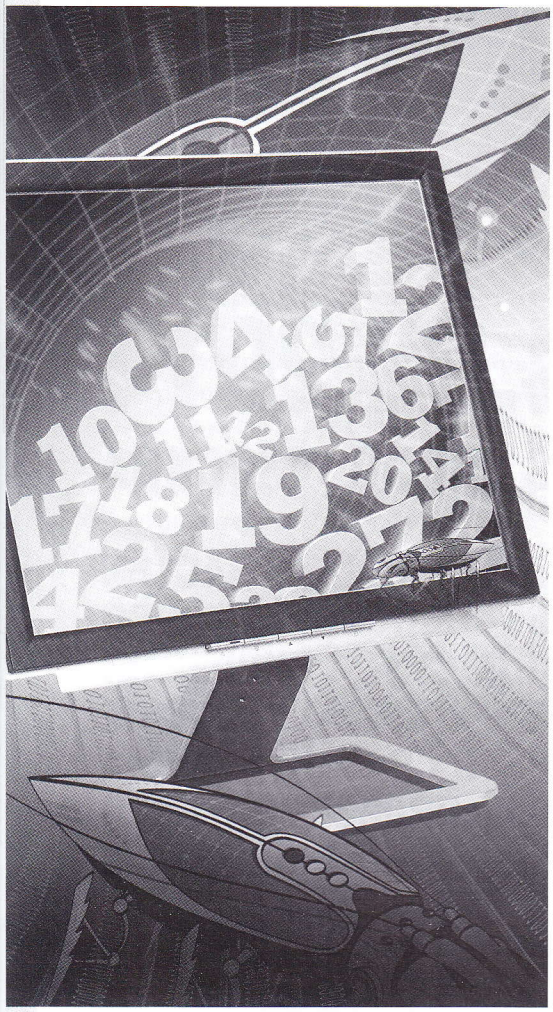
Что такое «закладочные устройства» и как с ними бороться. Часть 2

Г. А. Бузов, *кандидат военных наук, доцент, заведующий лабораторией защиты информации от утечки по техническим каналам*

Учебный центр «Информзащита»



В предыдущей статье мы разобрали вопросы, касающиеся, прежде всего, побудительных мотивов, которые должны подтолкнуть руководителя фирмы к принятию решения об организации и проведении поисковых работ для выявления различного рода закладных устройств (ЗУ) с целью пресечения утечки информации конфиденциального характера. Кроме того, выяснили, что, обеспечивая собственную безопасность, можно выполнять поисковые работы без лицензии ФСБ России на данный вид деятельности.

При рассмотрении различных возможных ситуаций был дан краткий анализ необходимых мероприятий, проведение которых наиболее целесообразно в том или ином случае. При этом мы выяснили, что наиболее полный комплекс мероприятий проводится после принятия решения о проведении профилактической проверки.

Однако в любом случае работы по подготовке к комплексной проверке начинаются после принятия управленческого решения о ее проведении. Как правило, целью такой проверки является выявление и закрытие возможных каналов утечки информации через различного рода ЗУ. Свое решение руководитель принимает, основываясь на выводах из анализа конкретной ситуации, полученных специалистами отдела технической защиты информации.

Таким образом, вся черновая работа по вопросам грамотного и обоснованного принятия руководителем управленческого решения, по организации защиты информации ложится на плечи специалистов по обеспечению информационной безопасности фирмы. Для своевременной и качественной подготовки исходных материалов, для принятия управленческого решения они должны в полном объеме владеть методикой его принятия. Этому немаловажному вопросу и посвящается данная статья.

Прежде всего необходимо разобраться в том, что же представляет собой управленческое решение. Согласно определению, управленческое решение – это волевой, творческий, организационно-распорядительный акт руководителя (менеджера), определяющий содержание и порядок действий подчиненных при выполнении поставленной задачи.

Управленческое решение является результатом знаний, опыта, воли и творчества руководителей, и в первую очередь, главного руководителя (президента, генерального директора), поскольку он утверждает, а зачастую и единолично принимает решение и несет за него всю полноту ответственности. От качества принятого решения зависит эффективность работ по выявлению ЗУ, поэтому процессу принятия решения предшествует процесс его выработ-

ки. Он включает в себя как поиск наилучших путей достижения цели, так и выявление проблем, требующих немедленного решения.

Если принятие решения – всегда прерогатива начальника, то выработка путей его реализации, процесс его оптимизации – обычно коллективное творчество группы специалистов, заинтересованных в принятии наилучшего варианта.

Наиболее общим подходом к выбору и обоснованию управленческого решения, включающим выбор принципов, форм, средств, логических операций для осуществления процесса выработки решения, является общая методология выработки управленческого решения (рис. 1). Для каждой конкретной области деятельности на базе общей методологии выработки управленческого решения разработана своя методика принятия последнего, учитывающая специфические особенности той сферы деятельности, в которой таковое принимается.

Рассмотрим вариант выработки управленческого решения о проведении комплексной проверки с целью защиты информации от утечки через различного рода ЗУ. Алгоритм принятия такого решения представлен на рис. 2.

Более детально рассмотрим каждый блок, входящий в алгоритм.

Уяснение поставленной задачи является исходным и важным этапом выработки решения. Именно здесь начинает свое рождение основная идея выполнения комплексной проверки, которая на последующих этапах будет углубляться и детализироваться с учетом конкретных особенностей обстановки и возможных ее изменений. Известно, что все явления и процессы окружающего нас мира взаимосвязаны. Эти причинные зависимости порой так обширны и многогранны, что не всегда можно легко и просто их проанализировать, при этом требуется слаженная мыслительная работа. Параллельно с уяснением задачи оценивается обстановка.

Под ***оценкой обстановки*** в ходе выработки решения понимается установление причинно-следственных связей всех ее элементов и их влияния на выполнение стоящей задачи. Основная цель оценки обстановки состоит в установлении степени влияния различных факторов на успешность выполнения поставленной задачи. При этом руководитель может сделать выводы о том, действия каких факторов следует нейтрализовать как препятствующих выполнению задачи, а действия каких факторов следует использовать в качестве способствующих ее выполнению. В зависимости от содержания поставленной задачи оценка обстановки может проводиться различно, так как на процесс решения задач могут влиять в той или иной мере абсолютно разные факторы. Наиболее оптимальным при принятии решения на проведение комплексной проверки представляется следующий вариант оценки обстановки:

- оцениваются потенциальные возможности вероятного противника (злоумышленника);
- собственные силы и возможности;
- условия, в которых придется решать поставленные задачи.

В данном варианте оценка обстановки условно разделена на блоки. Это позволяет в процессе оценки не пропустить элементы, которые могут оказать существенное влияние на грамотное принятие решения. В ре-

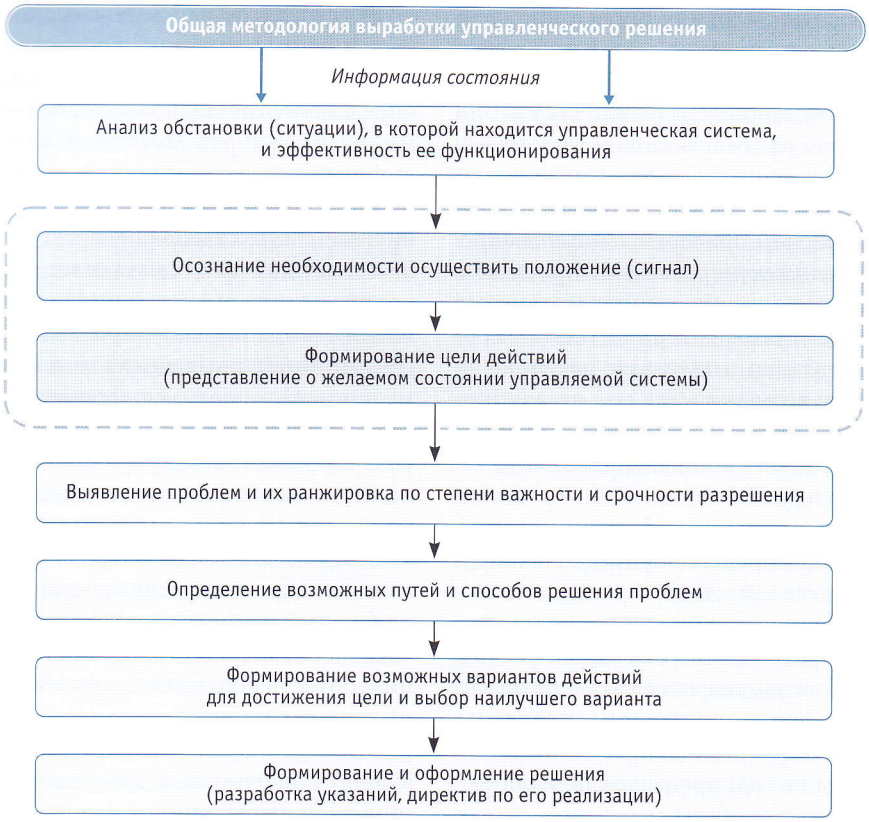


Рис. 1. ***Общая методология выработки управленческого решения***

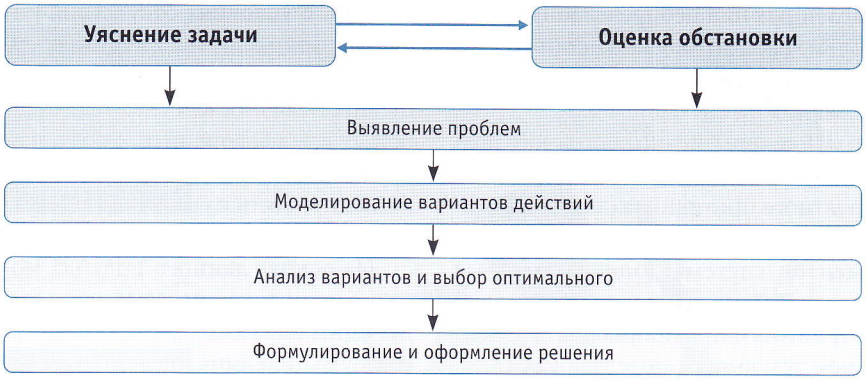


Рис. 2. ***Алгоритм принятия управленческого решения***

альных условиях оценка производится комплексно, и зачастую бывает невозможно разделить общую оценку обстановки на блоки, так как они тесно взаимосвязаны между собой.

Львиную долю времени при принятии решения на проведение комплексной проверки занимает ***определение портрета потенциального злоумышленника***, интересующегося сведениями, которыми обладает организация, и оценка его потенциальных возможностей для несанкционированного получения вашей информации конфиденциального характера. Сложность задачи заключается в том, что в большинстве случаев не представляется возможным с высокой степенью вероятности определить противостоящую сторону, то есть в этом случае мы вынуждены решать слабо определенные или неопределенные проблемы. И здесь на помощь приходит системный подход при решении неопределенных проблем.

Системный подход – это концепция решения сложных слабо определенных или неопределенных проблем, рассматривающая объект изучения (исследования) или проектирования в виде системы.

При применении системного подхода определение возможностей вероятного противника (злоумышленника) будет являться одним из элементов системы, оценка которых сводится к моделированию действий вероятного противника. В дальнейшем результаты моделирования ложатся в основу разработки вариантов проведения комплексной проверки. Моделирование действий вероятного противника, направленных на добывание информации, предусматривает анализ способов ее хищения с целью оценки наносимого этими способами ущерба и разработки вариантов противодействия.

Оно включает:

- моделирование способов физического проникновения злоумышленника к местам возможной циркуляции интересующей его информации;
- моделирование и оценку возможностей получения информации с использованием технических каналов утечки информации.

Действия злоумышленника по добыванию информации, так же как и других материальных ценностей, определяются поставленными целями и задачами, его мотивами, квалификацией и технической оснащенностью. Аналогично криминалистике, где расследование преступления начинается с поиска ответа на вопрос «кому это выгодно?», выявление потенциального противника следует начать с выяснения того, кому нужна защищаемая информация, с последующей оценкой возможностей злоумышленника по проникновению на объект защиты с целью установки ЗУ.

Для создания модели угрозы физического проникновения достаточно близкой к реальной необходимо «перевоплотиться» в злоумышленника, то есть попытаться мысленно проиграть с позиции последнего варианты проникновения к месту циркуляции информации. Чем больше при этом будет учтено факторов, влияющих на эффективность проникновения, тем выше адекватность модели. В условиях отсутствия информации о злоумышленнике, его квалификации, технической оснащенности во избежание грубых ошибок лучше переоценить угрозу, чем ее недооценить, хотя такой подход может привести к увеличению затрат на защиту.

На основе данного подхода модель злоумышленника выглядит следующим образом:

- злоумышленник представляет собой серьезного противника, тщательно готовящего операцию проникновения, он изучает обстановку вокруг территории организации, наблюдаемые механические преграды, средства охраны, телевизионного наблюдения и дежурного (ночного) освещения, а также сотрудников, с целью добывания от них информации о способах и средствах защиты;
- он имеет в распоряжении современные технические средства проникновения и преодоления механических преград;
- всеми доступными способами добывает и анализирует информацию о расположении зданий и помещений организации, о рубежах охраны, о местах хранения источников информации, видах и типах средств охраны, телевизионного наблюдения, освещения и местах их установки;
- проводит анализ возможных путей проникновения к источникам информации и ухода после выполнения задачи.

При моделировании действий квалифицированного злоумышленника необходимо также исходить из предположения, что он хорошо представляет современное состояние технических средств защиты информации, типовые варианты их применения, слабые места и «мертвые» зоны диаграмм направленности активных средств охраны.

Так как искусственно созданные каналы являются рукотворными, для их организации в помещение или в технические средства должны внедряться те или иные электронные компоненты устройств съема или дорабатываться сами объекты с целью усиления требуемых свойств. Таким образом, для их нейтрализации необходимо обнаружить непосредственно физическое тело (схему, компонент) устройства съема или демаскирующие признаки работ по усилению естественных свойств информационных полей.

Обнаружение и распознавание каналов утечки информации, так же как любых объектов, производится по их демаскирующим признакам. При этом моделирование технических каналов утечки информации по существу, является единственным методом достаточно полного исследования их возможностей, определения демаскирующих признаков с целью последующей разработки способов и средств для выявления ЗУ. В основном для этой цели применяются вербальные и математические модели.

Физическое моделирование каналов утечки затруднено и часто невозможно по следующим причинам:

- приемник сигнала, поступающего по каналу, является средством злоумышленника, его точное месторасположение и характеристики службе безопасности неизвестны;
- канал утечки включает разнообразные инженерные конструкции

(бетонные ограждения, здания, заборы и др.) и условия распространения носителя (переотражения, помехи и т. д.), воссоздание которых на макетах невозможно или потребуют огромных расходов.

Применительно к моделям каналов утечки информации целесообразно иметь модели, описывающие каналы в статике и динамике.

Статическое состояние канала характеризуют структурная и пространственная модели. Структурная модель описывает структуру (состав и связи элементов) канала утечки. Пространственная модель содержит описание положения канала утечки в пространстве:

- места расположения источника и приемника сигналов, удаленность их от границ территории организации;
- ориентация вектора распространения носителя информации в канале утечки информации и его протяженность.

Структурную модель канала целесообразно представлять в табличной форме, пространственную – в виде графа на плане помещения, здания, территории организации, прилегающих внешних участков среды. Структурная и пространственная модели не являются автономными, а взаимно дополняют друг друга.

Динамику канала утечки информации описывают функциональная и информационная модели. Функциональная модель характеризует режимы функционирования канала, интервалы времени, в течение которых возможна утечка информации, а информационная содержит характеристики информации, утечка которой возможна по рассматриваемому каналу: количество и ценность информации, пропускная способность канала, прогнозируемое качество принимаемой злоумышленником информации.

Указанные модели объединяются и увязываются между собой в рамках комплексной модели канала утечки. В ней указываются интегральные параметры канала утечки информации: источник информации и ее вид, источник сигнала, среда распространения и ее протяженность, ориентировочное место размещения приемника сигнала, информативность канала и величина угрозы безопасности информации.

Каждый вид канала содержит свой набор показателей, характеризующих источник и приемник сигналов в канале. Анализ этих показателей позволяет оценить максимальную дальность канала и возможности органов государственной и коммерческой разведки.

Так как приемник сигнала является принадлежностью злоумышленника и точное место его размещения и характеристики не известны, то моделирование канала проводится применительно к гипотетическому приемнику, в качестве которого целесообразно рассматривать приемник с параметрами, соответствующими современному уровню, и рационально выбранным местом размещения. Уважительное отношение к интеллекту и техническим возможностям противника гарантирует

Многофукциональные поисковые устройства
ST131 «ПИРАНЬЯ II», ST131N

СИГНАЛ-Т

НАЗНАЧЕНИЕ

Многофукциональные поисковые устройства **ST131 «ПИРАНЬЯ II» и ST131N** предназначены для обнаружения и определения местоположения специальных технических средств негласного получения информации, а так же выявления естественных и искусственно созданных каналов утечки информации.

КАНАЛЫ ОБНАРУЖЕНИЯ

ST 131 имеет четыре канала обнаружения перекрывающие частотный диапазон 10 Гц – 18 ГГц

РАДИО
Высокоскоростной панорамный приемник
СВЧ детектор

ПРОВОДНОЙ
Адаптер проводных линий с дифференциальным входом и разъемами RJ 45 с возможностью выбора пар.

ОПТИЧЕСКИЙ
ИК датчик с расширенным спектральным диапазоном.

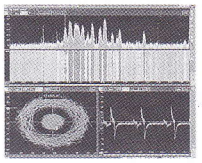
АКУСТОЭЛЕКТРИЧЕСКИЙ
Ультразвук.
Датчик магнитного поля.

ДЕТЕКТОР НЕЛИНЕЙНЫХ ПЕРЕХОДОВ В ПРОВОДНЫХ ЛИНИЯХ (только для ST131N)
Генератор контрольного сигнала

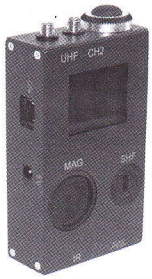
ДВА ВАРИАНТА ИСПОЛЬЗОВАНИЯ:

ПЕРЕНОСНОЙ, предназначенный для оперативного поиска

СТАЦИОНАРНЫЙ с использованием специального программного обеспечения.



Использование программы «ST 131 ANALYSER PRO» расширяет возможности ST 131 по анализу сигналов и сохранению результатов работы.



НОВОЕ

УСТРОЙСТВО ПРОВЕРКИ РАБОТОСПОСОБНОСТИ ST131.TEST

Санкт-Петербург
Ленинский пр., д. 160
+7 (812) 677 10 75

info@signal-t.ru
www.signal-t.ru

от крупных ошибок в значительно большей степени, чем пренебрежительное.

При описании приемника сигнала необходимо учитывать реальные возможности злоумышленника. Очевидно, что приемники сигналов коммерческой разведки не могут, например, размещаться на космических аппаратах.

Что касается технических характеристик средств добывания информации, то они для государственной и коммерческой разведки существенно не отличаются. Расположение приемника злоумышленника можно приблизительно определить исходя из условий обеспечения значения такого отношения сигнал/помеха на входе приемника, который необходим как для съема информации с допустимым качеством, так и безопасности злоумышленника или его аппаратуры.

Если возможное место размещения приемника сигналов выбрано, то в ходе моделирования канала рассчитывается энергетика носителя на входе приемника с учетом мощности носителя на выходе источника, затухания его в среде распространения, уровня помех, характеристик сигнала и его приемника.

Например, разрешение при фотографировании находящихся в служебном помещении людей и предметов из окна противоположного дома легко оценить по известной формуле:

$$H = hL/f,$$

где h – разрешение в долях миллиметра системы «объектив – матрица», f – фокусное расстояние телеобъектива фотоаппарата, L – расстояние от объекта наблюдения до фотоаппарата. Если фотографирование производится фотоаппаратом с $f = 300$ мм и $h = 0{,}03$ мм (разрешение 33 лин/мм), то для $L = 50$ м H равно 5 мм. Учитывая, что для обнаружения и распознавания объекта его изображение должно состоять из не менее чем 9 точек, то минимальные размеры объекта составляют 15×15 мм. Очевидно, что на фотографии можно будет рассмотреть человека, продукцию, но нельзя прочитать машинописный текст на бумаге или экране монитора.

Все выявленные потенциальные каналы утечки информации и их характеристики целесообразно отобразить в табличной форме (см. таблицу).

В графе 4 указываются основные элементы среды распространения и возможные места размещения приемника сигналов. По физической природе носителя определяется вид канала утечки информации.

Оценка показателей угроз безопасности представляет собой достаточно сложную задачу в силу перечисленных далее обстоятельств.

Добывание информации нелегальными путями не афишируется, а реальные статистические данные по видам угроз безопасности информации фактически отсутствуют или очень скудно представлены в литературе. Кроме того, следует иметь в виду, что характер и частота реализации угроз зависят от криминогенной обстановки в районе нахождения организации, и данные об угрозах, например, в странах с развитой рыночной экономикой, не могут быть однозначно использованы для российских условий.

Оценка угроз безопасности информации основывается на прогнозе действий органов разведки. Учитывая скрытность подготовки и проведения разведывательной операции, их прогноз приходится проводить в условиях острой информационной недостаточности.

Многообразие способов, вариантов и условий доступа к защищаемой информации существенно затрудняет возможность выявления и оценки угроз безопасности информации. Каналы утечки информации могут распространяться на достаточно большие расстояния и включать в качестве элементов среды распространения труднодоступные места.

Априори не известен состав, места размещения и характеристики технических средств добывания информации злоумышленника.

Оценки угроз информации в результате проникновения злоумышленника к источнику или ее утечки по техническому каналу носят вероятностный характер. При этом рассматривается вероятность $P_р$ реализуемости рассматриваемого пути или канала, а также стоимости соответствующего элемента информации $C_и$.

Угроза безопасности информации, выраженной в величине ущерба $C_{уи}$ от ее попадания к злоумышленнику, определяется для каждого пути или канала в виде

$$C_{уи} = C_и P_р.$$

Моделирование угроз безопасности информации завершается их ранжированием.

На каждый потенциальный способ проникновения злоумышленника к источнику информации и канал утечки информации целесообразно завести карточку, в которую заносятся в табличной форме характеристики моделей канала. Структурная, пространственная, функциональная и информационная модели являются приложениями к комплексной модели канала утечки.

Более удобным вариантом является представление моделей на основе машинных баз данных, математическое обеспечение которых позволяет учесть связи между разными моделями, быстро корректировать данные в них и систематизировать каналы по различным признакам, например по виду, положению в пространстве, способам и средствам для их выявления и блокирования.

Оценка условий, в которых придется решать поставленную задачу, происходит в комплексе совместно с оценкой вероятного противника

Таблица

№ элемента информации	Стоимость информации	Источник сигнала	Путь утечки информации	Вид канала	Оценки реальности канала	Величина угрозы	Ранг угрозы
1	2	3	4	5	6	7	8

и своей организации, так как невозможно качественно смоделировать процесс, отрывая его от условий, в которых он происходит. Выделение оценки условий в отдельный параграф позволяет избежать возможных упущений при комплексной оценке обстановки.

В процессе оценки условий прежде всего:

- анализируется расположение объекта на местности с учетом окружающей его территории и размещенных на ней посторонних объектов;
- оценивается контролируемая зона и возможности по снятию информации из-за ее пределов;
- обследуется сам защищаемый объект.

При непосредственном знакомстве с защищаемым объектом прежде всего:

- выясняют взаимное расположение контролируемых и смежных помещений, режимы их посещения;
- устанавливают факты и сроки ремонтных работ, монтажа и демонтажа коммуникаций, замены предметов мебели и интерьера;
- изготавливают планы помещений, на которые наносят все входящие и проходящие коммуникации;
- изучают конструктивные особенности ограждающих поверхностей, материалы покрытий.

Особое внимание в условиях плотной застройки уделяют подготовке плана прилегающей территории, которая может быть использована для парковки автомобилей с приемной радиоаппаратурой, развертывания систем видеонаблюдения или дистанционного аудиоконтроля.

Результаты проведенного анализа в конечном итоге составляют основу *«Модели вероятного противника»*.

Модель позволяет учитывать:

- типы и состав защищаемых информационных ресурсов объекта (ИР);
- значимость (стоимость) каждого из ИР;
- оперативные возможности противника;
- технические возможности противника;
- финансовые возможности противника;
- порядок эксплуатации объекта и уже реализованные меры обеспечения безопасности информации (организационные, режимные, инженерные, технические), затрудняющие или делающие невозможным съем информации по тому или иному каналу.

На основании перечисленных исходных данных модель описывает весь перечень каналов утечки, считающихся потенциально опасными.

Результат оценки обстановки в виде полученной *«Модели вероятного противника»* позволяет выявить и произвести ранжирование проблем, стоящих перед руководителем при решении вопроса о принятии решения о проведении комплексной проверки.

Ранее уже упоминалось, что в теории решений под проблемой понимается всякое различие между имеющимся и необходимым положением дел. Всякая попытка устранить это различие, естественно, связана с определенными трудностями. Различный уровень этих трудностей и обусловил наличие нескольких типов *проблем: стандартных, хорошо определенных, слабо определенных, неопределенных.*

Однако в практике управления руководитель, как правило, не задумывается о том, с каким типом проблем он имеет дело. В проблеме он прежде всего видит трудности на пути достижения поставленной цели, разрешение которых не лежит на поверхности, а требует от руководителя принятия особых мер, выходящих за пределы привычных стандартных действий. А поскольку разрешение всякой проблемы связано с необходимостью затраты определенных сил и средств, то очень важно выявить в первую очередь истинные, а не ложные проблемы, чтобы своевременно их разрешить.

Разрешить проблему – значит найти те действия, с помощью которых состояние системы (объекта) управления изменится с действительного на желаемое – являющееся целью действий. Каждая выявленная проблема должна быть четко сформулирована. Закончив выявление проблем, руководитель должен осуществить их ранжирование, то есть каждой выявленной проблеме определить место (ранг) в ряду других по важности, а значит, и степень срочности ее разрешения. При этом могут возникнуть следующие вопросы:

- какую из проблем следует считать главной;
- как разрешить противоречия между ними;
- чем поступиться, если противоречие неразрешимо?

Для определения важности выявленных проблем и места каждой из них можно воспользоваться ответом на следующий вопрос: *«Что будет, если проблема не будет решена?»* Ответ на этот вопрос позволит в полной мере оценить важность и актуальность решения той или иной проблемы. Теперь, когда руководителю стало ясно, какие проблемы и в какой последовательности необходимо решить, он уже может выбрать конкретный метод своей работы и определить, какие вопросы должен решить сам, а какие – поручить специалистам отдела (службы, фирмы). При этом определяются сроки подачи предложений по разрешению поставленных им задач.

На заключительной стадии оценки обстановки все найденные пути решения проблем обобщаются и синтезируются руководителем в возможные ***варианты решения стоящей задачи*** для достижения цели действий и затем из них выбирается наилучший, позволяющий достичь поставленной цели действий с наименьшими затратами сил, средств, и более качественно. Из анализа практических решений по защите информации можно сделать вывод, что возможных вариантов приемлемых решений в каждом случае не так уж много: максимум 4–6. При наличии нескольких вариантов задача руководителя выбрать из них такой, который при безусловном достижении поставленной цели обеспечит максимальную эффективность работ. Для этого необходимо оценить выбранные варианты и определить среди них наиболее подходящий для конкретных условий.

На практике применяются два подхода к выбору оптимального варианта:

- сравниваются несколько вариантов;
- анализируется один вариант, но он выбирается по этапам (шагам).

Однако при использовании того или другого подхода возникает необходимость сравнения вариантов или различных элементов (шагов) одного варианта для выбора из них лучшего. Для этой цели приходится использовать какие-то критерии, для чего выбираются такие показатели, которые наиболее полно характеризуют оцениваемый процесс.

При этом может использоваться несколько способов выбора оптимального варианта действий.

1 вариант: выбирается критерий, наиболее полно отражающий степень достижения цели действий, и по нему сравнивают предлагаемые варианты;

2 вариант: задаются определенные ограничения значений критериев, и варианты, не удовлетворяющие критериям с введенными ограничениями, отбрасываются, а затем из оставшихся вариантов выбирается наилучший по максимуму значений используемых критериев;

3 вариант: задается удельный вес (коэффициент значимости) каждому критерию и выбирается обобщенный критерий эффективности;

4 вариант: варианты ранжируются согласно выбранным критериям эффективности.

Решение проблемы защиты информации с точки зрения системного подхода можно сформулировать как трансформацию существующей системы в требуемую. Выбор лучшего варианта производится по максимуму обобщенного критерия как имеющего в этом случае лучшее соотношение эффективности и стоимости. Затем выбранные варианты, соответствующие наиболее рациональной организации подготовки и проведения комплексной проверки с целью выявления ЗУ, предлагаются руководству.

После рассмотрения руководством предлагаемых вариантов (лучше двух – для предоставления выбора), учета предложений и замечаний наилучший с точки зрения принимающего решения лица вариант ложится в основу ***замысла решения руководителя об организации и проведении комплексной проверки в компании*** (объектах защиты).

В данной статье были рассмотрены теоретические аспекты и методологические основы принятия управленческого решения. Практические вопросы принятия решения о подготовке и проведении комплексной специальной проверки будут рассмотрены в последующих статьях.

ЛИТЕРАТУРА

1. *Бузов Г. А., Калинин С. В., Кондратьев А. В. Защита от утечки информации по техническим каналам. – М.: Горячая линия-Телеком, 2005 – 416 с.*
2. *Бузов Г. А. Практическое руководство по выявлению специальных технических средств несанкционированного получения информации. – М.: Горячая линия-Телеком, 2010 – 240 с.*