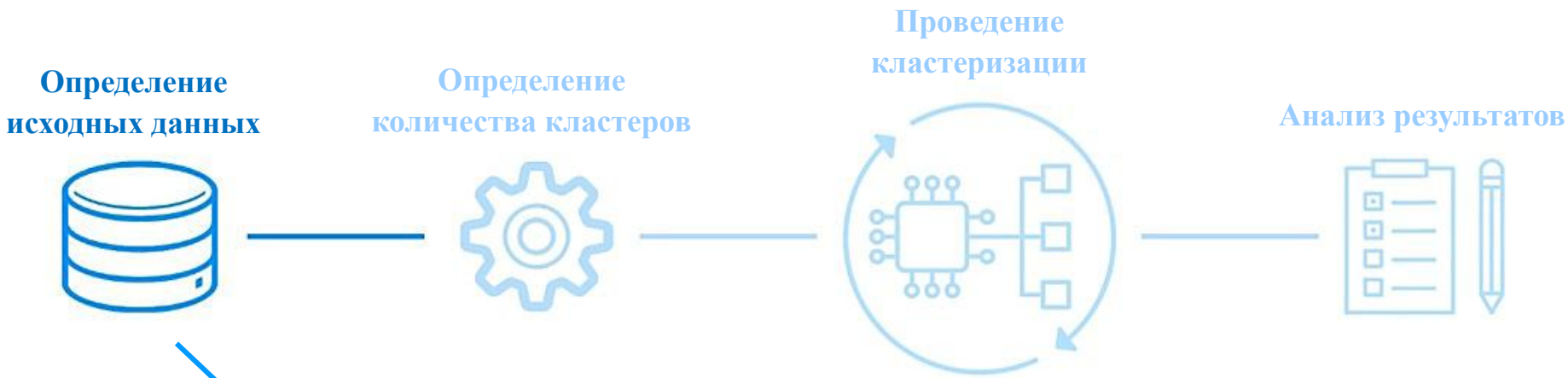
3. Циклическое проведение процедур кластеризации методом k-средних (STATISTICA)

4. Анализ результата

Методика снижения размерности пространства

Этап 1

Определение исходных данных (объектов кластеризации)



Исходные данные:

- 135 объектов воздействия;
- 6 типов нарушителей (источников угрозы);
- 7 видов последствий реализации угрозы;
- 2 критерия кластеризации

Исходные данные

Последствия реализации угроз

- нарушение конфиденциальности, целостности и доступности (КЦД);
- нарушение конфиденциальности и целостности (КЦ);
- нарушение конфиденциальности и доступности (КД);
- нарушение целостности и доступности (ЦД);
- нарушение конфиденциальности (К);
- нарушение целостности (Ц);
- нарушение доступности (Д).

Потенциал нарушителя

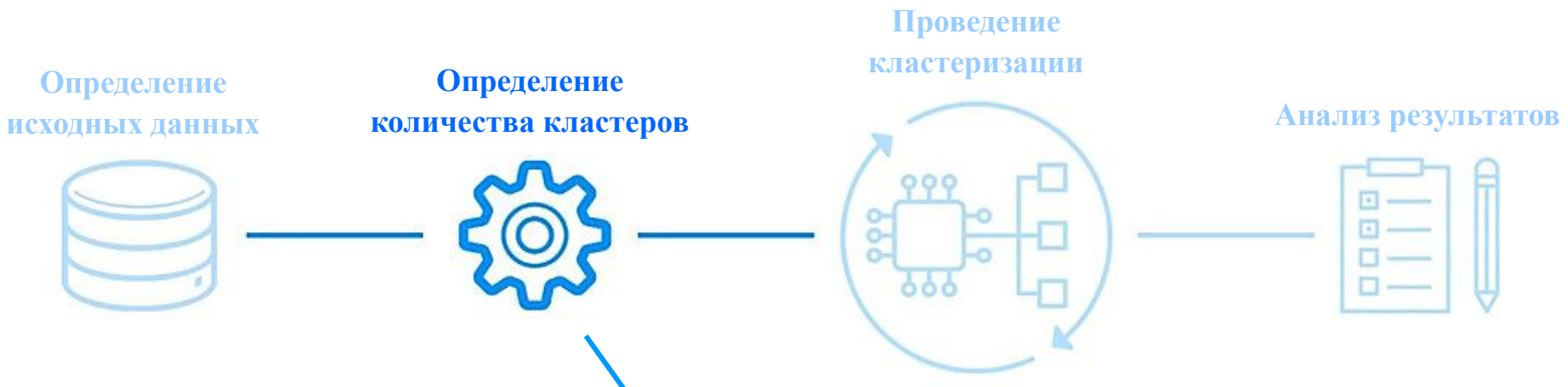
- внешний нарушитель с высоким потенциалом (ВншНВП);
- внешний нарушитель со средним потенциалом (ВншНСП);
- внешний нарушитель с низким потенциалом (ВншННП);
- внутренний нарушитель с высоким потенциалом (ВнтНВП);
- внутренний нарушитель со средним потенциалом (ВнтНСП);
- внутренний нарушитель с низким потенциалом (ВнтННП).

Критерии кластеризации

- последствия реализации угроз;
- потенциал нарушителя.

Методика снижения размерности пространства

Этап 2
Определение количества формируемых кластеров



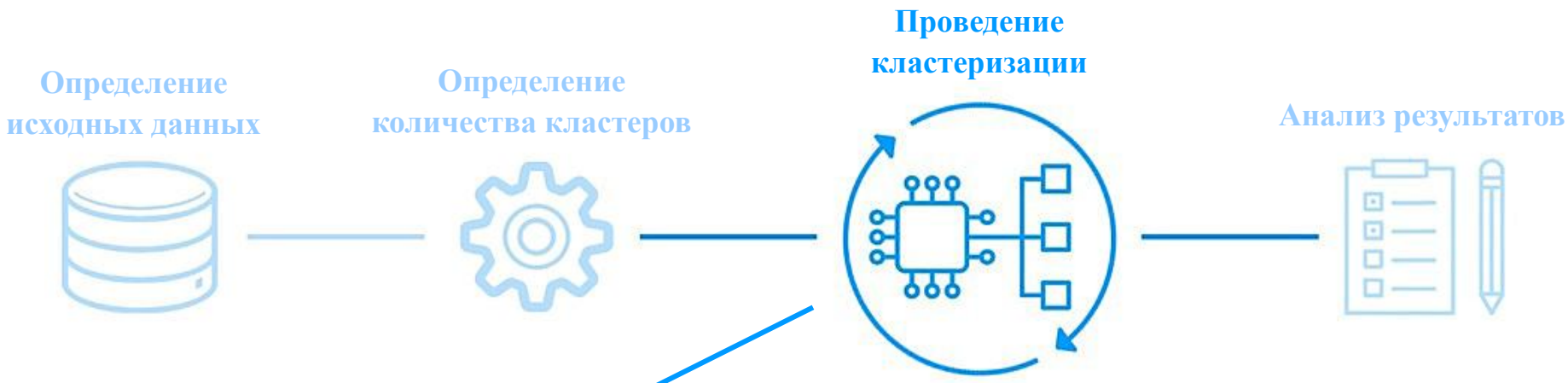
Использование субтрактивной кластеризации:

- последствия реализации угроз - 5 кластеров
- потенциал нарушителя - 5 кластеров

Методика снижения размерности пространства

Этап 3

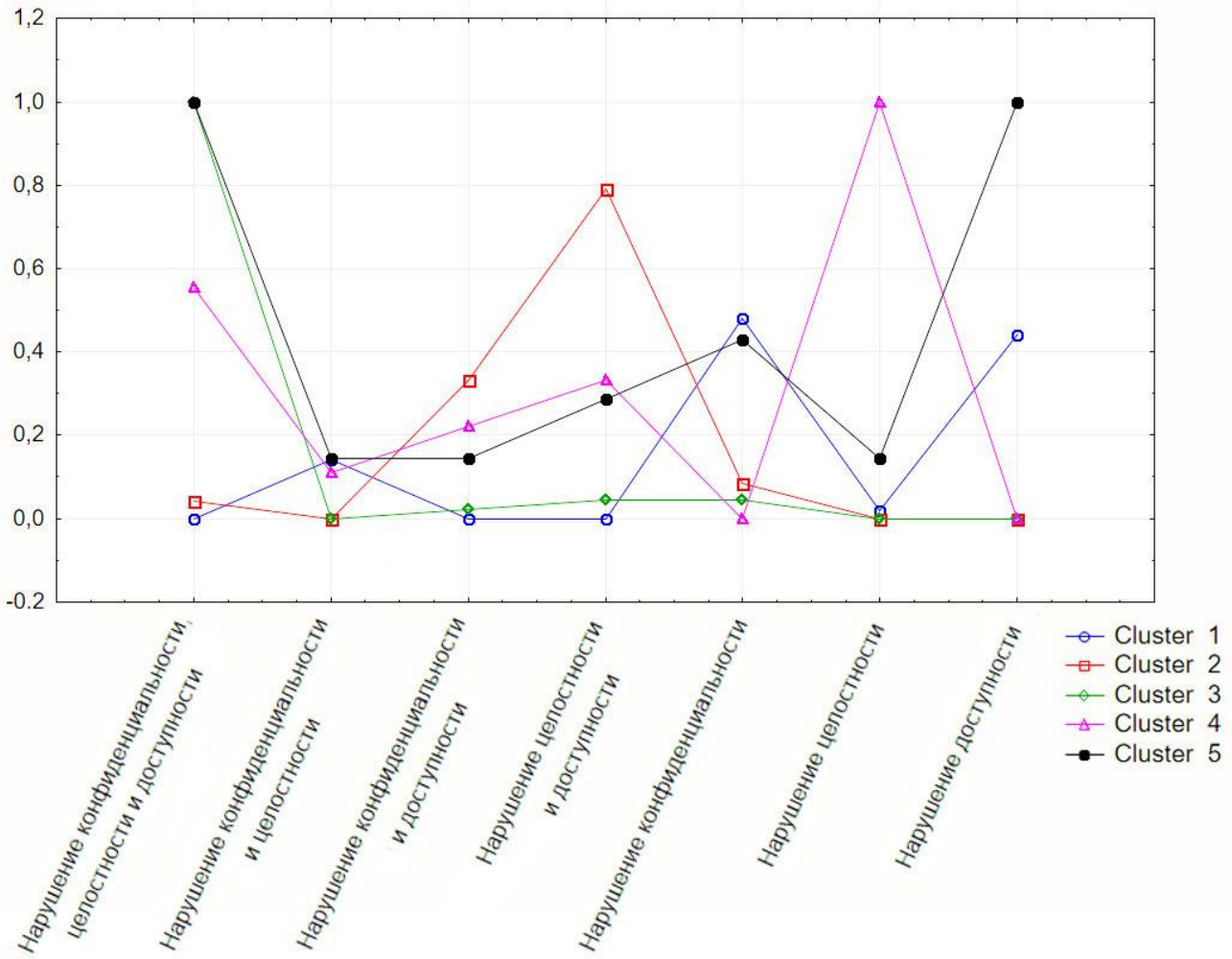
Проведение нескольких итераций процедур кластеризации методом k-средних и выбор наилучшего результата кластеризации



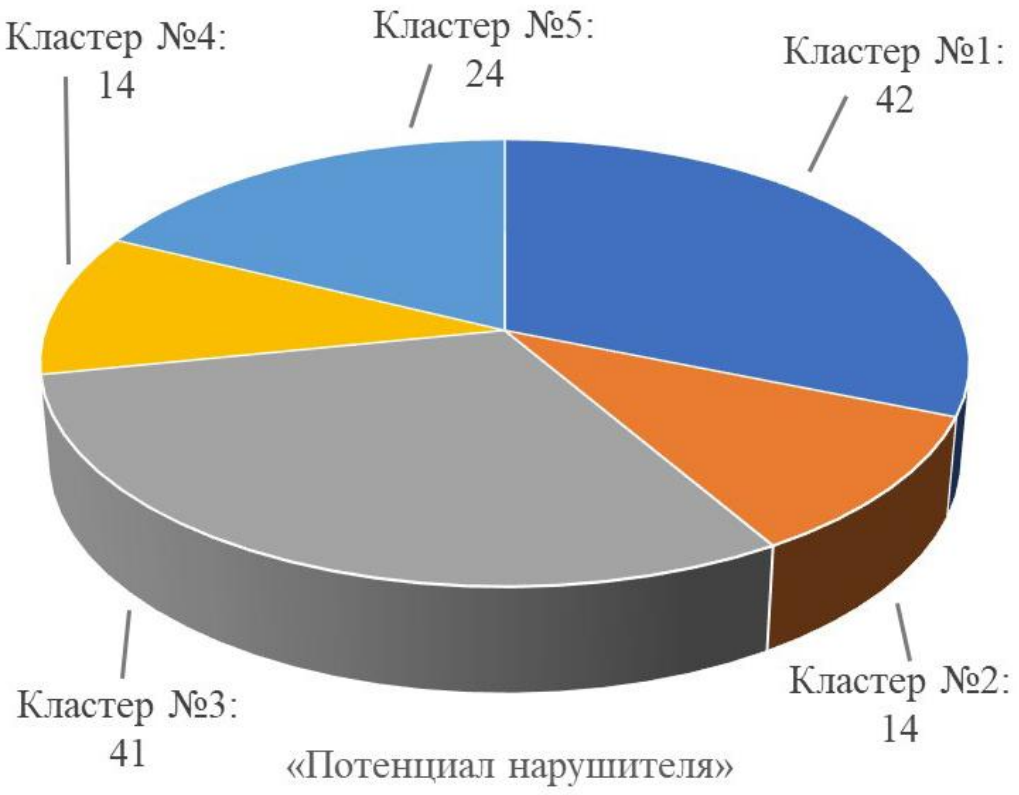
Способы выбора начальных центров кластеров:

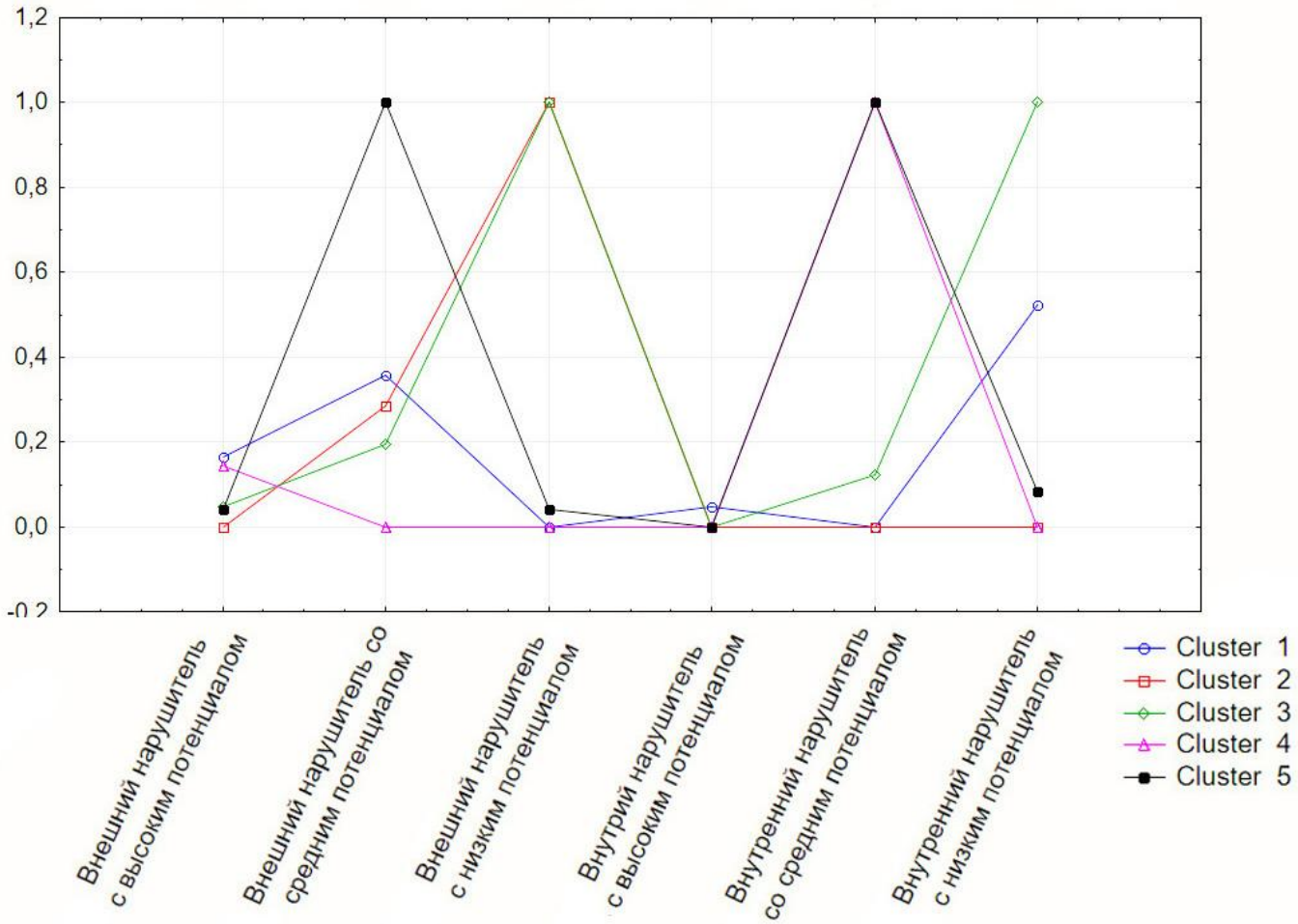
- выбор первых n (число кластеров) наблюдений;
- максимизация начальных расстояний между кластерами;
- сортировка расстояний и выбор наблюдений на постоянных интервалах.

Результат кластеризации по критерию кластеризации «Последствия реализации угроз»



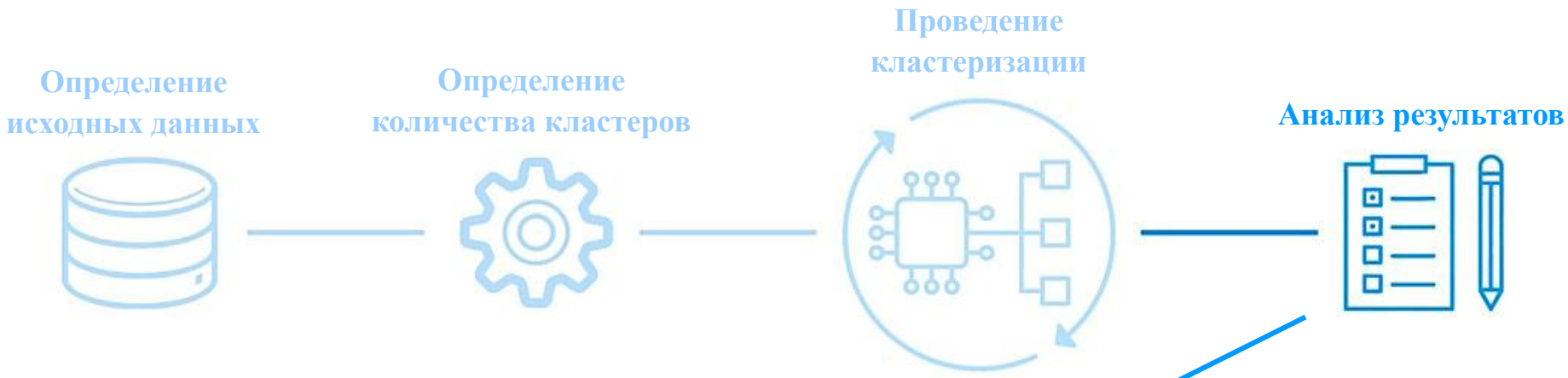
Результат кластеризации по критерию кластеризации «Потенциал нарушителя»





Методика снижения размерности пространства

Этап 4
Анализ полученных кластеров



Анализ результатов

- вычисление средних значений;
- вычисление дисперсии;
- принятие решения о значимости признака на основе критерия Сэвиджа

Результат определения значимых признаков кластеров по критерию «Последствия реализации угроз»

Значимые признаки объектов кластеризации

кластер № 1

нарушения конфиденциальности и нарушения доступности;

кластер № 2

нарушения целостности и доступности;

кластер № 3

нарушения конфиденциальности, целостности и доступности;

кластер № 4

нарушения конфиденциальности, целостности и доступности, а также нарушения целостности;

кластер № 5

нарушения конфиденциальности, целостности и доступности, а также нарушения доступности.

Значения критерия Сэвиджа

Последствия реализации угроз Значение критерия Сэвиджа	Нарушение КЦД	Нарушение КЦ	Нарушение КД	Нарушение ЦД	Нарушение К	Нарушение Ц	Нарушение Д
Кластер №1	0,5	0,36	0,5	0,5	0	0,48	0,06
Кластер №2	0,75	0,79	0,46	0,06	0,69	0,79	0,79
Кластер №3	0,04	1	0,98	0,96	1	1	1
Кластер №4	0,44	0,89	0,78	0,67	1	0,28	1
Кластер №5	0,3	0,86	0,86	0,71	0,6	0,86	0,3

Результат определения значимых признаков кластеров по критерию «Потенциал нарушителя»

Значимые признаки объектов кластеризации

кластер № 1

нарушения, совершаемые внешними нарушителями со средним потенциалом и внутренними нарушителями с низким потенциалом;

кластер № 2

нарушения, совершаемые внешними нарушителями с низким потенциалом;

кластер № 3

нарушения, совершаемые нарушителями с низким потенциалом;

кластер № 4

нарушения, совершаемые внутренними нарушителями со средним потенциалом;

кластер № 5

нарушения, совершаемые нарушителями со средним потенциалом

Значения критерия Сэвиджа

Потенциал нарушителя / Значение критерия Сэвиджа	ВншНВП	ВншНСП	ВншННП	ВнтНВП	ВнтНСП	ВнтННП
Кластер №1	0,35	0,16	0,52	0,47	0,52	0
Кластер №2	1	0,71	0,22	1	1	1
Кластер №3	0,95	0,8	0,16	1	0,88	0,16
Кластер №4	0,86	1	1	1	0,13	1
Кластер №5	0,96	0,08	0,96	1	0,08	0,92

Выводы