В последнее время в связи со сложной экономической ситуацией многие руководители коммерческих структур пытаются найти способ оптимизации затрат. Большинство из них пытается уменьшить затраты, напрямую не приносящие прибыль, при этом многие считают, что защита информации – никому не нужное дело, а действия специалистов по защите информации только мешают работе сотрудников.

Геннадий БУЗОВ, заведующий кафедрой «Защиты информации от утечки по техническим каналам» учебного центра «Информзащита», кандидат военных наук, доцент

Защита информации – необходимая реальность или пустая трата сил и средств?

Таким образом, возникла острая необходимость понять, так ли это. Прежде всего определимся, о защите какой информации будет идти речь. Вопрос о защите информации является прерогативой руководителя фирмы, и, прежде чем решить, нужна защита или нет, в компании необходимо провести предварительную аналитическую работу.

Необходимо провести анализ информации, циркулирующей на предприятии, и определить, какая может иметь конфиденциальный характер. Оценить виды информации, порядок ее обработки и циркуляции. Определить, подпадает ли она под требования законодательных актов о защите информации, и если да, подпадает, то в соответствии с положениями этих актов и нормативно-методических документов определить необходимую степень защиты.

При этом если вопросы защиты определены в нормативных документах и деятельность фирмы подпадает под требования данных документов, то руководство обязано неукоснительно выполнять их. Если информация не подпадает под требование законодательных актов, то решение о необходимости защиты принимает руководитель компании. Прежде всего он должен определить:

- востребована ли продукция или услуги фирмы на рынке;
- какие потери понесет фирма, если произойдет утечка информации;
- кто из конкурентов заинтересован в получении информации о деятельности фирмы;
- у кого из конкурентов наибольшие возможности по несанкционированному получению информации о фирме.

Затем необходимо определить, по каким каналам возможна утечка интересующей конкурентов информации, и какие потери понесет фирма, если информация попадет к ним. Это и является отправной точкой для принятия решения о необходимости защиты. Если потери незначительны и не окажут серьезного влияния на деятельность фирмы, то, как говорится, не стоит и суетиться, так как реальная защита требует серьезных затрат на ее организацию и дальнейшее поддержание на необходимом уровне. А если потери значительны, то здесь возникает явная необходимость для защиты данной информации. Вопрос, каким образом можно защитить информацию с наименьшими затратами и с требуемой эффективностью, мы и рассмотрим более детально.

Эффективное противодействие обеспечивается только при комплексном использовании технических средств, организационных и технических методов в целях защиты охраняемых сведений об объекте, осуществляемых в соответствии с целями и задачами противодействия, этапами жизненного цикла объекта защиты и способами противодействия. При этом к защите информации предъявляется ряд требований, основными из которых являются своевременность, активность, разнообразность, непрерывность, рациональность, комплексность, плановость, скрытность.

Своевременность. Одним из основных требований является своевременность принятия решения на организацию защиты информации. Ускорение процесса выработки решения необходимо, во-первых, для того, чтобы своевременно решить возникшие проблемы и не давать им разрастись до такого состояния, когда решение их станет невозможным или бесполезным, во-вторых, для того чтобы подчиненные имели достаточно времени для выполнения поставленных перед ними задач.

Активность противодействия прежде всего предусматривает наступательный, активный характер противодействия, основанный на анализе складывающейся обстановки, умении сделать правильные выводы о возможных действиях потенциального противника, позволяющие упредить их и настойчиво осуществлять эффективные меры противодействия.

Разнообразие противодействия направлено на исключение шаблона в организации и проведении мероприятий и подразумевает творческий подход к его организации и осуществлению.

Комплексность предусматривает проведение комплекса мероприятий, направленных на своевременное закрытие всех возможных каналов утечки информации об объекте. Недопустимо применять отдельные технические средства или методы, направленные на защиту только некоторых из общего числа возможных каналов утечки информации.

Непрерывность противодействия предусматривает проведение мероприятий по комплексной защите объекта информатизации на всех этапах жизненного цикла разработки и существования

специальной продукции или обеспечения производственной деятельности объекта защиты.

Плановость проведения мероприятий означает предусмотренные заранее, еще на стадии проектирования и строительства объекта, мероприятия, направленные на защиту информации.

Скрытность проведения мероприятий направлена прежде всего на то, чтобы противник не смог принять контрмеры по выключению дистанционно управляемых активных средств съема информации. Поэтому важно, чтобы мероприятия по противодействию выглядели правдоподобно и отвечали условиям обстановки, выполнялись в соответствии с планами защиты информации объекта. В связи с этим разрабатываются и осуществляются практические меры по легендированию и маскировке мероприятий, направленных на защиту.

Особое внимание при проведении таких мероприятий должно обращаться на выбор замысла защиты информации объекта, замысла противодействия. Замысел защиты – общая идея и основное содержание организационных, технических мероприятий и мер, направленных на маскировку, обеспечивающих устранение или ослабление (искажение) демаскирующих признаков и закрытие технических каналов утечки охраняемых сведений.

В основе защиты информации лежит совокупность правовых форм деятельности собственника, организационных и технических мероприятий, реализуемых с целью выполнения требований по сохранению защищаемых сведений и информационных процессов, а также мероприятия по контролю эффективности принятых мер защиты информации. Необходимо отметить, что защита информации не является отдельными, разовыми эпизодами и мероприятиями, а, как указано в требованиях, предъявляемых к защите, должна вестись комплексно и непрерывно. Грамотное построение эффективной системы защиты в организации требует настойчивой и целенаправленной повседневной работы. Для создания эффективной системы защиты прежде всего необходимо определиться с пониманием слова «система» применительно к организации и осуществлению мероприятий по защите информации.

Любая система состоит из управляющего объекта и объекта управления (рис. 1) и создается под заданные требования с учетом существующих ограничений. Всякая система может нормально функционировать только при наличии в ней определенных связей между объектом управления и управляющим объектом. Обязательным для нормального функционирования системы является наличие обратной связи. В общем случае для функционирования любой системы необходимы прежде всего побудительные причины, которые могут появиться как от внешнего воздействия, так и от внутренней неудовлетворенности состоянием дел.

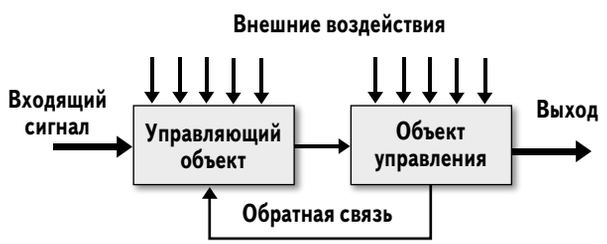

Рис. 1. Принципиальная схема системы управления с обратной связью

Рассмотрим динамику функционирования системы на уровне организации, работающей с категорированной информацией. Так как любая система создается для решения определенного рода задач, то в своем функционировании она ограничивается как объективными, так и субъективными факторами. К ним относятся:

- перечни защищаемых сведений, составляющих государственную и коммерческую тайну;
- требуемые уровни безопасности информации;
- актуальные угрозы безопасности информации;
- показатели, по которым будет оцениваться эффективность системы защиты.

Входами системы инженерно-технической защиты информации являются:

- воздействия злоумышленников при физическом проникновении к источникам информации конфиденциального характера с целью ее хищения, изменения или уничтожения;
- различные физические поля, электрические сигналы, создаваемые техническими средствами злоумышленников, которые воздействуют на средства обработки и хранения информации;
- стихийные силы, прежде всего пожары, приводящие к уничтожению или изменению информации;
- физические поля и электрические сигналы с информацией, передаваемой по функциональным каналам связи;
- побочные электромагнитные и акустические поля, а также электрические сигналы, возникающие в процессе деятельности объектов защиты и несущие информацию конфиденциального характера.

Выходами системы защиты являются меры по защите информации, адекватные входным воздействиям. Алгоритм процесса преобразования входных воздействий (угроз) в меры защиты и определяет вариант системы защиты.

Общая цель системы защиты – обеспечение требуемого уровня безопасности информации на фирме, в организации, на предприятии (в общем случае – на объекте защиты). Частные цели конкретизируют задачи применительно к видам и категориям защищаемой информации, а также элементам объекта защиты и отвечают на вопрос, что надо сделать для достижения целей. Кроме того, уровень защиты нельзя рассматривать в качестве абсолютной меры безотносительно ущерба, который может возникнуть от потери информации и использования ее злоумышленником во вред владельцу информации.

В качестве критериев при выборе рационального варианта для оценки требуемого уровня защиты целесообразно выбрать соотношение между ценой защищаемой информации и затратами на ее защиту. Уровень защиты рационален, когда обеспечивается требуемая степень безопасности информации и минимизируются расходы на ее защиту. Эти расходы $C_{ри}$ складываются из:

- затрат на защиту информации $C_{зи}$;
- ущерба $C_{уи}$ за счет попадания информации к злоумышленнику и использования ее во вред владельцу.

Между этими слагаемыми существует достаточно сложная связь, так как ущерб из-за недостаточной безопасности информации уменьшается с увеличением расходов на ее защиту. Если первое слагаемое может быть точно определено, то оценка ущерба в условиях скрытности разведки и неопределенности прогноза использования злоумышленником полученной информации представляет достаточно сложную задачу. Ориентировочная оценка ущерба возможна при следующих допущениях.

Владелец информации ожидает получить от ее материализации определенную прибыль, которой он может лишиться в случае попадания ее конкуренту. Кроме того, последний, используя информацию, может нанести владельцу еще дополнительный ущерб за счет, например, изменения тактики продажи или покупки ценных бумаг и т. д. Дополнительные неблагоприятные факторы чрезвычайно трудно поддаются учету. Поэтому в качестве граничной меры для оценки ущерба можно использовать величину потенциальной прибыли $C_{пп}$, которую ожидает получить от информации ее владелец, т. е.

$$C_{уи} \geq C_{пп}.$$

В свою очередь, величина ущерба зависит от уровня защиты, который определяется расходами на нее. Максимальный ущерб возможен при нулевых расходах на защиту, гипотетический нулевой ущерб обеспечивается при идеальной защите. Но идеальная защита

требует бесконечно больших затрат. При увеличении расходов на защиту вероятность попадания информации злоумышленнику, а, следовательно, и ущерб уменьшаются. При этом рост суммарных расходов на информацию с увеличением затрат на ее защиту будет в период создания или модернизации системы, когда происходит накопление мер и средств защиты, которые еще не оказывают существенного влияния на безопасность информации. Например, предотвращение утечки информации по отдельным каналам без снижения вероятности утечки по всем остальным не приводит к заметному повышению безопасности информации, хотя затраты на закрытие отдельных каналов могут быть весьма существенными. Образно говоря, для объекта защиты существует определенная «критическая масса» затрат на защиту информации, при превышении которой эти затраты обеспечивают эффективную отдачу.

При некоторых рациональных затратах на защиту информации выше критических наблюдается оптимум суммарных расходов на защиту. При затратах ниже рациональных увеличивается потенциальный ущерб за счет повышения вероятности попадания информации конфиденциального характера к злоумышленнику, при более высоких затратах – увеличиваются прямые расходы на защиту.

Ограничения системы представляют собой выделяемые на защиту информации людские, материальные и финансовые ресурсы, а также ограничения в виде требований к системе. Суммарные ресурсы удобно выражать в денежном эквиваленте. Независимо от выделяемых на защиту информации ресурсов они не должны превышать суммарной цены защищаемой информации. Это верхний порог ресурсов.

Ограничения в виде требований к системе предусматривают принятие таких мер по защите информации, которые не снижают эффективность функционирования системы при их выполнении. Например, можно настолько ужесточить организационные меры управления доступом к источникам информации, что наряду со снижением возможности ее хищения или утечки ухудшатся условия выполнения сотрудниками своих функциональных обязанностей.

При оценке вариантов защиты информации наиболее целесообразно использовать тот, когда задается удельный вес (коэффициент значимости) каждому критерию и выбирается обобщенный критерий эффективности. В качестве этого критерия может быть использован обобщенный критерий в виде отношения эффективность/стоимость, учитывающий основные характеристики системы, или представлять собой набор частных показателей. В качестве частных показателей критерия эффективности системы защиты информации используются в основном те же, что и при оценке эффективности разведки. Это возможно потому, что цели и задачи, а, следовательно, значения показателей эффективности разведки и защиты информации близки по содержанию, но противоположны по результатам. То, что хорошо для безопасности информации, плохо для ее съема, и наоборот.

Частными показателями эффективности системы защиты информации являются:

- вероятность обнаружения и распознавания злоумышленниками объектов защиты;
- качество (разборчивость) речи на выходе приемника злоумышленника;
- достоверность (вероятность ошибки) дискретного элемента информации (буквы, цифры, элемента изображения).

Очевидно, что система защиты тем эффективнее, чем меньше вероятность обнаружения и распознавания объекта защиты злоумышленником, чем ниже точность измерения им признаков объектов защиты, разборчивость речи, выше вероятность ошибки приема злоумышленником дискретных сообщений. Однако при сравнении вариантов построения системы по нескольким частным показателям возникают проблемы, обусловленные возможным противоположным характером изменения значений разных показателей: одни показатели эффективности одного варианта могут превышать значения аналогичных показателей второго варианта, другие, наоборот, – имеют меньшие значения. Кроме того, важным показателем системы защиты являются затраты на обеспечение требуемых значений оперативных показателей. Поэтому результаты оценки эффективности защиты по совокупности частных показателей, как правило, неоднозначные.

Для выбора рационального (обеспечивающего достижение целей, решающего поставленные задачи при полном наборе входных воздействий с учетом ограничений) варианта путем сравнения показателей нескольких вариантов используется обобщенный критерий в виде отношения эффективность/стоимость. Под эффективностью понимается степень выполнения системой задач, под стоимостью – затраты на защиту. В качестве критерия эффективности $K_э$ применяются различные композиции частных показателей, чаще их «взвешенная» сумма:

$$K_э = \Sigma \alpha_j K_j,$$

где α_j – «вес» частного показателя эффективности K_j.

«Вес» частного показателя определяется экспертами (руководством, специалистами организации, сотрудниками службы безопасности) в зависимости от характера защищаемой информации. Если защищается в основном семантическая информация, то больший «вес» имеют показатели оценки разборчивости речи и вероятности ошибки приема дискретных сообщений. В случае защиты объектов наблюдения выше «вес» показателей, характеризующих вероятности обнаружения и распознавания этих объектов.

Для оценки эффективности системы защиты информации по указанной формуле частные показатели должны иметь одинаковую направленность влияния на эффективность, при увеличении их значений повышается значение эффективности. С учетом этого требования в качестве меры обнаружения и распознавания объекта надо использовать вероятность необнаружения и нераспознания, а вместо меры качества подслушиваемой речи – ее неразборчивость. Остальные частные показатели соответствуют приведенным выше.

Выбор лучшего варианта производится по максимуму обобщенного критерия, так как он имеет в этом случае лучшее соотношение эффективности и стоимости. Затем выбранные варианты, которые соответствуют наиболее рациональному построению и организации защиты, предлагаются руководству. Руководитель, оценив наиболее опасные угрозы для информации, утечка которой может привести к наибольшим потерям, и стоимость защиты, может обоснованно принять решение о необходимости защиты и о том, на что необходимо обратить особое внимание в тот или иной период деятельности фирмы.