Процедура формирования относительно полного множества задач защиты информации

Корчев А. В.

Корчев Алексей Владимирович / Korchev Aleksej Vladimirovich - магистрант,
кафедра информационной безопасности,
институт информационных технологий и коммуникаций,
Астраханский государственный технический университет, г. Астрахань

Аннотация: *в статье рассматривается применение системного анализа для формирования перечня задач, возникающих в процессе функционирования систем информационной безопасности. Предложена процедура формирования относительно полного множества задач защиты информации.*
Ключевые слова: *защита информации, системный анализ, обеспечение информационной безопасности.*

Введение

Одним из основных принципов построения и совершенствования систем обеспечения информационной безопасности (СОИБ) является принцип комплексности, который опирается на системно-концептуальный подход к решению всех проблем и задач, возникающих в процессе функционирования системы. Здесь концептуальность подхода означает, что система защиты информации должна строиться на основе единой для всей системы концепции, в которой представлены все объекты и явления, способные оказать значимое влияние на процесс функционирования СОИБ, а также связи между ними. Системность подхода означает, что все средства и возможности, имеющиеся в системе по обеспечению информационной безопасности, должны быть включены в единую технологию, которая обеспечивает выбор наиболее эффективных средств и способов противодействия угрозам и атакам на информационные активы объекта защиты и СОИБ. Последнее требование влечет необходимость формирования относительно полного состава задач, которые могут возникнуть в процессе функционирования СОИБ. Здесь слово «относительный» означает, что представленная совокупность задач содержит все значимые на текущий момент задачи, но при изменении условий функционирования объекта защиты или СОИБ состав решаемых задач может быть изменен с учетом изменившихся условий функционирования СОИБ. Таким образом, одним из важных условий реализации принципа комплексности построения СОИБ, логически вытекающем из самой сути этого принципа, является необходимость формирования относительно полного множества задач защиты информации для данного конкретного объекта в конкретных условиях его функционирования. Именно этой задаче и посвящена данная работа. В работе ставится еще более важная проблема – проблема формирования состава задач в их оптимизационной постановке, нацеленной на обеспечение максимально возможной эффективности решения этих задач.

Таком образом, цель данной работы заключается в описании процедуры формирования относительно полного множества оптимизационных задач (ОЗ) обеспечения информационной безопасности. Проблема оптимизации в системах защиты информации (СЗИ) поставлена в [1], методология решения проблемы оптимизации рассмотрена в [2].

Описываемая ниже процедура позволяет при необходимости получить на каждый момент времени множество классов ОЗ, которое на текущий момент времени может рассматриваться как достаточно полное для целей его использования – это множество выше названо относительно полным. Получаемое множество ОЗ содержит все элементы, реально значимые на текущий момент в контексте рассматриваемой проблемы. Но это множество при существенных изменениях условий функционирования системы обработки данных (СОД) или СОИБ может пополниться новыми элементами, и из нее могут быть удалены уже неактуальные элементы.

Класс ОЗ будет представлен ОЗ с наиболее общей постановкой, то есть отбрасывание любой характеристики или связи, входящей в постановку этой задачи, приведет к тому, что либо эта задача как задача оптимизации станет тривиальной, либо она потеряет содержательный смысл. Другие задачи, входящие в класс, получаются из задачи с наиболее общей постановкой либо путем наложения дополнительных ограничений на параметры и характеристики задачи, либо путем введения новых предположений о свойствах и взаимосвязях характеристик. Отметим, что в результате введения дополнительных предположений может измениться форма оптимизируемого функционала и, следовательно, постановка ОЗ. Дополнительные ограничения на параметры и характеристики, вообще говоря, сужают область поиска. В результате получающаяся задача часто требует для своего решения методов решения, отличных от тех, которые могут быть использованы для решения первоначальной задачи. Однако решения первоначальной задачи могут служить отправной точкой для поиска решений в задачах с более специальной, частной постановкой.

Процесс формирования относительно полного множества задач опирается на системный подход. Близкий результат приведен в [1].

Описание процедуры формирования

При формировании относительно полного множества ОЗ функционирования СОИБ будем исходить из результатов анализа функциональных процессов защиты информации (ЗИ) в СОД [3], в результате которого

выделены следующие функции защиты информации (см. также [2]).

1. Предупреждение условий, порождающих дестабилизирующее воздействие (ДВ) (**ПУ**).
2. Предупреждение проявления ДВ в процессе функционирования АСОД **(ПП).**
3. Обнаружения проявившихся ДВ **(ОП).**
4. Предупреждение воздействия ДВ на информацию (**ПВ**).
5. Обнаружения воздействия ДВ на информацию (**ОВ**).
6. Локализация воздействия ДВ на информацию (**ЛВ**).
7. Ликвидация последствий воздействия ДФ **(ЛП).**
8. Планирование **(Пл).**
9. Оперативно-диспетчерское руководство в процессе выполнения планов (**ОДУ**).
10. Календарно-плановое руководство выполнением планов **(КПР).**
11. Обеспечение повседневной деятельности системы управления **(ОПД).**

Процесс формирования классов задач состоит из следующих этапов.

Первый этап: формирование полного множества функций управления ЗИ.

Второй этап: для каждой из этих функций формируются совокупности соответствующих макрозадач ЗИ, где под макрозадачей понимается описание конкретной проблемы, требующей решения в наиболее общей ее постановке – с учетом только наиболее важных особенностей объекта защиты и условий его функционирования.

Третий этап: для каждой макрозадачи путем ее уточнения по отдельным характеристикам и атрибутам СОИБ формируется множество классов ОЗ ЗИ, в каждой из которых учитываются определенные более конкретные аспекты функционирования объекта защиты и СОИБ. Таким образом, процесс формирования множества классов ОЗ ЗИ заключается в последовательном поэтапном формировании уровней описаний, на каждом из которых раскрываются и уточняются постановки проблем предыдущего уровня по различным особенностям функционирования системы до тех пор, пока на некотором уровне не будет сформировано множество классов ОЗ ЗИ, имеющих конкретное постановочное содержание, которое пригодно для выбора конкретных методов и процедур ее решения.

Для формирования отдельных уровней необходимо на каждом уровне описать те признаки и характеристики, по которым будет производиться разбиение и детализация элементов предыдущего уровня в зависимости от содержания этих признаков и значений характеристик. При этом основным базовым принципом подобного разбиения является следующий: выделенные классы подпроцессов должны обеспечивать наиболее эффективную реализацию средств и мероприятий противодействия угрозам. Одним из наиболее важных подходов к повышению эффективности любой системы является максимальное использование методов узкой специализации специалистов и подразделений в процессе обеспечения ЗИ. Применительно к рассматриваемой задаче разбиения на подпроцессы это условие означает, что основным принципом разбиения должно быть обеспечение наибольшей однородности и однотипности всех подпроцессов, входящих в один и тот же класс. Таким образом, применительно к процессу обеспечения ЗИ признаками для разбиения выделенных подпроцессов ЗИ на отдельных уровнях являются, прежде всего, однотипность подпроцессов по их месту в общем процессе обеспечения ЗИ и однородность используемых при их реализации действий, способов и мероприятий, поскольку, чем однотипнее подпроцессы, связанные с обеспечением ЗИ, тем однотипнее методы и средства, используемые при их реализации.

Критерием разбиения каждой функции управления ЗИ на макрозадачи является требование однородности в рамках одной задачи мероприятий и действий, проводимых с целью обнаружения или противодействия ДВ в соответствующих ситуациях. Основными мероприятиями, проводимыми при реализации функций обнаружения, является регистрация (фиксация) данных, контроль состояний всех компонентов СОИБ во всех режимах их работы и сигнализация о состоянии контролируемых объектов и процессов. Множество всех мероприятий по противодействию ДВ допустимо разделить на следующие два семейства:

- мероприятия, осуществляемые как ответная реакция на ДВ, т. е. апостериорно;
- мероприятия, осуществляемые превентивно с целью создания неблагоприятных условий для возникновения и развития ДВ, т. е. априорно.

В соответствии с различными рубежами противодействия множество всех вынужденных мероприятий можно разбить на следующие группы.

1. Ликвидация источника ДВ.
2. Изменение интенсивности и мощности ДВ, других его характеристик.
3. Локализация источника ДВ.
4. Направление ДВ в других направлениях, по другим путям.
5. Изолирование компонентов АСОД с целью защиты от ДВ.
6. Изолирование подвергшихся ДВ компонентов СОД.
7. Ликвидация подвергшихся ДВ элементов системы с их воссозданием заново или передачей их функций другим компонентам.

Возможные действия при проведении превентивных мероприятий:

- уничтожение ненужных элементов;
- изолирование отдельных частей и компонентов СОД друг от друга или от общей технологии;

- изменение состояний компонентов;
- дублирование и резервирование элементов;
- защитные преобразования в компоненте;
- адаптивные изменения в технологии и в структуре СОД;
- использование средства обеспечения защиты информации (СОЗИ).

В результате описанного анализа в [3] выделяется 98 макрозадач ЗИ.

Для формирования множества классов ОЗ ЗИ содержание полученных макрозадач уточняется по следующим признакам.

1. Компоненты системы (внешние факторы, аппаратно-программные средства, персонал и др.).
2. Территориально-временные характеристики и особенности рассматриваемого компонента (этапы жизненного цикла, статические и динамические характеристики и др.).
3. Средства и ресурсы, имеющиеся в АСОД и в СЗИ.
4. Условия функционирования компонента (характер ДВ, уровень нагрузки и др.).
5. Технология функционирования (возможные способы действий и мероприятий, процедура обработки информации).

Для примера рассмотрим функцию ПВ. Одной из макрозадач этой функции является локализация и нейтрализация источника ДВ. Пусть ДВ есть «проникновение злоумышленника». При проецировании на элемент «программные средства» первого атрибута «компоненты» приходим к необходимости рассмотрения задач недопущения проникновения злоумышленника к защищаемой информации, его выявления и нейтрализации. Дополнительное проецирование по элементу «этапы жизненного цикла» из второго атрибута позволяет получить более содержательные постановки указанных задач. В частности, получаем задачи обеспечения недопущения возможностей проникновения злоумышленника в систему на стадии разработки программных средств, его выявление и нейтрализация в процессе апробации и использования программного продукта. Для получения постановок задач, содержательно отличающихся на всех трех этапах жизненного цикла, необходимо добавить хотя бы еще по одному атрибуту. Так, если в качестве третьего атрибута добавить атрибут «средства» (например, финансовые ресурсы), то приходим, в частности, к следующим классам ОЗ.

ПВ 1.1. Распределение работ на разработку программных средств.

ПВ 1.2. Выбор тестовых задач.

ПВ 1.3. Выбор способа действий при проникновении злоумышленника.

Множество ОЗ, которые могут быть сформированы на основе рассматриваемой макрозадачи при проецировании по атрибутам «программные средства, этапы жизненного цикла», значительно шире приведенных трех задач. В частности, выше не проанализированы задачи выявления и нейтрализации каналов проникновения злоумышленника на этапе разработки программных средств, недопущения возникновения новых каналов на этапе апробации и эксплуатации.

Аналогично можно рассмотреть процесс формирования классов ОЗ той же макрозадачи при ее проецировании по атрибутам «аппаратные средства», «этапы жизненного цикла». При этом на этапе проектирования системы приходим, в частности, к задаче выбора состава аппаратных средств обеспечения ЗИ, минимизирующим суммарные издержки в СОИБ, связанные с приобретением и эксплуатацией аппаратных средств и потенциальными потерями от проникновения злоумышленника к защищаемой информации. На этом же этапе целесообразно рассмотреть задачи разработки процедур переключения и исключения подвергшихся ДВ аппаратных средств из процесса обработки информации (в частности, состав этих аппаратных средств и моменты переключения и отключения могут быть параметрами оптимизации). На этапе внедрения приходим, в частности, к задачам определения оптимальной степени (глубины) апробации аппаратных средств, проверки (с расходом минимальных ресурсов на эти цели) способности аппаратуры правильно функционировать в различных реально возможных условиях проявления ДВ. На этапе эксплуатации представляют интерес, в частности, задачи определения оптимальной периодичности диагностирования аппаратных средств и выбора оптимальных режимов их эксплуатации.

Проецирование той же макрозадачи по атрибутам «внешние факторы», «этапы жизненного цикла» приводит, в частности, к рассмотрению задачи ликвидации и локализации источника ДВ с минимальными суммарными издержками, причем оптимальная последовательность действий разрабатывается на этапе проектирования системы или ее совершенствования (до возникновения ДВ рассматриваемого типа) и уточняется в процессе возникновения и проявления ДВ. Схожие задачи возникают и при проецировании по атрибутам «субъекты», «этапы жизненного цикла».

Аналогично формируется множество классов ОЗ для других функций ЗИ. На основе сформированного относительно полного множества ОЗ ЗИ и совокупности соответствующих моделей может быть организована база данных по ОЗ ЗИ. Такая база данных позволит создать достаточно хорошие предпосылки для повышения эффективности решения и числа решаемых в процессе формирования и функционирования СЗИ оптимизационных задач. Это существенно повысит эффективность оптимизации в СЗИ. Структурная компонента такой базы должна содержать достаточно полную информацию о конкретном классе ОЗ.

Предлагается следующая структура информации, составляющей содержание компонента.

1. Нумерация и краткое наименование класса задач.
2. Формулировка типовой задачи класса в наиболее общей ее постановке.

3. Возможные дополнительные ограничения и условия в задаче.

4. Полный список требуемых исходных данных.

5. Перечень моделей задачи с указанием требуемых для их решения дополнительных данных и перечислением дополнительных предположений о характеристиках задачи.

6. Список литературы, где проводится анализ задач из рассматриваемого класса или подобных им задач.

7. Статистические сведения о результатах использования и решения в процессе ЗИ задач из рассматриваемого класса.

Исходные данные получаются в основном на основе экспертных методов, однако многие характеристики могут быть получены на основе обработки статистической информации.

Отметим, что при формализации задачи оптимизируемый критерий и структура модели в существенной степени зависят от структуры и полноты исходной информации. В зависимости от состава исходных данных конкретная ОЗ представляется совокупностью моделей и соответствующих им методов решений. Покажем на примере двух задач.

ПП 1. Резервирование информации в статических условиях функционирования.

Пусть известны число информационных массивов в компоненте СОД и их объемы, объем внешней памяти для хранения информации, потери от простоя средств обработки информации, средние потери от отсутствия каждого массива, затраты на копирование информации. Найти такое распределение памяти на хранение копий массивов информации, при которой суммарные потери минимальны.

Исходные данные:

$k_э$ - коэффициент эффективности, p_j - вероятность успешного решения задачи с использованием j-го массива; μ_j - вероятность того, что массив не будет разрушен при решении задачи в режиме использования; $Z_{M,j}$ - стоимость j единиц машинного времени; $Z_{B,j}$ - стоимость восстановления разрушенного j-го массива; $Z_{H,j}$ - стоимость j-го носителя информации; ν_j - плотность потока обращений к j-му массиву; $\widetilde{W}$ - событие, заключающееся в том, что за время T массив не будет разрушен; $\widetilde{W}'$ - дополнительное к $\widetilde{W}$ событие; $W = P(\widetilde{W});\ Z_{Д,j}$ - стоимость дублирования j-го массива информации; T_j - случайное время решения задачи с использованием j-го массива; N- число различных массивов информации; k_j – число создаваемых копий j-го массива ($1 \le j \le n$); q_j - вероятность разрушения j-го массива или его копии за единичный интервал; $\Pi(k_1,..., k_n)$ - средние затраты машинного времени на копирование данных при стратегии резервирования ($k_1,..., k_n$); $k_{Гi}$ - коэффициент готовности i-го массива; $F_i(k_i)$ - функция затрат при стратегии копирования k_i копий для i-го массива; ρ_j - доля времени, затрачиваемого на работу с j-ым массивом.

Модели.

1) Все данные известны.

$$R \overset{def}{=} \sum_{j=1}^{N} \{\rho_j \left[W\, Z_{M,j} M(T_j / \widetilde{W}) + (1-W) Z_{M,j} M(T_j / \widetilde{W}') + (1-\mu_j) Z_{B,j}\right] \nu_u T +$$

$$+ (1-\rho_j)\left[Z_M M(T_j / \overline{\rho_j}) + Z_{B,j} + Z_{ДВ}\right] \nu_u T + (k_j + 1) Z_{H.j}\} \underset{k}{\longrightarrow} \min$$

либо

$$k_{\hat{Y}} = \frac{\sum_{j=1}^{N} \rho_j W\, Z_{M,j} M(T_j / \widetilde{W})}{R} \underset{k}{\longrightarrow} \min$$

при условии

$$\sum_{i=1}^{N} k_i = k\ ,\ \sum_{i=1}^{N} M(T_i) \le \widetilde{T} \qquad (1)$$

2) Неизвестны часть из величин $\{Z_{Mj}, Z_{Bj}, Z_{Hj}\}$, но все Z_{Mj} однопорядковы по J:

$\sum_{i=1}^{N} M(T_i) \underset{k}{\longrightarrow} \min$ и выполнено (1).

3). Неизвестны часть из величин $\{Z_{Mj}, Z_{Bj}, Z_{Hj}\}$, но известно, что $Z_{Mj} >> Z_{Bj} + Z_{обн}$ и однопорядковы по j величины $\{Z_{Mj}, Z_{Bj}, Z_{Hj}\}$:

$\prod_{j=1}^{N} \mu_j \underset{k}{\longrightarrow} \max$ и выполнено (1).

4) Неизвестны часть из $\{Z_{Mj}, Z_{Bj}, Z_{Hj}\}$, но все эти величины однопорядковы и $Z_{Hj} << Z_{Mj}$:

$$k_{\text{п.д.}} \overset{def}{=} \frac{\sum_{j=1}^{N} \rho_j M(T_j / W)}{\sum_{j=1}^{N} M(T_j)} \xrightarrow[k]{} \max$$

и выполнено (1), где $k_{n.p.}$- коэффициент полезной работы.

5) Неизвестны величины, требуемые для полного нахождения $\nu_u Z_M MT_j$ и $\nu_u (1-\mu_j) Z_B$:

$\sum_{j=1}^{N} \rho_j \xrightarrow[k]{} \max$ и выполнено (1).

Отметим, что решению указанной задачи посвящена [4].

ПП 2. Выбор состава средств обеспечения защиты информации.

Выбрать состав состава средств обеспечения защиты информации (СОЗИ) в СОД таким образом, чтобы суммарные издержки в компоненте были минимальны.

Исходные данные: *m* - число учитываемых дестабилизирующих воздействий (ДВ), *n* - число всех возможных СОЗИ, p_i - вероятность проявления *i*-го ДВ; k_{ij} - вероятность предотвращения *i*-го ДВ при использовании *j*-го СОЗИ; s_j - стоимость *j*-го СОЗИ, ν_i - средние потенциальные потери, порождаемые *i*-ым ДВ.

Модели.

1. Все исходные данные имеются:

$$\sum_{i=1}^{m} \sum_{j=1}^{n} p_i \chi_j (k_{ij} \nu_i + s_j) \xrightarrow[\{\chi_j\}]{} \min$$

при условии

$$\sum_{j=1}^{n} s_j \chi_j \le c \text{ и } \chi_j = 0 \vee 1. \qquad (2)$$

2. Неизвестны $\nu_i (i = \overline{1,n})$.

2.1. Все $\nu_i (i = \overline{1,n})$ однопорядковы

$$\sum_{i=1}^{n} p_i (1 - \prod_{j=1}^{m} (1-k_{ij})^{\chi_j}) \xrightarrow[\{\chi_j\}]{} \max$$

и выполнено (2).

2.2. $\nu_i (i = \overline{1,n})$ разнопорядковы

$$\{(1 - \prod_{j=1}^{m} (1-k_{lj})^{\chi_j}), i = \overline{1,n}\} \xrightarrow[\{\chi_j\}]{} \max$$

и выполнено (2).

3. Отсутствуют ν_i для $i \in I \subset T \overset{def}{=} \{1,2,...,n\}$, а для $i \in T \setminus I$ значения ν_i известны:

$$\sum_{i \in T \setminus I} \sum_{j=1}^{m} p_i \chi_j (k_{ij} \nu_i + s_j) \xrightarrow[\chi_j]{} \min,$$

$$\sum_{i \in I} p_i (1 - \prod_{j=1}^{m} (1-k_{ij})^{\chi_j}) \xrightarrow[\chi_j]{} \max$$

и выполнено (2).

4. { p_i, ν_i } случайны с известными распределениями:

$$d \xrightarrow[\chi_j]{} \max,$$

$$P\{\sum_{i=1}^{n} \sum_{j=1}^{m} p_i \chi_j (k_{ij} \nu_i + c_i) \le d\} \ge \gamma,$$

и выполнено (2), где $\gamma \in (0;1)$ - число, близкое к 1 (уровень доверия).

5. { p_i, ν_i } случайны с прогнозируемыми значениями

$$M(\sum_{i=1}^{n}\sum_{j=1}^{m} p_i\chi_j(k_{ij}\nu_i + c_i) + \sum_{i=1}^{n}\mu_i y_i(p_i - p_i^*)) \xrightarrow[\chi_j]{} \min,$$

$$\sum_{j=1}^{m} c_j\chi_j + \sum_{i=1}^{n} y_i \le c,\ \chi_j = 0 \vee 1,\ y_i \ge 0,$$

где c - заданные ресурсы, { p_i^* }- статические оценки { p_i }.

6. { p_i, ν_i } заданы функциями предпочтения (ФП). Надо найти ФП μ на множество $\{\chi_j\}_{j=1}^{n}$ такую, что (см.(1))

$$\min K \xrightarrow[\{\chi_j\}]{} \max,$$

и выполнено $\mu(\{\chi_j\}) \ge \lambda$, где λ- заданный уровень.

7. Нет достаточных данных о *{p_i, ν_i}* , но есть возможность получения экспертных оценок.

Приведенная процедура при ее полной реализации позволит сформировать полный набор макрозадач и оптимизационных задач, решение которых может потребовать в процессе обеспечения защиты информации в процессе обработки данных. Реализация подобной процедуры, описанная в [1], позволила сформировать набор из более чем трехсот задач. Из полученной совокупности на основе экспертного отбора выбрасываются те из них, которые не представляют интереса в текущий момент на рассматриваемом объекте защиты. Оставшиеся задачи целесообразно оценить и упорядочить по степени их важности.

Заключение

В работе описана формализованная, опирающаяся на системный подход процедура формирования относительного полного множества задач защиты информации для конкретного объекта защиты, решение которых может потребоваться в процессе обеспечения информационной безопасности.

Литература

1. *Попов Г. А., Попова Е. А*. Системный подход к формированию множества угроз информационному и образовательному пространству. – Сборник трудов Межд. научно-практ. конф. «Эволюция системы научных коммуникаций», Ассоциация университетов прикаспийских государства. – Астрахань, 2008, с. 127-132.
2. *Герасименко В. А., Таирян В. И., Попов Г. А*. Основы оптимизации в системах управления. Монография. – Деп. в ВИНИТИ 12.03.1989, № 213-В89-68.
3. *Попов Г. А*. Методологические основы комплексной оптимизации в системах защиты информации. Докт. дис. – М., РГГУ, 1991. – 406 с.
4. *Кульба В. В., Ковалевский С. С., Шелков А. Б*. Достоверность и сохранность информации в АСУ. – М., Синтег, 2003. – 500 с.