Методика оценки и выбора типовых средств защиты информации для автоматизированных систем защищенного исполнения территориальных органов внутренних дел

Орлов
Олег Владимирович,
начальник Пензенского филиала
ВИПК МВД России,
полковник полиции

В автоматизированных системах защищенного исполнения (АСЗИ), обрабатывающих конфиденциальную информацию, выбор средств защиты информации (СрЗИ) всегда остается одной из важных проблем, от решения которой зависит эффективность функционирования таких систем. Особенно остро эта проблема возникает в связи с использованием стандартных (открытых) протоколов передачи данных, которые создают возможности удаленного несанкционированного доступа (НСД) к данным и вычислительному процессу со стороны злоумышленников. Поэтому при проектировании АСЗИ ОВД задача защиты информационных процессов от НСД, модификации и искажений программ и данных является весьма актуальной и **практически** значимой. О важности такой задачи на государственном уровне подчеркивается в федеральном законе «Об информации, информатизации и защите информации» (от 27.06.2006 № 149-ФЗ).

Можно выделить следующие основные задачи, которые должны решаться при выборе СрЗИ для разрабатываемой АСЗИ ОВД:

- обеспечение безопасности данных, особенно при их хранении, обработке и передаче по каналам связи (методы криптографии, разделения доступа и т. д.);
- обеспечение безопасности аппаратных средств (спецпроверки на закладные устройства, специсследования на побочные электромагнитные излучения и наводки и т. д.) и программного обеспечения (дополнительное тестирование на отсутствие недекларированных возможностей);
- обеспечение защиты от утечки информации по техническим каналам, связанным с использованием строительных конструкций и инженерных коммуникаций помещений и зданий (акустический, виброаккустический каналы, по линиям связи, питания и т. д.);
- использование программно-аппаратных средств защиты от НСД (для отдельных рабочих мест, сетевых и межсетевых);
- сочетание перечисленных выше направлений с организационно-техническими мерами в рамках СрЗИ.

Основной целью средств и систем ЗИ является обеспечение противодействия потенциальным угрозам информации в АСЗИ ОВД.

Оптимальный выбор средств защиты информации для проектируемой АСЗИ ОВД предполагает определение природы угроз, формы и пути их возможного проявления и реализации в автоматизированных системах защищенного исполнения. Решение поставленной задачи заключается в том, что все многообразие угроз и путей их воздействия сводится к простейшим видам и формам, которые были бы адекватны их множеству в типовых АСЗИ.

Угрозы для АСЗИ можно классифицировать как непреднамеренные и преднамеренные:

- **непреднамеренные** — это угрозы, обусловленные случайными или ошибочными действиями персонала, которые при возникновении легко устраняются и поэтому не создают проблемы при проектировании АСЗИ ОВД;
- **преднамеренные** — это угрозы, обусловленные несанкционированным доступом к информации.

Для АСЗИ ОВД наиболее опасными являются преднамеренные угрозы, к которым относятся: несанкционированный доступ к информации, хранящейся в памяти компьютерной системы; специальное программное обеспечение, предназначенное для осуществления несанкционированного доступа; программные продукты, частично либо полностью выводящие из строя компьютерную систему; компьютерные вирусы; подделка электронных подписей; несанкционированная модификация, приводящая к нарушению целостности данных; перехват данных по каналам утечки информации.

Преднамеренные угрозы могут быть реализованы программным путем либо внепрограммными средствами.

Для АСЗИ ОВД наиболее опасными угрозами становятся нелегальные программные средства и вирусы. Наиболее опасными из них являются вирусы, осуществляющие преодоление защиты программных продуктов, приводящие к сбоям и уничтожению данных. Поэтому важной задачей при проектировании АСЗИ ОВД является анализ ее уязвимых компонент и мест, которые должны быть надежно перекрыты типовыми СЗИ.

Методика составления процедур выбора типовых СрЗИ для проектируемой АСЗИ ОВД

В качестве типового объекта защиты в статье рассматривается вычислительная система, которая может быть элементом автоматизированной системы ОВД.

Возможные способы воздействий на информационные ресурсы в защищенных компьютерных сетях можно классифицировать по следующим признакам.

1. По принципу несанкционированного доступа (физическая атака; логическая атака).
2. По положению источника несанкционированного доступа (в локальной сети; вне локальной сети).
3. По режиму выполнения несанкционированного доступа (атаки, выполняемые при участии человека; специальными программами).
4. По типу используемых слабостей системы информационной безопасности (атаки, основанные на: недостатках организации информационной безопасности; ошибках административного управления компьютерной сетью; недостатках алгоритмов защиты; ошибках реализации проекта СЗИ).
5. По пути несанкционированного доступа (атаки, ориентированные на использование: прямого стандартного пути доступа к информационным ресурсам; скрытого нестандартного пути).
6. По текущему месту расположения конечного объекта (атаки на информацию: хранящуюся на внешних запоминающих устройствах; предаваемую по линии связи; обрабатываемую в основной памяти компьютера).
7. По непосредственному объекту атаки (атаки на организацию информационной безопасности и процесс административного управления; атаки на постоянные компоненты СЗИ; атаки на сменные элементы СЗИ; нападения на протоколы взаимодействия; нападения на функциональные элементы компьютерной сети).

Конечным объектом атаки всегда является защищаемая информация. Под непосредственным же объектом атаки понимается объект информатизации, анализ характеристик или непосредственное использование которого позволяет успешно реализовать несанкционированный доступ к защищаемой информации.

Применяемые для осуществления информационных атак разрушающие программные средства могут доставляться на объект воздействия локальных или телекоммуникационных сегментов компьютерных сетей с помощью традиционных методов (местного доступа, записи их на электронные носители и т. д.) либо дистанционно, с помощью передачи по сети, включая радиоканалы.

Внедрение разрушающих программных средств может осуществляться на этапах освоения или модернизации ПО, в результате преодоления СЗИ и несанкционированного доступа к ресурсам компьютерной сети, а также в результате нерегламентированных действий санкционированных пользователей.

Поскольку компьютерные сети представляют собой сложные системы, при разработке моделей информационных воздействий на эти объекты целесообразно использовать принцип функциональной декомпозиции.

В этой связи в отношении АП и их ПО могут иметь место следующие действия:

- искажение программ и данных в оперативной памяти АП;
- искажение файлов и системных областей;
- вмешательство в процесс обмена сообщениями по сети путем посылки хаотических сообщений;
- блокирование принимаемых или передаваемых сообщений, их искажений;
- имитация приглашений ввода пароля с целью запоминания паролей;
- накопление обрабатываемой конфиденциальной информации в скрытых областях внешней памяти;
- исследование оперативной памяти с целью выявления фрагментов ценной информации и т. д.
- В отношении серверов локальных сетей могут возникать следующие угрозы:
- искажение проходящей через сервер информации (при обмене между АП);
- искажение или уничтожение собственной информации сервера (например, идентификационных таблиц) и, как следствие, нарушение работы сети;
- заражение вирусами пересылаемых внутри локальной сети или на удаленные АП файлов;
- сохранение проходящей информации в скрытых областях внешней памяти и т. д.

Могут также возникнуть угрозы: разрушения собственного ПО коммутационных машин сети и вывода из строя вместе с коммутационным узлом всех присоединенных АП; внедрения разрушающих программных средств в пакеты, формируемые коммутационными машинами; засылки пакетов не по адресу; потери обрабатываемых пакетов, их неверной сборки и подмены.

В системе передачи данных компьютерной сети возможны:

- перехват, искажение и навязывание информации со стороны коммуникационных фрагментов сети;
- имитация посылки ложных сообщений на «локальные» фрагменты сети;
- внедрение в транзитную информацию разрушающих программных
- средств;
- перехват, навязывание и искажение информации при передаче ее по линиям связи локальных, региональных и глобальных сегментов компьютерной сети.

Особенности построения системы защиты информации в АСЗИ ОВД

Типовая СЗИ, базовой структурой которой является КСЗИ, представляет собой сложную организационно-техническую систему, включающую различные технические и программные подсистемы и элементы, объединенные в программно-технические (ПТК) и программно-моделирующие комплексы (ПМК), вместе образующие комплекс средств защиты информации в АСЗИ ОВД и характеризующиеся большим количеством разнородных параметров. Следовательно, повышение эффективности функционирования АСЗИ ОВД требует совершенствования существующего и разработки нового методического обеспечения, охватывающего различные задачи и этапы данного процесса, которое должно основываться на создании соответствующего математического обеспечения (МО), включающего математические и имитационные модели, реализующиеся в программном (ПО) обеспечении, что позволит повысить качество и автоматизировать основные этапы выбора СрЗИ при проектировании АСЗИ ОВД.

Таким образом, при выборе КСЗИ для разрабатываемой АСЗИ ОВД требуется решить задачи двух типов: осуществить структурный и параметрический синтез проектируемой системы в рамках возможных угроз и каналов утечки информации и провести анализ ее эффективности в процессе функционирования с целью выбора наиболее эффективных (достаточных) способов и СрЗИ.

Задачу проектирования АСЗИ ОВД, включающую формирование

его рациональной структуры и выбор наиболее эффективных СрЗИ (программных и технических), можно представить в виде совокупности следующих процедур:

1. Анализ исходных данных (назначение, структура, функциональные схемы, характеристики, состав технических средств и программного обеспечения, виды и гриф информации в АСЗИ и т. д.), выработка требований к СЗИ, формирование набора показателей ее эффективности и установление их граничных значений, обеспечивающих минимально допустимый уровень ИБ (защиты).
2. Определение всех возможных каналов утечки и НСД к информации в АСЗИ. Определение из всех выявленных каналов НСД и утечки информации конкретного подмножества потенциально возможных каналов для использования нарушителями предполагаемого класса.
3. Выбор типовой структуры КСЗИ (синтез), программных и технических средств защиты (определение требований на вновь создаваемые средства в случае отсутствия готовых). Оценка показателей эффективности каждого предлагаемого средства ЗИ относительно всех перекрываемых им каналов утечки и НСД к информации и угроз, которым осуществляется противодействие (анализ) и их объединение в комплекс путем решения задачи оптимального синтеза [61]. Таким образом удается перекрыть все выявленные и учитываемые каналы утечки информации и НСД к информации (обеспечить противодействие угрозам) с заданной нормой эффективности ЗИ.
4. Оценка комплексной эффективности выбранных КСЗИ в целом (анализ), структурно-параметрическая доработка с целью достижения заданных требований (замена отдельных средств защиты информации, введение дублирования для наиболее опасных каналов, угроз и т. д.).

Анализ содержания этих этапов и входящих в них процедур позволяет сделать вывод, что они содержат задачи как слабоформализуемые, требующие для выполнения квалифицированных специалистов, привлечения экспертов, применения эвристических методов и подходов, так и такие, которые могут быть формализованы в рамках задач и методов структурного синтеза с привлечением положений теории математического программирования (формирование структуры КСЗИ, оптимальный выбор состава СрЗИ), а также на основе методов математического моделирования случайных процессов и систем (расчет, оценка и анализ показателей эффективности СрЗИ и КСЗИ в целом).

Множество способов и средств для использования на уровне АСЗИ ОВД будет включать в себя операции: контроля доступа на территорию объекта, в помещение сервера и к рабочим станциям; контроля вскрытия аппаратуры; шифрования в ЛВС, сервере, отдельных ПЭВМ; опознания, разграничения и контроля доступа к ресурсам сети, ОС, БД, пользовательскому ПО и данным; снижения уровня информационного наполнения и преобразования опасных побочных электромагнитных излучений и наводок (ПЭМИН); контроля целостности информационно-программной среды на уровне ЛВС, ОС и прикладном; противодействия утечки по техническим каналам различной природы и т. д.

Выбор необходимых средств из всего подобного множества доступных (сертифицированных) для построения КСЗИ, обеспечивающих перекрытие выявленных и предполагаемых каналов утечки и НСД к информации с заданными нормами эффективности, представляет собой задачу, которая может быть формализована с привлечением методов и положений оптимального структурного синтеза сложных систем и направлена на максимальное выполнение требований к уровню ИБ (норм эффективности ЗИ). Эти требования и нормы лежат в основе формирования соответствующих целевых функций и ограничений, составляют исходную базу для решения всех возникающих подзадач синтеза и оптимизации. Анализ существующих подходов к данной задаче, в том числе рекомендаций, изложенных в государственных стандартах и руководящих документах (РД) ОВД РФ, позволяет достаточно полно представить номенклатуру основных требований к СЗИ в АСЗИ ОВД. Конкретные требования к СЗИ, обусловленные спецификой автоматизированной обработки защищенной информации, определяются совокупностью следующих факторов: характером обрабатываемой информации; объемом обрабатываемой информации; продолжительностью пребывания информации в АСЗИ; структурой АСЗИ; грифом защищаемой информации; технологией обработки информации; вычислительного процесса в АСЗИ; этапом жизненного цикла АСЗИ.

Формирование структуры и состава КСЗИ в СЗИ базируется на таких требованиях и основных принципах защиты, приведенных в РД, которые устанавливают, что программно-технические средства защиты не должны существенно ухудшать основные функциональные характеристики АСЗИ ОВД. Также указывается, что неотъемлемой частью работ является оценка эффективности средств защиты, которая должна осуществляться по методикам, учитывающим всю совокупность технических характеристик оцениваемого объекта, включая технические решения и практическую реализацию средств защиты.

При этом следует учитывать, что система защиты информации в целом является сложным организационно-техническим объектом, выполняющим множество функций, кроме того идентификацию пользователей, разграничение их полномочий, закрытие технических каналов утечки информации и т. д. Для каждого структурного элемента КСЗИ и выполняемой функции возможно применение различных программных и технических средств, во множестве представленных на рынке. Следовательно, возможно построить множество вариантов КСЗИ в конкретной АСЗИ, отличающихся структурой, составом, технико-экономическими показателями (быстродействие, надежность, стоимость и т. д.). Так как большинство подобных показателей взаимно противоречивы, то выбор конкретного КСЗИ на основе принципа «необходимой достаточности» приводит к необходимости решать оптимизационную задачу, что требует наличия набора показателей эффективности ЗИ и соответствующих критериев оптимальности построения защиты.

Показатели эффективности (y) являются некоторым множеством функций от характеристик системы (x):

$$y_n = f(x_i);\ n = \overline{1,K};\ i = \overline{1,N}.$$

Характеристики СЗИ имеют как количественный (параметры), так и качественный характер. На основе множества показателей формируются критерии, позволяющие сравнивать различные варианты построения защиты и выбирать наилучший.

В качестве основных критериев обычно используются: вероятность непреодоления злоумышленником системы защиты информации, надежность КСЗИ, стоимость, прочность защиты информации, время преодоления защиты, стойкости шифра, сложность и т.д. Следовательно, задача синтеза оптимального КСЗИ, включающая в качестве подзадач формирование структуры, выбор состава СрЗИ, объединение СрЗИ в комплекс, расчет и оценку показателей эффективности программных и технических средств ЗИ в отдельности и всего получаемого КСЗИ в целом, является многокритериальной и многоэтапной и требует использования специальных методов решения, в том числе экспертных. При оптимизации необходимо обязательно учитывать ограничения, налагаемые на привлекаемые ресурсы, т.е. имеется задача условной оптимизации.

Таким образом, рассматривая задачу построения оптимального КСЗИ в СЗИ как задачу проектирования сложного технического объекта, ее математическую постановку можно представить в следующем виде.

Исходные данные:

$F = \{f_1 \ldots f_n\}$ — защитные функции;

$Y = \{y_1 \ldots y_n\}$ — показатели, характеризующие эффективность ЗИ;

$M = \{m_1 \ldots m_n\}$ — множество средств защиты имеющихся типовых программно-аппаратных комплексов, реализующих различные способы и функции защиты и возможных для применения в конкретном случае;

$U = \{u_1 \ldots u_n\}$ — способы управления ЗИ.

Критерии оптимальности $K = \varphi(Y)$, где $Y = (F, M, U)$.

Постановка задачи: найти такие значения $M^* \in M$, при которых $K(Y^*) \in extr$, $Y^* \in Y_D$, где Y_D — множество допустимых значений показателей.

Таким образом, требуется сформировать структуру КСЗИ и выбрать состав способов и СрЗИ из множества доступных, которые обеспечивают выполнение всех необходимых функций при условии достижения оптимума используемого критерия и выполнение ограничений на показатели эффективности и затрачиваемые ресурсы.

Значения показателей, необходимые для расчета критериев, определяются с помощью математического моделирования, экспериментальных исследований, экспертных оценок. При этом следует учитывать, что результаты исследований различных авторов позволяют сделать вывод о предпочтительности использования в качестве показателей эффективности ЗИ вероятностных, в том числе вероятностно-временных, характеристик функционирования СрЗИ и КСЗИ в целом.

Рассмотренная выше задача разработки КСЗИ с оптимальным составом в части формирования структуры и выбора СрЗИ может быть отнесена к классу проектных задач структурного синтеза. Для решения подобной задачи, сводимой к выбору наиболее предпочтительного варианта в конечных множествах, возможно применение автоматизированных средств формального синтеза совместно со средствами анализа и оценки характеристик создаваемого объекта и поддержки принятия решений в интерактивном режиме. Как было показано выше, часть процедур оптимального формирования состава и структуры КЗСИ могут быть формализованы и приведены к виду, допускающему применение методов математического программирования, в том числе и алгоритмов решения стандартных задач дискретного программирования.

Задачей таких методов и процедур является преобразование исходного описания объекта (требования, условия эксплуатации, ограничения на стоимость и другие ресурсы и т.д.) в результирующий, содержащий сведения о структуре, составе элементов, способах их взаимодействия. Исходное описание формируется на базе ТЗ.

Принятие решений по выбору оптимального варианта создаваемой системы включает в себя следующие основные подзадачи: представление множества оцениваемых вариантов (альтернатив) в наглядной и удобной форме; выбор необходимых показателей эффективности функционирования проектируемой системы; построение модели синтезируемого объекта; анализ функционирования объекта; определение значений показателей и критериев оптимальности; формирование предпочтений при учете множества критериев; установление порядка предпочтений вариантов при использовании качественных показателей; выбор методов поиска оптимальных вариантов (сокращенного перебора альтернатив); сведение задач синтеза к стандартным задачам оптимизации и их решение известными методами математического программирования. При этом следует учитывать, что все используемые характеристики, показатели и критерии должны иметь (быть преобразованы) в числовую (количественную) форму.

Для поиска оптимальных вариантов, если задачу формирования состава КСЗИ удается формализовать и представить варьируемые параметры в числовой форме, возможно применить методы дискретного математического программирования. Тогда данную задачу можно представить в следующем виде:

$F(X) \to extr,$

$X \in D \;\; W(X) > 0, Z(X) > 0,$

где $F(X)$ — целевая функция, математически выражающая критерии оптимальности;

X — множество варьируемых переменных, включающее как параметры СрЗИ, так и показатели эффективности их функционирования;

D — множество допустимых значений X; W (X), Z (X) — ограничения.

Анализ содержания задачи формирования КСЗИ при проектировании, имеющихся подходов и методик, математических методов, применяемых, рекомендуемых и возможных к применению для формализации и решения, показывает, что целесообразно математическую постановку и решение такой задачи осуществлять на основе методик дискретного математического программирования. При этом данная задача может быть сведена к совокупности известных задач.

Предлагается следующая постановка основных задач оптимального выбора состава СрЗИ при разработке наиболее рациональных вариантов построения КСЗИ.

Имеется множество угроз ИБ объекта информации АСЗИ u_j, $j = \overline{1,m}$, каждая из которых связана с определенными каналами НСД и утечки.

Также имеется конечное множество способов и средств ЗИ Z_i, $i = \overline{1,n}$, которые при противодействии каждой j-й угрозе обеспечивают эффективность зашиты $\mathring{A}_{ij}$, оцениваемую показателем в форме вероятности непреодоления защиты i-го средства при реализации угрозы j P_{ij}.

Заданы требования по комплексной эффективности ЗИ при наличии множества всех данных угроз E в форме вероятности непреодоления защиты $P_з$ [61], а также по эффективности защиты от каждой угрозы $\mathring{A}_j$ (вероятность непреодоления защиты P_j .

Необходимо выбрать оптимальный состав СрЗИ, обеспечивающих при объединении в КСЗИ противодействие всем учитываемым угро-

зам с эффективностью не меньше заданной (E_3, E).

В качестве основных критериев целесообразно использовать следующие:
- минимальное количество используемых средств ЗИ;
- минимальное число типов используемых средств;
- максимальное значение эффективности СрЗИ; E_i или (и) Е при ограничениях затрат (например, стоимость набора средств ЗИ

$$C = \sum_{k=l}^{l} C_K$$

где $C_к$ — стоимость выбранного средства ЗИ, l — число выбранных средств;
- минимальная стоимость (затраты) набора средств ЗИ при обеспечении заданного уровня эффективности;
- минимальное отвлечение ресурсов ВС при функционировании средств ЗИ (требуемые ресурсы для каждого средства на Z_i известны) и т. д.

Выбор необходимых средств Z_i из всего подобного множества доступных (сертифицированных) Z для построения КСЗИ, обеспечивающего перекрытие заданных каналов утечки и НСД к информации и противодействия угрозам с требуемой эффективностью, сформулируем в виде постановки задачи полного оптимального покрытия. Найти вектор целочисленных варьируемых переменных $X = \{x_1\}$, $i = \overline{1,n}$, минимизирующих линейную целевую функцию

$$\sum_{i=l}^{n} x_i \to \min$$

при ограничениях

$$\sum a_{ij} x_i \geq 1, j = \overline{1,m},$$

где x_i — принимают значения 0 или 1; n — число рассматриваемых средств ЗИ;

m — количество учитываемых каналов (угроз) НСД и утечки информации;

α_{ij} — коэффициенты, характеризующие функциональные возможности каждого средства защиты: $\alpha_{ij} = 1$, если i-е средство обеспечивает перекрытие j-го канала (противодействие j-му типу угроз); $\alpha_{ij} = 0$ противном случае.

Значение $x_i = 1$ соответствует включению в проектируемую систему ИБ соответствующего (i-го) способа СрЗИ, $x_i = 0$, в противном случае.

Условия выражают требования обеспечения ЗИ от доступа или утечки по любому из возможных каналов (противодействие любой угрозе) с помощью хотя бы одного из используемых способов и средств.

В случае необходимости учета дополнительных свойств средств ЗИ критерии оптимальности представляется в виде

$$\sum_{i=l}^{n} c_i x_i \to \min ,$$

где c_i — показатели, отражающие наиболее важные параметры и характеристики средств ЗИ (стоимость; интенсивность отказов; время, затрачиваемое на реализацию процесса защиты; объем требуемых ресурсов ЭВМ и т. д.).

Выражение позволяет оптимизировать как состав, так и ресурсные и надежностные характеристики создаваемой СЗИ АСЗИ.

Выбор типовых СрЗИ для проектируемой АСЗИ ОВД с использованием разработанной методики оценки эффективности их функционирования

Методика комплексной оценки эффективности СП АССУ ОВД с использованием разработанных имитационных и аналитических моделей включает в себя:
1. Выбор типовых вариантов структуры СП.
2. Формальное описание процедур противодействия угрозам безопасности корпоративной сети АССУ ОВД.
3. Оценка временных характеристик процедур противодействия угрозам безопасности с использованием разработанных математических моделей.
4. Оценка временных показателей эффективности СП первого уровня иерархии в виде статистических выборок из результатов имитационного моделирования процедур противодействия.
5. Расчет показателей эффективности СП второго уровня иерархии.
6. Расчет показателей эффективности СП третьего уровня иерархии.
7. Определение интегрального (обобщенного) показателя эффективности СП как показателя четвертого уровня иерархии.

Для опробирования разработанной методики проведем сравнительную оценку, для чего выберем состав типовых вариантов КСЗИ, имеющих оценку, полученную другими, уже используемыми методами. Проведем оценку применяемых в ряде территориальных органов внутренних дел СП «Снег» (имеющей оценку вероятности защиты 0,8) и СП «Кобра» (вероятность защиты — 0,45).

Применение новой методики (расчеты могут быть представлены заинтересованным лицам) дает результаты: применение СП «Кобра» — 0,45, СП «Снег» — 0,8. Расчеты подтверждают эффективность применения СП «Снег» почти в два раза выше по сравнению с СП «Кобра».

Соответствие полученных результатов известным оценкам свидетельствует о корректности разработанной методики расчета, которая, в отличие от известных, сокращает объем используемых формул, что упрощает инженерные расчеты при проектировании АСЗИ ОВД. Аналогично могут быть проведены расчеты и по другим, в том числе новейшим СКЗИ, любого звена управления территориальных органов внутренних дел.