Практическая работа 1

По предмету «Технологии интеллектуального анализа данных мониторинга безопасности»

Выполнил: Воронцов С. А.

Проверил: Латыпова О. В.

ИСПОЛЬЗОВАНИЕ МЕТОДОВ КЛАСТЕРНОГО АНАЛИЗА ДЛЯ ОПТИМИЗАЦИИ КАЧЕСТВЕННОЙ ОЦЕНКИ РИСКОВ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ

Цели и задачи работы

- Описать ситуацию возникновения риска для информации;
- Описать и оценить угрозы и их степень на влияние информационного актива;
- Реализовать один из методов кластерного анализа для оценки рисков информационной безопасности.

Выявление уязвимостей

На некотором здравоохранительном предприятия в результате неправильно проведенных технических и организационных работ по обеспечению информационной безопасности появились следующие уязвимости средств критической информационной инфраструктуры:

- неправильная инсталляция запоминающих сред;
- отсутствие контроля за эффективным изменением конфигурации;
- отсутствие механизмов идентификации и аутентификации, например аутентификации пользователей;
- неконтролируемая загрузка и использование программного обеспечения;
- плохое управление паролями;
- отсутствие резервных копий;
- незащищенные линии связи;
- неадекватное управление сетью.

Выявление угроз

Исходя из выявленных уязвимостей, были определены следующие угрозы:

1. аппаратные отказы;
2. несанкционированное использование носителей данных;
3. программные сбои;
4. использование программного обеспечения несанкционированными пользователями;
5. использование программного обеспечения несанкционированным способом;
6. нелегальное проникновение злоумышленников под видом санкционированных пользователей;
7. ошибка операторов;
8. перегруженный трафик;
9. перехват информации;
10. анализ трафика.

Оценка угроз

Оценка угроз производилась согласно методикам из документа ИСО/МЭК ТО 13335-3-2007 «МЕТОДЫ И СРЕДСТВА ОБЕСПЕЧЕНИЯ БЕЗОПАСНОСТИ. Часть 3 «Методы менеджмента безопасности информационных технологий».

Угрозы оценивались на степень реализации (первая цифра) и степень влияния на информационный актив КИИ предприятия (вторая цифра) по 10 бальной шкале. Номер угрозы совпадает с ее порядковым номером из предыдущего слайда:

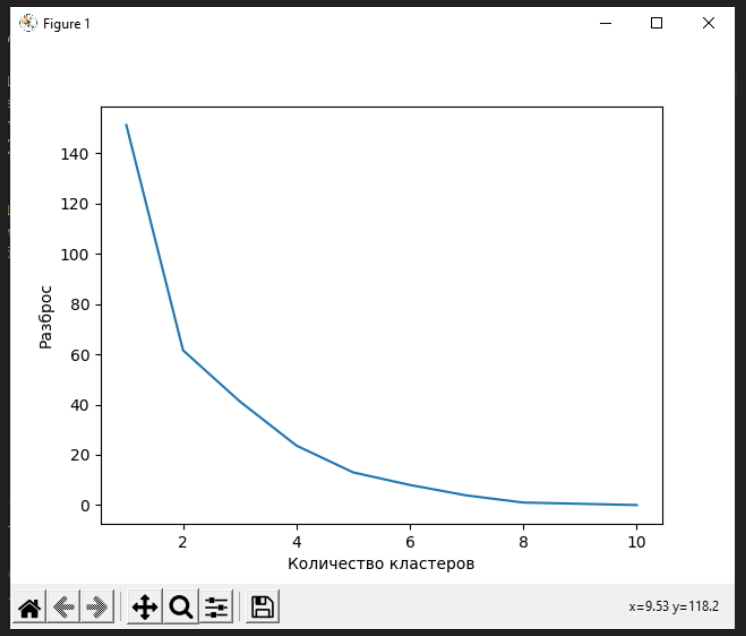
- 1 (5, 8);
- 2 (5, 7);
- 3 (3, 2);
- 4 (4, 10);
- 5 (7, 10);
- 6 (10,10);
- 7 (8, 4);
- 8 (7, 7);
- 9 (6, 10);
- 10 (9,1);

Выбор метода кластерного анализа

В качестве метода кластерного анализа был выбран алгоритм K-средних. Суть алгоритма заключается в разбиение точек на кластеры на основании их близости к центру кластера. Центр кластера каждый раз пересчитывается, чтобы более точнее соответствовать точкам на координатной плоскости. Количество кластеров, как и возможные значения его центров, задаются пользователем.

Реализация метода кластерного анализа

Для наиболее точного определения количества кластеров, был использован «метод локтя». Данный метод заключается в поиске оптимального количества кластеров. Он подразумевает многократное циклическое исполнение алгоритма с увеличением количества выбираемых кластеров, а также последующим откладыванием на графике балла кластеризации, вычисленного как функция от количества кластеров.

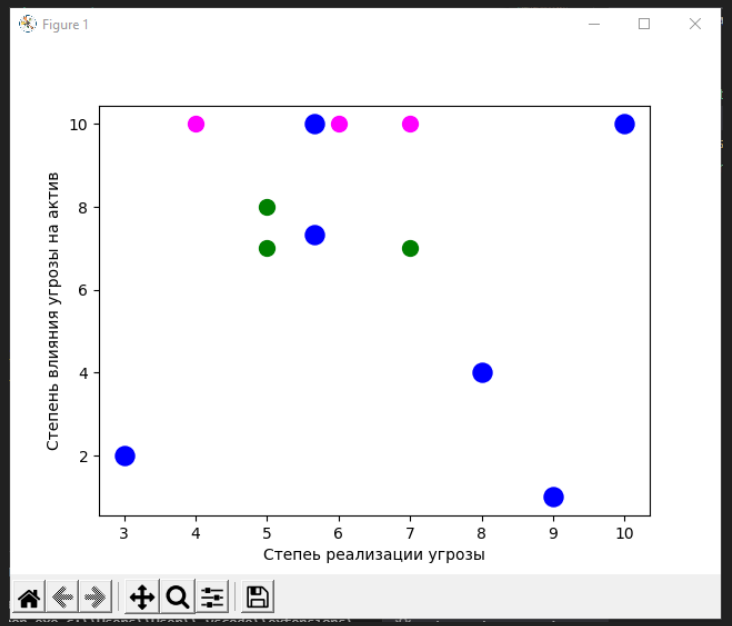


Из графика можно заметить, что оптимальное количеством кластеров будет в районе 6 – 7 штук.

Применение метода кластерного анализа

Результат работы метода кластерного анализа представлен на графике ниже.
Были выделены 6 кластеров:

- К 1 (угроза 3);
- К 2 (угрозы 4, 5, 9);
- К 3 (угрозы 1, 2, 8);
- К 4 (угроза 7);
- К 5 (угроза 10);
- К 6 (угроза 6).



В результате большого разброса точек на координатной плоскости, большинство кластеров оказались одиночными, те состоящими из одной точки.

Выводы

В результате выполнения данной практической работы был изучен и реализован метод кластерного анализа с применением алгоритма K-средних.