Мистров Л.Е., Кравцов Е.В.

Методика обеспечения и управления информационной безопасностью критически важных объектов

Аннотация: Предложена методика обоснования способов применения комплексов мониторинга и управления информационной безопасностью критически важных объектов на основе оптимального распределения ресурса средств контроля эффективности защиты информации и элементов управления организационно-технической системы критически важных объектов.

Ключевые слова: контроль эффективности защиты информации, информационная безопасность критически важных объектов, оптимальное распределение ресурса средств контроля и управления информационной безопасностью

Для реализации функционирования критически важных объектов (КВО) необходимо применение организационно-технических систем (ОТС) мониторинга и управления информационной безопасностью (ИБ) защищаемых ресурсов данных объектов. Такие ОТС представляют собой совокупность организационно объединенных единством цели подсистем (органов) управления, контроля эффективности защиты информации и исполнения. Основу исполнительной подсистемы ОТС составляют средства комплексного мониторинга и обеспечения ИБ КВО.

Комплексы мониторинга и управления информационной безопасностью (КМУИБ) являются неотъемлемой частью КВО и используются по плану ОТС применительно к исходным данным уровня типовых ситуаций. Обоснование способов применения КМУИБ осуществляется по критерию разумной достаточности на основе рассмотрения во взаимообусловленной связи таких факторов, как важность защищаемых ресурсов, наличие информативных каналов утечки информации, возможности злоумышленника по восстановлению сведений о КВО и ресурсы на преодоление систем обеспечения ИБ. Применение КМУИБ всегда связано с временными и материальными затратами. Практически всегда выделяемые для этих целей ресурсы ограничены, поэтому

чрезвычайно важно определить достаточный уровень обеспечения ИБ, позволяющий обеспечить эффективное функционирование КВО с минимально возможными затратами.

Эффект от применения КМУИБ состоит в уменьшении времени в подготовке и принятии решений в различных контурах подсистем (органах) управления, добывания информации и исполнения мероприятий обеспечения ИБ на основе снижения информированности противостоящей стороны о защищаемых ресурсах КВО и в повышении эффективности применения ОТС за счет оптимального распределения ресурса средств контроля эффективности защиты информации и элементов управления ОТС КВО.

Вследствие динамического, нелинейного, стохастического и конечного характера конфликта ОТС и условий использования различного типа и количества КМУИБ с учетом расходования своего внутреннего ресурса по этапам конфликта, задача оптимизации способов применения ОТС для обеспечения заданной эффективности функционирования КВО представляет оптимизационную нелинейную задачу с экстремальными переменными и ограничениями.

Исходя из этого, задача разработки методики обоснования способов оптимального применения и распределения ресурса средств контроля эффективности защиты информации и элементов управления ОТС КВО для реализации заданной эффективности применения ОТС в конфликте является актуальной, а её решение имеет важное прикладное значение.

Цель статьи состоит в разработке методики решения оптимизационной задачи планирования применения разнотипных КМУИБ при обеспечении эффективных действий ОТС ИБ. Результаты решения данной задачи используются в качестве исходных данных для оценки эффективности применения КВО при обеспечении защиты информационных ресурсов на различных уровнях иерархии их целевой функциональной системы.

Для этапа планирования применения КМУИБ и организации ОТС характерны две группы типовых задач. Первая группа связана с распределением выделенного ресурса (заданного типа и количества) разнотипных КМУИБ и входящих в их состав различных типов средств исполнения по объектам защиты КВО при

различных способах контроля эффективности защиты информации (объектовый, зональный, комбинированный). Вторая группа задач определяет оптимальное распределение внутреннего ресурса КМИУБ (при заданной максимальной эффективности способа контроля эффективности защиты информации) по объектам воздействия в определенных участках диапазона условий применения систем нарушения информационной безопасности и по рубежам применения средств противостоящей стороны.

В соответствии с этим рассматриваются постановки частных задач планирования и организации применения КМУИБ и приводятся основные положения методов их решения.

Задача обеспечения и управления ИБ КВО, обеспечивающая поддержку принятия решений в органах управления ОТС.

Процесс управления ИБ КВО можно представить в виде модели стратегического управления, ориентированной на прогнозирование поведения ОТС на каждом выделенном интервале времени (с учетом результатов моделирования процессов противостоящей стороны) и на этой основе осуществить выбор стратегии организации и ведения контроля эффективности защиты информации КВО.

На начальном этапе решения задачи формируется экспертная матрица взаимосвязи между показателями системы управления ИБ КВО на основе правил когнитивного (концептуального) моделирования. На основе матрицы взаимосвязей при установленных начальных условиях моделируется поведение системы управления ОТС при данном «макрорешении» на *i*-м интервале и определяется ее финальное состояние (в конечной точке интервала). Для выбранного «макрорешения» формируется графоаналитическая модель сценария его выполнения, проводится компьютерное моделирование выполнения выбранного «макрорешения» и находится фактическое состояние результатов контроля эффективности защиты информации в конечной точке *i*-го интервала.

Модель обеспечения и управления ИБ КВО представляется в виде сети из взаимосвязанных элементов ОТС: органы управления, координирующие работу системы обеспечения ИБ КВО, и КМУИБ, принимающие решения по защите информационных ресурсов (см. рис. 1).

Методика (реализующие алгоритмы) рационального распределения разнородного ресурса комплексов и средств контроля эффективности защиты информации по защищаемым ресурсам КВО. Методика (в виде системы взаимосвязанных частных методик) предназначена для обоснования перечня объектов защиты (ОЗ), подлежащих контролю в первую очередь в условиях ограниченного ресурса сил, средств и времени, при планировании мероприятий по обеспечения ИБ КВО. Ее реализация базируется на алгоритме определения перечня и состава ОЗ, в основу которого положен графоаналитический метод. Предполагается, что имеются данные о местоположении ОЗ, составе их демаскирующих признаков и каналах утечки защищаемых информационных ресурсов.

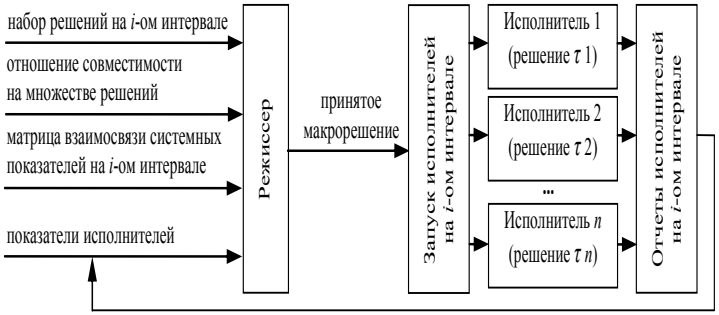

Рис. 1 – Обобщенная схема модели обработки информации и принятия решений в ОТС системы обеспечения ИБ КВО

Существо алгоритма состоит в следующем.

1. По графику потребностей в контроле эффективности защиты информации составляются перечни объектов, директивные сроки контроля которых перекрываются. В соответствии с возможностями и составом каждого КМУИБ определяются границы зон контроля по всем объектам защиты КВО.

2. Для каждого объекта выбирается то средство контроля эффективности защиты информации, у которого радиус зоны контроля максимален. На карту с расположением объектов наносятся окружности с радиусами минимальных зон контроля. На пересечении этих зон выбираются места возможного развертывания

средств контроля, при этом в первую очередь рассматриваются те позиции, откуда возможен контроль демаскирующих признаков и защищаемых ресурсов наиболее важных элементов КВО и одновременно обеспечивается охват большого количества ОЗ.

3. Важность определяется по индексу приоритета. Наиболее важные объекты имеют индекс приоритета, равный 1. Объекты с одинаковым приоритетом, если нет дополнительных условий, ранжируются по удаленности от позиционного района группы контроля.

4. Распределение средств контроля эффективности защиты информации по объектам защиты начинается с объекта, имеющего максимальный приоритет. Если в пределах зоны контроля вблизи этого объекта находятся другие объекты, подлежащие контролю, то выбирается позиция, обеспечивающая охват максимального количества объектов. Для проведения наиболее точных расчетов может быть использован алгоритм определения план-графика применения сил и средств контроля эффективности защиты информации.

Алгоритм распределения разнородного ресурса средств контроля эффективности защиты информации по объектам защиты. Распределение ресурса средств контроля и защиты информации *при реализации оперативных действий* по обеспечению информационной безопасности базируется на применении основных положений метода «двух функций» с измененным порядком ранжирования ОЗ КВО.

Распределение ресурса средств КМУИБ *при реализации долгосрочных действий* по управлению ИБ КВО базируется на реализации принципа оптимальности Беллмана и применения аппарата динамического программирования. Общая эффективность за операцию пропорционально количеству комплексов и средств контроля эффективности защиты информации, привлекаемых для решения задач ИБ КВО на каждом рассматриваемом этапе операции.

Алгоритм определения план-графика применения сил и средств контроля эффективности защиты информации предназначен для выбора средств КМУИБ с учетом требований по полноте, достоверности и оперативности контроля эффективности защиты информации ограниченным ресурсом средств контроля и

определения на этой основе наилучшего план-графика, обеспечивающего наибольшее значение показателя «степени охвата» ОЗ.

В качестве оптимизируемого показателя используется относительная суммарная «степень охвата» ОЗ и их контролируемых характеристик, взвешенная по их относительной важности и информативности их защищаемых ресурсов в основных физических полях.

В основу *алгоритма определения требуемой частоты и продолжительности контроля эффективности защиты информации* положен метод теории выборочного контроля, суть которого состоит в следующем. Средствами обеспечения ИБ контролируются не все сеансы излучений ОЗ, а лишь часть из них. При этом часть нарушений требований по ИБ может быть пропущена с определенной вероятностью. Необходимо оценить, какое количество сеансов излучений следует проконтролировать, чтобы с заданной вероятностью не пропустить определенное количество нарушений в не проконтролированных сеансах излучений.

Таким образом, использование предложенной методики обоснования способов применения КМУИБ КВО позволяет определить не только оптимальные планы распределения заданного количества средств КМУИБ различного типа при защите разнотипных ОЗ, но и сформировать предложения по оптимальным вариантам их размещения и способам применения.