

Оптимальный выбор программы криптографической защиты информации методом анализа иерархий с помощью MPriority

Козич Виталий Геннадьевич

*Приамурский государственный университет имени Шолом-Алейхема
Студент*

Баженов Руслан Иванович

*Приамурский государственный университет имени Шолом-Алейхема
к.п.н., доцент, зав. кафедрой информационных систем, математики и
правовой информатики*

Аннотация

В данной статье рассмотрен метод анализа иерархий (МАИ) на примере программного продукта MPriority при выборе оптимальной программы криптографической защиты информации.

Ключевые слова: метод анализа иерархий, МАИ, криптографическая защита, MPriority, информационные технологии.

Optimal choice of the program for cryptographic information protection by the hierarchy analysis method using MPriority

Kozich Vitaliy Gennadievich

*Sholom-Aleichem Priamursky State University
Student*

Bazhenov Ruslan Ivanovich

*Sholom-Aleichem Priamursky State University
Candidate of pedagogical sciences, associate professor, Head of the Department
of Information Systems, Mathematics and legal informatics*

Abstract

This article discusses the analytic hierarchy process (AHP) as an example MPriority software product when choosing the optimal program for cryptographic protection of information.

Keywords: Analytic hierarchy process, AHP, cryptography, MPriority, information technology.

В настоящее время типичный пользователь компьютера сталкивается с проблемой выбора какого-либо программного продукта. В подобных случаях обычно он просит совета другого человека для принятия решения. Но есть более разумный вариант, если конечно же, подходить к данному вопросу с головой. Можно воспользоваться методом анализа иерархий (МАИ).

Это такой математический инструмент системного подхода к решению вопроса о принятии решения. Он не навязывает человеку так называемое «правильное решение», а дает возможность в интерактивном режиме найти такую альтернативу, которая самым лучшим образом соотнесется с его точкой зрения на эту суть проблемы. В 1970 году этот способ поиска решения был придуман Томасом Саати. И на сегодняшний день МАИ хорошо развивается и имеет широкое применения на практике. Его можно использовать не только для сравнения различного рода вещей, но и для поиска решений более глобальных проблем прогнозирования, управления и т.д.

Главным плюсом МАИ является его невероятная универсальность: анализ всевозможных сценариев для разнообразных ситуаций, распределение ресурсов, выбор лучшего сотрудника на предприятии и т.д. Также есть и минус: существует необходимость в получении огромного объема информации от экспертов. Метод лучшего всего подходит для ситуаций, когда большая часть данных соотносится с желаниями лица, принимающего решения (ЛПР) в процессе выбора лучшей альтернативы из многих других.

Для манипуляции методом анализа иерархий был разработан программный продукт под названием MPriority. Использование присутствующего в программе механизма шаблонов (готовых иерархий), позволяет пользователю подстроить метод под область своей деятельности. Целью данной статьи и будет рассмотрение метода в данной программе на примере выбора оптимального программного продукта криптографической защиты информации.

По тематике данной статьи было сделано много исследований. Использование метода анализа иерархий в задачах выбора приоритетов исследовала М.В. Мальцева [1]. М.Г. Илларионов применил метод анализа иерархий в принятии управленческих решений [2]. Метод анализа иерархий в задачах оценки и анализа рисков информационной безопасности рассмотрел И.В. Аникин [3]. Т.А. Соловьева применил программу Mpriority для оптимального выбора системы электронного документооборота [4]. Р.И. Баженов и другие исследовали МАИ на различных примерах [5-7]. Также на данную тему были опубликованы статьи и зарубежными учеными [8-10].

Начнем с того, что более подробно познакомимся с описанием данных продуктов от экспертов для выявления критериев сравнения. В список попали 6 программ криптозащиты: DriveCrypt, Files Cipher, PGP Personal Desktop, DigiSecret, TrueCrypt, BestCrypt. Выбор пал именно на эти продукты из-за их популярности на просторах интернета.

Изучив эти программы на различных форумах можно выделить 3 важнейших критерия: уровень защиты, сложность алгоритмов и производительность. Перечислены они в порядке убывания их важности.

Запустив программу MPriority, начнем с создания проекта. Здесь определяемся с количеством уровней в иерархии и числом элементов (см. рис. 1).

Создание нового проекта

Параметры нового проекта

Цель проекта: ВЫБОР

Число уровней в иерархии: 3

Максимальное число элементов: 6

Комментарии

Да Отменить

Рисунок 1. Окно заполнения параметров нового проекта

Критерий «Уровень защиты» является самым важным, так как он определяет первоначальное значение программного продукта.

Критерий «Сложность алгоритмов» связан со временем выполнения алгоритмов.

Критерий «Производительность» не так важен для пользователей, которые хотят лучше защитить свои данные, но она напрямую зависит от оптимизации. Так как плохо оптимизированная программа может долго рассчитывать даже самый простой алгоритм.

Далее в режиме эксперта сравним важность критериев в интерактивном режиме (см. рис. 2).

Качественная шкала

Сравниваем объект А: ПРОИЗВОД

с объектом В: ЗАЩИТА

Относительно объекта верхнего уровня: ВЫБОР

А по значимости абсолютно превосходит В
<<промежуточное значение>>

А явно важнее В
<<промежуточное значение>>

А значительно важнее В
<<промежуточное значение>>

А незначительно важнее В
<<промежуточное значение>>

А и В одинаково важны
<<промежуточное значение>>

В незначительно важнее А
<<промежуточное значение>>

В значительно важнее А
<<промежуточное значение>>

В явно важнее А
<<промежуточное значение>>

В по значимости абсолютно превосходит А

Да Отмена

Рисунок 2. Шкала сравнения критериев

Программа автоматически формирует таблицу и производит расчеты приоритетности. Получаем цифры, которые соотносятся с описанием важности вышеперечисленных критериев (см. рис. 3).

Работа эксперта

Производим попарные сравнения относительно объекта

ВЫБОР

		1.	2.	3.	Приоритет
1.	ПРОИЗВОД	1	1/9	1/5	0,0581
2.	ЗАЩИТА	9	1	5	0,7351
3.	АЛГОРИТМ	5	1/5	1	0,2066

СЗ: 3,117 Применить

ИС: 0,0585 Закреть

ОС: 0,1009 Отмена

Исследовать

Рисунок 3. Результаты сравнения критериев

Следующим шагом будет попарное сравнение программ криптографической защиты информации относительно каждого из критериев (см. рис. 4-6). Для того чтобы итоговые результаты были адекватны, необходим требуемый уровень согласованности данных. Для оценки согласованности нужна величина отношения согласованности (ОС), которая должна быть как можно ближе к нулю.

Работа эксперта

Производим попарные сравнения относительно объекта

ПРОИЗВОД

		1.	2.	3.	4.	5.	6.	Приоритет
1.	DRIVECRYP	1	1/7	3	1/9	1/9	1/9	0,0306
2.	FILES CIP	7	1	5	3	1/3	3	0,2298
3.	PGP	1/3	1/5	1	1/5	1/9	1/7	0,0258
4.	DIGISECRE	9	1/3	5	1	1/5	1	0,1271
5.	TRUECRYPT	9	3	9	5	1	5	0,4521
6.	BESTCRYPT	9	1/3	7	1	1/5	1	0,1344

СЗ: 6,714 Применить

ИС: 0,1428 Закреть

ОС: 0,1151 Отмена

Исследовать

Рисунок 4. Сравнение программ относительно критерия «Производительность»

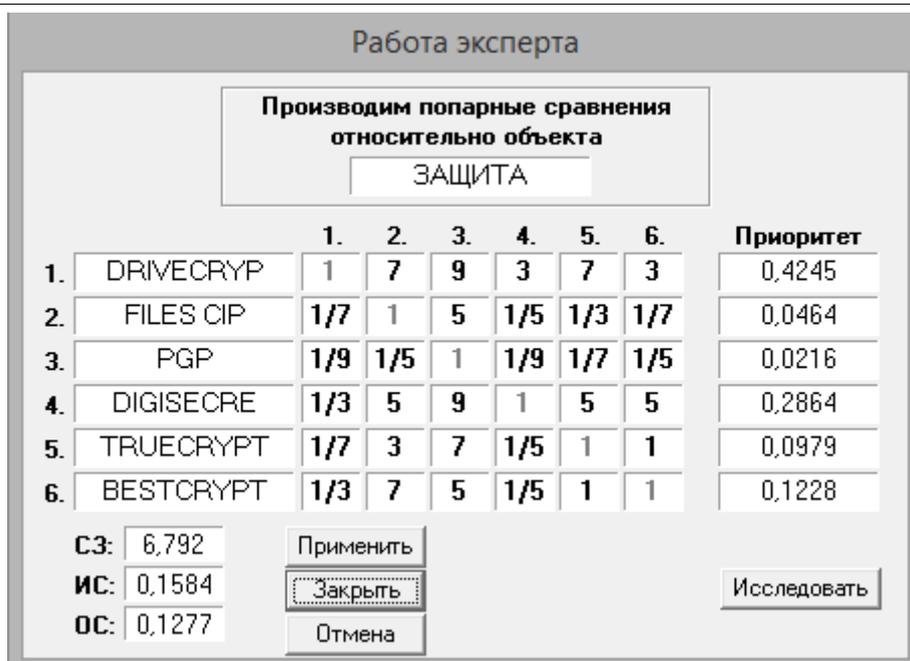


Рисунок 5. Сравнение программ относительно критерия «Уровень защиты».



Рисунок 6. Сравнение программ относительно критерия «Сложность алгоритмов».

В результате исследования получаем диаграмму, на которой видно какая программа лучше всего подходит для пользователя, использовавшего метод анализа иерархий. Ей стал продукт криптозащиты «DriveCrypt» (см. рис. 7).

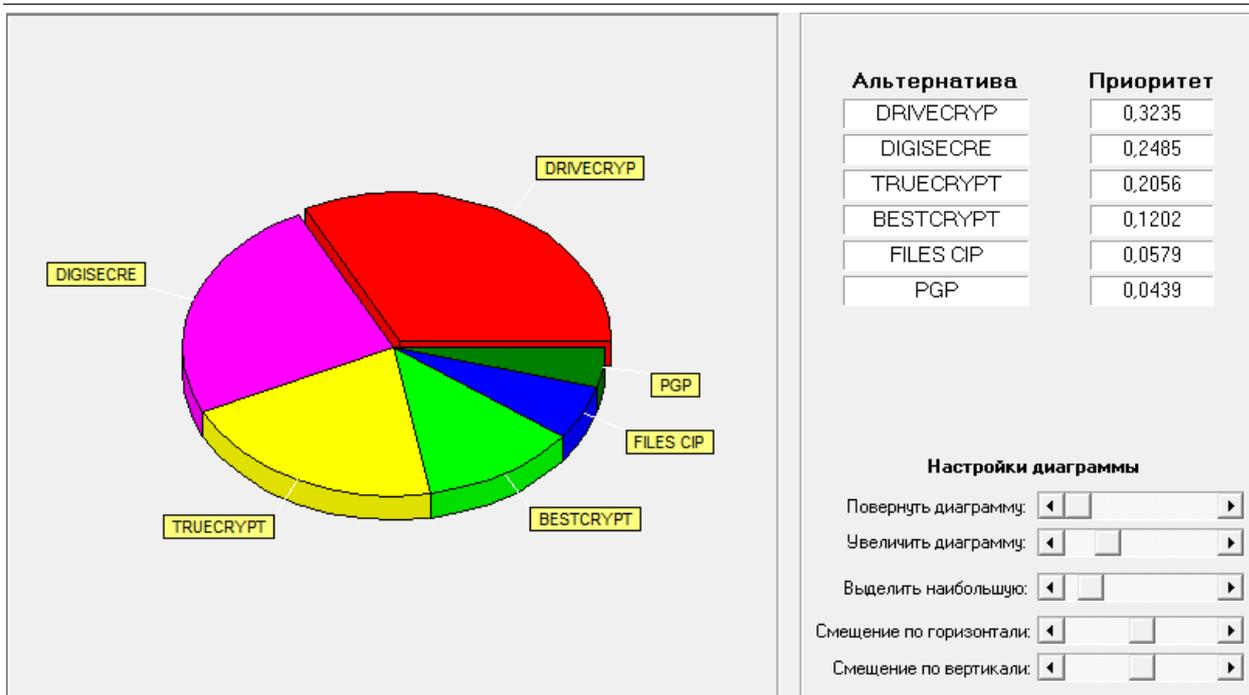


Рисунок 8. Результаты исследования наиболее эффективной программы криптографической защиты информации

Можно сделать вывод, что метод анализа иерархий (МАИ) отлично помогает пользователю найти ответы на слабоструктурированные задачи принятия решений. Данный метод в совокупности с продуктом MPriority может стать незаменимым помощником для тех, кто желает или вынужден по направлению своей деятельности принимать обоснованные рациональные решения. Данная статья будет полезна в изучении дисциплин, связанных с принятием решений и защитой информации.

Библиографический список

1. Мальцева М.В. Использование метода анализа иерархий в задачах выбора приоритетов // Вестник Иркутского государственного технического университета. 2008. №2(34). С. 141-144.
2. Илларионов М.Г. Применение метода анализа иерархий в принятии управленческих решений // Актуальные проблемы экономики и права. 2009. №1. С. 37-42.
3. Аникин И.В. Метод анализа иерархий в задачах оценки и анализа рисков информационной безопасности // Вестник Казанского государственного технического университета им. А.Н. Туполева. 2006. №3. С. 11-18.
4. Соловьева Т.А. Применение программы Mpriority для оптимального выбора системы электронного документооборота // Современная техника и технологии. 2014. №5(33). С. 25.
5. Винокуров А.С., Баженов Р.И. Использование метода анализа иерархий для принятия оптимального решения по выбору цифрового фотоаппарата // Современная техника и технологии. 2014. №9(37). С. 11-17.

6. Шиганова В.В., Баженов Р.И. Выбор сотового телефона для пожилых людей методом анализа иерархии // Современная техника и технологии. 2014. №11(39). С. 45-50.
7. Якимов А.С., Пасюков А.А., Баженов Р.И. Использование программного обеспечения Mpriority для выбора хостинга // Постулат. 2017. №7(21). С. 29.
8. Pamučara D., Stević Ž., Kazimieras E. Zavadskas ntegration of interval rough AHP and interval rough MABAC methods for evaluating university web pages // Applied Soft Computing. 2018. №67. С. 141-163.
9. Promentilla M. A. B., Aviso K. B., Lucas R. I. G., Razon L. F., Tan R. R. Teaching Analytic Hierarchy Process (AHP) in undergraduate chemical engineering courses // Education for Chemical Engineers. 2018. №23. С. 34-41.
10. Bian T., Hu J., Deng Y. Identifying influential nodes in complex networks based on AHP // Physica A: Statistical Mechanics and its Applications. 2017. №479. С. 422-436.