Миронова Наталья Николаевна

Магистрант

Направление: Информатика и вычислительная техника

Магистерская программа: Информационные системы

Многокритериальная задача повышения эффективности комплексной защиты информации корпоративных АИС на примере ФГУП «РФЯЦ ВНИИЭФ»

Аннотация. В статье описан комплексный критерий для аналитической оценки принимаемых решений, рассмотрен метод решения задач многокритериальной оптимизации на примере поиска Парето-оптимальных альтернатив, определен критерий эффективности технических решений, который использован при постановки многокритериальной задачи повышения эффективности комплексной защиты информации корпоративных автоматизированных информационных систем на примере ФГУП «РФЯЦ ВНИИЭФ».

Ключевые слова: многокритериальная задача, корпоративная сеть, защита информации, система, конфиденциальность, угроза.

На сегодняшний день информатизация и автоматизация вошли практически во все сферы нашей жизни. С каждым днем появляются все больше и больше новых технологий, которые облегчают жизнь, как определенного человека, так и крупных трансатлантических компаний. Вместе с тем, использование инновационных технологий породило ряд злоумышленников, которые пытаются воспользоваться неосведомленностью, непониманием и некомпетентностью сотрудников или пользователей различных информационных и автоматизированных систем, что и обуславливает актуальность выбора темы магистерской диссертации.

Появление новых информационных технологий и развитие мощных компьютерных систем хранения и обработки информации повысили требования к уровню защиты информации и определили необходимость разработки эффективных

механизмов защиты информации, адаптированной под современные архитектуры хранения данных

Несмотря на предпринимаемые попытки защиты корпоративных информационных систем от воздействий не имеют тенденций к снижению. Постоянное расширение функциональности информационных систем и нарастание зависимости от информационной инфраструктуры создаёт ситуацию, когда атаки на эту инфраструктуру могут приводить к последствиям, сравнимым с последствиями террористической активности.

В целом анализ текущего состояния защиты КИС от этих угроз показывает, что возможности существующих систем и методов защиты во многом не удовлетворяют требованиям практики. Одним из существенных их недостатков выступает невысокая адаптивность к изменяющимся условиям и видам угроз.

Научная значимость моей магистерской диссертации состоит в оптимизации и упорядочивании существующей научно-методологической базы по комплексному обеспечению информационной безопасности корпоративной АИС. В работе применен комплексный критерий для аналитической оценки принимаемых решений. Выбор и обоснование критерия эффективности технических решений использован при постановки многокритериальной задачи повышения эффективности комплексной защиты информации корпоративных автоматизированных информационных систем на примере ФГУП «РФЯЦ ВНИИЭФ».

Задачи принятия и нахождения эффективного решения при проектировании сложных технических систем, как правило, являются комплексными и описываются множеством критериев.

Критерий оптимальности - характерный показатель решения задачи, по значению которого оценивается оптимальность найденного решения, то есть максимальное удовлетворение поставленным требованиям. Совокупность радиоэлектронных средств, видеокамер, объединенных с помощью аппаратно-программного комплекса в единое целое составляет информационной защиты, который, в свою очередь, характеризуется многообразием вариантов исполнения и размещения. Задача оптимизации построения элементов информационной защиты,

его объектов сводится к обеспечению соответствующего уровня реализации их функций, что гарантирует, в свою очередь, выполнение системой надлежащих охранных требований [1, 2].

На практике подобные задачи возникают в те моменты, когда проектируемый объект либо не может быть описан однокритериальной зависимостью, либо объединить отдельные критерии в единый не представляется возможным. Именно такая ситуация, например, возникает при постановке задач оптимизации построения элементов систем охраны объектов и защиты информации в ФГУП «РФЯЦ ВНИИЭФ.

В случае необходимости оптимизации одного из показателей качества проектируемого объекта защиты с условием соблюдения ограничительных требований к остальным показателям формируется один частный критерий. Задача оптимизации при этом сводится к максимизации (минимизации) данного критерия с учетом заданных ограничений. Рассмотрим метод решения задач многокритериальной оптимизации на примере поиска Парето-оптимальных альтернатив [3].

Пусть имеется множество вариантов решения. По каждому из вариантов определены значения всех критериев. Представим множество оценок вариантов решения в пространстве критериев (рисунок 1).

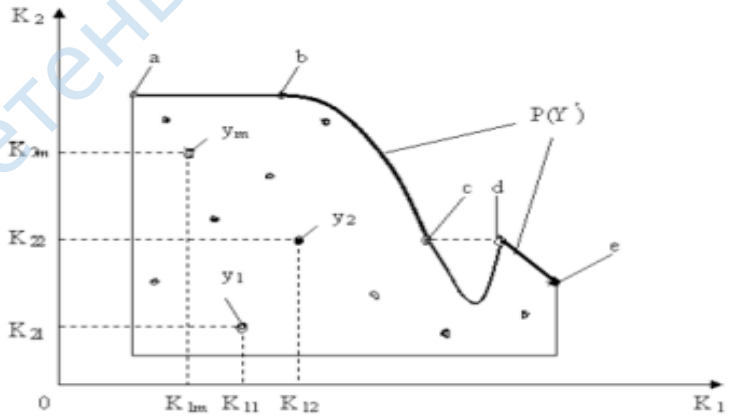

Рисунок 1. Иллюстрация поиска Парето-эффективных решений

Где: К1, К2 - критерии оценки вариантов решения; Y = {y1 , y2 , …, ym} - множество оценок альтернативных вариантов решения; К11, К12, … , К1m - значения первого критерия для 1, 2, … , m-го варианта решения; К21, К22, … , К2m - значения

второго критерия для 1, 2, … , m-го варианта решения; P(Y) - множество Парето-эффективных оценок решений

Множество Парето-эффективных оценок P(Y) представляет собой «северо-восточную» границу множества Y без тех его частей, которые параллельны одной из координатных осей или лежат в «глубоких» провалах.

Для случая, изображенного на рисунке 1, Парето-эффективные оценки состоят из точек кривой (bc), исключая точку (c), и линии (de). Рассмотренный метод обладает рядом преимуществ, а именно:

1) метод математически объективен;

2) критерии равнозначны.

Из недостатков метода можно выделить следующие:

1) одно окончательное решение получается только в частном случае, т.е. количество Парето-эффективных решений, как правило, более одного;

2) метод эффективен для ограниченного количества решений, т.к. его программная реализация для большого количества решений очень сложна, а графическое решение типа, представленного на рисунке 1 является проблематичным, а зачастую и невозможным.

Опыт решения задач оптимизации при построении систем защиты информации и объектов показывает, что необходимо одновременное рассмотрение данной проблематики сразу по нескольким функциям (критериям) [3].

Краеугольным понятием в данном вопросе является Парето-оптимальная альтернатива, являющаяся решением многокритериальной задачи. Рассмотрим суть данного метода, используя те критерии, которые для защиты информации и охраны объектов исследуемой организации в настоящее время являются наиболее актуальными. Выделить из них наиболее значимые, значит вплотную приблизиться к поиску эффективного решения. Очевидно, что наиболее значимым из совокупности критериев должен быть некоторый показатель, характеризующий эффективность системы защиты и охраны с точки зрения реализации ею конкретных функций в необходимом объеме и с заданной степенью качества.

Данный показатель должен предоставлять возможность не только количественной, но и качественной оценки функциональных возможностей системы защиты и проводить сравнение различных систем охраны в соответствии с заданными эксплуатационными требованиями. Таким критерием для объектов охраны является критерий комплексной эффективности (ККЭ). Целью данного критерия является объективная оценка эффективности организации защиты и охраны.

В общем случае, сформулированную выше задачу по оптимизации построения оптимальных моделей объектов охраны возможно решить с учетом лишь ККЭ, однако задача окажется решенной некорректно, т.к. вполне вероятно, что некоторые эффективные решения «выпадут» из рассмотрения. Поэтому в процесс решения рассматриваемой задачи целесообразно добавить еще один немаловажный критерий, а именно, экономическую стоимость варианта разрабатываемой системы охраны. Критерии при использовании данного метода будут являться равнозначными.

Рассмотрим пример, в котором оптимизируется некий гипотетический объект охраны по двум критериям - ККЭ и стоимости. Таким образом, поставленная задача, согласно теории оптимизации, является комбинаторной, относительно двух критериев: значения ККЭ и экономической стоимости.

Сложность нахождения решения заключается в отсутствии явного вида целевой функции. Это связано непосредственно с самой структурой системы охраны, которая чрезвычайно сложна, вследствие наличия большого количества неявных связей между ее элементами, а также особенностями конструктивного исполнения и логического аппарата. Главным аспектом в рассматриваемом вопросе становится проблема поиска оптимального варианта размещения элементов комплекса информационной защиты на рубежах охраны и режимных территориях. Процесс нахождения оптимального решения заключается в поиске решения с максимальным значением ККЭ и минимальной стоимостью его практической реализации.

Графически, согласно методу Парето, каждое решение представляет точку, описываемую двумя координатами, в роли которых выступают определенные вначале критерии. Предположим, что значения критериев оценки градуируются по 10

бальной шкале (с учетом того, что реальные значения ККЭ лежат в пределах от 0 до 1, а стоимости - есть произвольные положительные числа).

Будем считать, что введенная балльная система в состоянии объективно оценить реальный объект защиты. Заметим, что оценка стоимости производится с точки зрения дешевизны практической реализации рассматриваемого варианта объекта защиты и охраны, т.е. чем выше оценка, тем меньше стоимость. Процесс нахождения оптимального варианта модели объекта охраны заключается в поиске решения с максимальным значением ККЭ и минимальной стоимостью.

Графически, согласно метода Парето, каждое решение представляет точку, описываемую двумя координатами, в роли которых выступают определенные вначале критерии. На основе рассмотренных выше требований к критериям оценки организации охраны, разработаем таблицу значений и представим множество оценок вариантов решения в пространстве критериев. При оценке результатов, полученных путем построения графической зависимости значений ККЭ от стоимости, сделаем соответствующие выводы. Результаты оценки вариантов приведены в таблице 1.

Таблица 1 - Оценки вариантов размещения элементов комплекса информационной защиты по критериям комплексной эффективности и стоимости

Критерии	Оценки вариантов (баллы)									
	С1	С2	С3	С4	С5	С6	С7	С8	С9	С10
ККЭ	6	4	10	3	10	0	2	4	6	7
Стоимость	6	2	1	7	4	4	10	4	8	2

Представим множество оценок вариантов в пространстве критериев (рисунок 2).

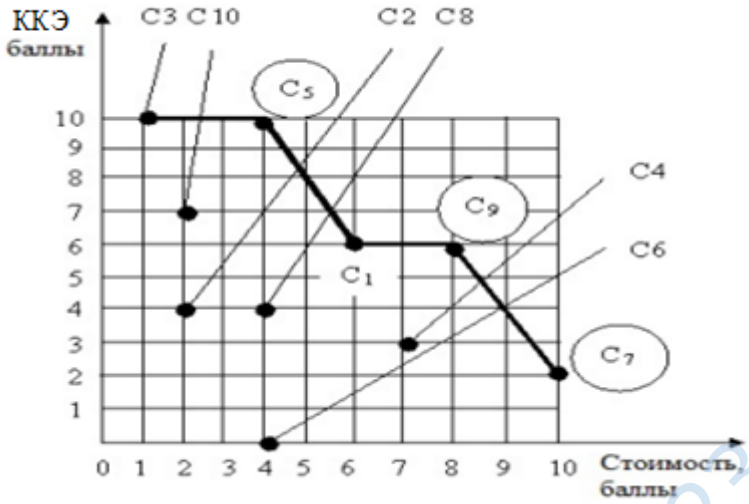

Рисунок 2. Пример поиска Парето-эффективных решений

Парето-эффективными решениями здесь являются варианты С5, С7 и С9. Необходимо учесть, что на окончательное решение задачи оптимизации даже после завершения процесса поиска оптимальных альтернатив может оказывать влияние некоторое количество дополнительных факторов. К примеру, обратим внимание на вариант С7. По стоимостным критериям он наиболее выгоден, но в процессе анализа становится очевидной его несостоятельность, так как значение ККЭ недопустимо мало, что не позволяет в конечном итоге говорить о рассматриваемой модели, как о полноценно функционирующей технической системе, обеспечивающей заданный уровень охраны и защиты информационной безопасности.

Литература

1. Зацаринный А.А., Ионенков Ю.С. Оценка эффективности информационно-телекоммуникационных систем / Под ред. д.т.н. А.А. Зацаринного. – М.: НИПКЦ Восход-А, 2020. – 120 с.

2. Ионенков Ю.С. Научно-практические аспекты оценки эффективности информационно-телекоммуникационных систем // Радиолокация, навигация, связь: Сборник трудов XXIV Международной научно-технической конференции (17-19 апреля 2018 г.). Том 1. – Воронеж: ООО «Вэлберн», 2018, - с. 140-149.

3. Ногин В.Д. Принятие решений в многокритериальной среде: количественный подход / В.Д. Ногин. М.: ФИЗМАТЛИТ. - 2022. - 176 с.