Глава 4. Основные направления безопасности предпринимательской деятельности

4.1. Экономическая безопасность

Девяностые годы прошлого столетия показали, что силовые методы в российской экономике стали постоянным и необходимым элементом хозяйственной жизни. За последние пятнадцать лет сформировались и активно продолжают развиваться профессиональные силовые структуры, как государственные так и негосударственные. Они активно ищут свои ниши в бизнесе, что красноречиво свидетельствует о действии в этом секторе экономики закона спроса и предложения[1].

Процесс этот связан с тем, что для российского предпринимателя «экономическая безопасность» из абстрактно-теоретического понятия превратилась в реально востребованную и крайне необходимую постоянно действующую систему мероприятий по обеспечению экономической безопасности его фирмы.

В начале 1990-х гг. большинство российских предпринимателей понимало экономическую безопасность фирмы как физическую безопасность руководителей и их родных и решало данную проблему по принципу: чем больше «мордоворотов», тем выше безопасность. Однако последующие годы убедительно показали, что даже охрана, набранная из бывших сотрудников знаменитого 9-го Управления КГБ СССР, не обеспечивает не только всего комплекса личной безопасности (уникальность «девятки» и ее высочайшая эффективность базировались на том, что на нее работали, снабжали необходимой информацией все другие оперативные подразделения КГБ – разведка и контрразведка), но даже и безопасности бизнеса. Такая ситуация потребовала скорейшего решения двух взаимосвязанных проблем.

Во-первых, привлечения специалистов, так как только профессионалы – оперативники, агентуристы, аналитики, «наружники» (бывшие сотрудники спецслужб и правоохранительных органов) – в состоянии эффективно решить задачи обеспечения экономической безопасности. Так, в России (1997 г.) в 10,5 тыс. зарегистрированных охранных предприятиях и службах безопасности работало 148,5 тыс. лицензированных сотрудников, из которых приблизительно 35 тыс. – бывшие сотрудники МВД, почти 15 тыс. – бывшие сотрудники

[1] Число охранно-сыскных структур с 1993 по 1999 г. выросло в 2,4 раза (с 4540 до 10804), в том числе частных охранных – в 4,8 раза (с 1237 до 5995) и служб безопасности – в 1,9 раза (с 2356 до 4580). В частных охранных фирмах России работает более 600.000 личных охранников для защиты VIP-персон. Чтобы оплатить их услуги, затрачиваются фантастические суммы, около 450 миллиардов рублей в год. В России используется самое большое количество в мире бронированных лимузинов стоимостью от 10 млн. руб. и выше. Криминал на прослушивании мобильных телефонов получает ежегодно прибыль около 25 миллиарда руб. По числу заказных убийств Россия занимает первое место в мире. Объем продаж различного рода жучков, подслушивающих и подглядывающих систем составляет ежегодно несколько сотен миллионов долларов США.

органов госбезопасности, около 1,5 тыс. – с опытом работы в прокуратуре, судах и в других правоохранительных органах.

Во-вторых, создания собственных служб безопасности, поскольку, как показывает мировой и российский опыт, наиболее защищенными являются те структуры, которые имеют собственные службы безопасности. Начинается стремительный рост зарегистрированных служб безопасности – с 2356 (1993 г.) до 5287 (1994 г.); с 1993 по 1997 гг. число зарегистрированных служб безопасности значительно превышало количество частных охранных предприятий (ЧОП). Необходимо отметить, что «колебания» в количестве служб безопасности в нашей стране связаны со следующим фактором: поскольку службы безопасности существуют за счет прибыли компании, то они в большей степени, чем ЧОП, подвержены экономическим ударам (последний пример – август 1998 г.). Кроме того, финансовые пирамиды, «мыльные» банки и другие подобные структуры имели службы безопасности, которые ликвидировались вместе с компаний.

Суть деятельности по обеспечению безопасности фирмы на практике сводится к прогнозированию угроз и определению мер по их локализации. В настоящее время в России для любой хозяйственной структуры основными угрозами во внешней среде являются криминал, конкуренты и государство, во внутренней – персонал. Поэтому основными направлениями работы службы безопасности являются следующие:

изучение криминальных аспектов рынка, состояния и влияния теневой экономики на рынок;

установление обстоятельств недобросовестной конкуренции со стороны других фирм;

рассмотрение фактов неправомерного использования товарных (фирменных) знаков компании;

расследование фактов разглашения коммерческой тайны фирмы;

сбор информации о лицах, заключивших с компанией контракты;

постоянная работа с использованием некоторых средств и методов оперативной деятельности со следующими группами персонала – сотрудниками, родственники которых работают у конкурентов, ранее судимыми, уволившимися с фирмы, работниками службы безопасности, вспомогательным персоналом, имеющим доступ к коммерческой тайне;

выявление некредитоспособных и ненадежных деловых партнеров;

предоставление руководству фирмы необходимой информации при проведении деловых переговоров;

обеспечение необходимого уровня безопасности в местах проведения фирмой конфиденциальных, представительских и массовых мероприятий;

консультирование и предоставление рекомендаций руководству и персоналу фирмы по вопросам обеспечения безопасности.

Понимая сложности кадрового состава коммерческих организаций и невозможность обеспечения всего комплекса работ по обеспечению безопасности, для эффективной работы по этим направлениям в структуре службы безопасности руководством фирмы должны быть созданы

*разведывательное и контрразведывательное подразделения. Если раньше большинство российских предприни*мателей считало, что бывшие сотрудники спецслужб переносят стереотипы государственной службы в рыночную систему, где эти структуры не нужны, то в настоящее время наученные собственным опытом те же руководители компаний, которые сумели сохранить и развить этот бизнес, осознали, что это не плод фантазии бывших чекистов, а необходимое и обязательное условие минимизации предпринимательских рисков.

Разведка и контрразведка – антиподы. Однако шпионаж в сравнении со своим противником, контршпионажем (контрразведкой), обладает тем преимуществом, что он – сторона нападающая и в силу этого пользуется фактором внезапности, определяет место действия, характер своих операций, их исполнителей. Как говорится, у волка сто дорог, у охотника – только одна.

Существующие условия развития бизнеса заставляют использовать накопленный опыт в этих направлениях и совершенствовать защиту операторской деятельности исходя из новых требований.

В настоящее время в России используются следующие названия разведывательной деятельности службы безопасности – экономическая разведка, деловая разведка, бизнес-разведка и конкурентная разведка. Хотя они имеют некоторые различия и особенности, можно считать их синонимами.

Возможны различные варианты существования так называемого разведывательного подразделения:

включается в состав службы безопасности;

не включается в состав службы безопасности и работает в структуре отдела экономического анализа, маркетинговых исследований или даже в отделе по связям с общественностью;

не входит в структуру компании, а является «самостоятельной» информационной или юридической фирмой, оказывающей услуги компании на коммерческой основе.

Независимо от названия и нахождения экономическая разведка должна работать по трем направлениям:

первое – сбор информации, наблюдение за конкурентами, что дает возможность своевременно раскрыть планы конкурентов по захвату лидерства или совершению других опасных для фирмы действий.

второе – поиск путей развития, позволяющих компании получить существенные преимущества над своими конкурентами.

третье – разработка принципиально новых подходов к ведению бизнеса, которые открывают фирме пути к захвату лидерства в отрасли.

В настоящее время *экономическая разведка – одна из базовых функций современного менеджмента*. Поэтому есть особенности, как в кадровом составе данного подразделения, так и в его взаимодействии с другими структурами фирмы. Современная бизнес-разведка – это не только оперативная и аналитическая работа, но и аудит, финансы, бухгалтерия, информационные технологии и многое другое. Ни одно из подразделений, обеспечивающих экономическую безопасность фирмы, не имеет таких постоянных контактов с

экономическими, финансовыми, юридическими структурами фирмы. Экономическая разведка не только участвует в разработке экономической стратегии предприятия, но непосредственно способствует ее реализации. Поэтому если в контрразведывательном подразделении все сотрудники должны иметь опыт оперативно-розыскной деятельности, то в разведке, как показывает российская практика, достаточно 30 % профессионалов, а остальные могут быть специалистами в области экономики, финансов, бухгалтерии, аудита, права.

Необходимо отметить, что пока руководители фирмы не осознают, что экономическая разведка есть необходимое условие эффективного управления предприятием в современных условиях и важный рычаг для достижения победы в конкурентной борьбе, вообще нет смысла организовывать разведывательное подразделение.

Как показала российская действительность, если экономической разведке в этой ситуации не выделить необходимых ресурсов (по оценкам специалистов, на разведку следует тратить 1,5 % от оборота фирмы), она окажется недостаточно осведомленной относительно актуальных, но еще не вполне осознанных проблем, стоящих перед фирмой; она сможет решать только второстепенные задачи. В итоге, представляемые разведкой материалы окажутся неактуальными, то есть ее влияние на деятельность фирмы будет ничтожным.

В настоящее время можно выделить следующие «болевые точки» безопасности бизнеса, которые эффективно могут решить только собственные СБ (службы безопасности). Первое направление – противодействие экономическому шпионажу, масштабы которого постоянно растут. По оценкам ФСБ России, каждая вторая российская фирма занимается промышленным шпионажем, а конкуренты занимаются против нее тем же самым (речь не идет о «пивных ларьках»). По экспертным оценкам, на долю экономического шпионажа приходится 60 % потерь от недобросовестной конкуренции.

По имеющимся данным, из фактов, которые стали достоянием гласности в Санкт-Петербурге и которые попадают под формулировку «промышленный шпионаж»[1], около 20 % – это профессионально проведенные мероприятия, преследующие чисто экономические цели, оставшиеся 80 % – это либо еще недостаточно профессиональные действия конкурентов, либо действия криминала.

Специалисты считают, что в России завершается третий этап развития промышленного шпионажа. Каждый предыдущий этап сопровождался появлением более квалифицированных кадров и более совершенной спецтехники, что позволяло более профессионально проводить подобные операции. В России еще, к счастью, экономический шпионаж не стал пока самостоятельным видом предпринимательства. Хотя в нашей стране уже функционируют отдельные компании, специализирующиеся на экономической

[1] Поскольку в УК отсутствует статья, предусматривающая наказание за подобные действия, то российские фирмы не всегда обнародуют подобные факты.

разведке и контрразведке с использованием самой современной техники. Видимо, в ближайшее время, учитывая темпы и масштабы роста промышленного шпионажа, и у нас появятся аналоги американской «Джордж Уоккенхам корпорейшн» со штатом около 20 тыс. сотрудников.

Сегодня основными направлениями экономического шпионажа являются: перехват выгодных контрактов и инвестиционных проектов, перехват поставщиков и каналов сбыта, программы расширения и НИОКР. Кроме того, необходимо помнить, что российские компании пока еще не потеряли своей привлекательности для зарубежных государственных и корпоративных служб безопасности.

Следует отметить, что ни одно из направлений обеспечения экономической безопасности российского бизнеса не получило такого фундаментального освещения в специальной литературе, как промышленный шпионаж. Так, в 1997 г. в Москве был издан двухтомник «Р-система: введение в экономический шпионаж. Практикум по экономической разведке в современном российском предпринимательстве». На 970 страницах авторы достаточно оригинально реализуют цель работы, которую они сформулировали следующим образом: «Наша цель – сдать карты для игры на равных – научить оперативной работе всех, кому мы не по карману» (имеется в виду невозможность оплаты услуг профессионалов). Однако, как свидетельствует наш опыт, в природе не существует людей, которые способны научиться оперативной работе по книге. Тем не менее, как наглядно показала российская действительность, определенная часть наших предпринимателей страдает жадностью и невежеством, поэтому они жалеют средства на обеспечение безопасности и не понимают сути комплексной системы защиты, то есть не учитывают тот факт, что обеспечить разработку и функционирование системы безопасности способны лишь профессионалы.

Второе направление – это ведение деловой разведки по настоящим и предполагаемым партнерам, клиентам, заказчикам.

Как известно, «национальными особенностями» российского бизнеса стали обман, мошенничество, невыполнение условий договора. Поэтому проведение проверки должно стать необходимым и обязательным условием для российских фирм. В настоящее время возможны три варианта подобной проверки: силами собственных служб безопасности, с помощью специализированных российских и зарубежных информационных фирм и используя дружественные связи руководителя службы безопасности в государственных структурах (МВД, РУБОП, ФСБ). На практике чаще всего встречается сочетание всех трех. Кроме того, большинство сотрудников петербургских (как и московских) компаний, предоставляющих информационные услуги, составляют профи из КГБ – ФСБ, которые достаточно быстро научились говорить с «абсурдным» российским бизнесом на понятном ему языке и с которыми проще иметь дело руководителям службы безопасности, так как они, нередко, тоже выходцы из той же системы. Наконец, только настоящий «опер» сможет при обращении к информационной компании так все организовать, что не будет понятно, что же на самом деле его

интересует. Не надо объяснять, что основная часть руководителей и подавляющее большинство сотрудников частных охранных структур не в состоянии заниматься деловой разведкой.

Третье направление – это отслеживание ситуации с ценными бумагами компании (акциями, облигациями, векселями), с кредитами (льготные условия предоставления, альтернативные предложения кредитора по их погашению и т. д.), со своевременным выполнением своих обязательств перед компаниями, которые могут быть «пятой колонной» конкурентов. Это направление деятельности службы безопасности достаточно новое, и, как показывает практика Санкт-Петербурга, службы безопасности еще не всегда готовы к подобной деятельности. Часто в качестве примера приводится перехват управления всемирно известной компанией находящейся в Петродворце: на достаточно льготных условиях банк предоставил компании кредит, а когда компания не смогла его вернуть вовремя, банк в качестве возможного погашения долга предложил передачу пакета акций. В результате этого маневра четыре места из семи в Совете директоров компании оказались за банком. Целенаправленная деятельность новых членов совета директоров привела компанию на грань банкротства. И тогда банк продал все свои кредиторские претензии к компании некой фирме. Как выяснилось, банк контролировался структурами, которые были собственниками одного из основных конкурентов Петербургской компании.

С большой степенью достоверности можно прогнозировать, что скупка пакетов акций (блокирующего и контрольного) с помощью неизвестных организаций из оффшорных зон, изменения в базе этих владельцев и руководителей компании, целенаправленное доведение ее до банкротства и приход внешнего управляющего с дальнейшей продажей компании за бесценок конкурентам – все это становится постоянной угрозой для многих российских АО и потребует изменений в работе служб безопасности.

4.2. Враждебные слияния и поглощения

Мировой рынок трансграничных и национальных слияний и поглощений в последние годы развивается очень активно, так как количество и объем сделок слияний и поглощений значительно возросли. Россия здесь играет не последнюю роль. Так, среди крупнейших слияний и приобретений в 2003 г. специалисты выделяют следующие: ТНК (Россия) и BP PLC (Великобритания), Оренбургнефть (Россия) и ТНК (Россия), Лензолото (Россия) и Норильский никель (Россия), Rouge Industries (США) и Северсталь (Россия) и др. (отчет компании Ernst & Young о рынке слияний и приобретений в России от 24 марта 2004 г.)[1].

[1] Заикин В., Калашников Г. Механизмы и защиты компаний // Управление компанией. – № 7. – 2004.

Всплеск слияний и поглощений, прошедший в России 5 лет назад говорит о том, что Россия наравне с США, Японией и Европой становится равноценным игроком на рынке корпоративных слияний и поглощений.

Мировая практика показывает, что в большинстве случаев слияния и поглощения проводятся по взаимному согласию высшего управленческого персонала обеих компаний. Однако нередка и практика враждебных слияний и поглощений, когда компанией или ее активом устанавливается полный контроль как в юридическом, так и в физическом смысле вопреки воле менеджмента и/или собственника (собственников) этой компании или активов[1].

Недружественное поглощение (захват) – это нечто среднее между чисто силовой акцией и юридической процедурой и осуществляется, как правило, хоть и на минимальных, но правовых основах. Недружественные поглощения и корпоративные захваты[2] являются на сегодняшний день объективной реальностью взаимоотношений участников предпринимательской деятельности. С этим явлением приходится сталкиваться практически всем предпринимателям. Бесспорен также тот факт, что инициирование корпоративного спора и организация корпоративного захвата к настоящему времени стали самостоятельными видами деятельности, целью которой является изъятие имущества и имущественных прав как у компании, так и у отдельных участников обществ.

Основная сфера интересов рейдеров[3] – недооцененная или проблемная компания, располагающая избыточным (эффективно используемым) имущественным комплексом. В качестве рейдеров наиболее часто встречаются следующие субъекты:

- финансово-промышленные группы, поглощающие в целях развития или диверсификации существующих бизнес-империй или создания новых отраслевых холдингов;
- инвестиционные компании, сделавшие поглощения своим основным бизнесом, поглощение компании и/или их активы могут быть оставлены для диверсификации собственного бизнеса или проданы заинтересованным лицам;
- инвестиционные компании-посредники, действующие в интересах захватчиков;
- инвестиционные компании – профессиональные грин-мэйлеры.

Часто рейдеры позиционируют себя как агентства недвижимости, управляющие или инвестиционные компании. Компания берет в управление объект, а потом пытается захватить его в собственность. В качестве примера можно привести укрепляющие компании «Сектор». В начале 2005 г. «Сектор» посягнул на двухэтажный имущественный комплекс, который передан ему в

---

[1] Рудык Н.Б., Семенкова Е.В. Рынок корпоративного контроля: слияния, жесткие поглощения и выкупы долговым финансированием. – М.: Финансы и статистика, 2000.

[2] Корпоративное плутовство: анатомия проблемы / Шалапугин А. // Управление компанией. – № 6. – 2006.

[3] *Raider* (англ.) – налетчик. Этим словом также называют средний крейсер. В бизнесе – компанию или специалиста по перехвату управления предприятием (имущественным комплексом).

доверительное управление. В настоящее время дело находится в арбитражном суде.

Любая рейдерская операция начинается с разведки. Уточняется все: от влияния и боеспособности собственников до юридической чистоты объекта. Если анализ информации показывает, что недружественное поглощение возможно, начинается реализация апробированных схем. В акционерных обществах, созданных в процессе приватизации, не всегда налажен учет объектов недвижимости, что облегчает рейдерам захват имущественного комплекса.

Излюбленная мишень рейдеров – бывшие НИИ, преобразованные в АО. Во-первых, они обладают солидным имуществом. Во-вторых, акционирование многих организаций происходило с правовыми неточностями.

Например, в документации одного ОАО фигурировал гараж с хозяйственной пристройкой. Как оказалось, «пристройка» представляла собой капитальное пятиэтажное здание.

Очень часто рейдеры покупают руководителей организаций, чтобы они действовали в их интересах. Это может быть обременение компании долгами, в результате чего накладывается арест на недвижимость и счета предприятия, в результате, имущественный комплекс переходит в собственность кредитора-рейдера.

После достижения цели рейдеры начинают продавать имущество и «заметать следы». Поглощенная недвижимость проходит цепь сделок купли-продажи с участием трех-четырех лиц. Добросовестным приобретателем является лишь последний покупатель. Остальные – фирмы-однодневки или оффшорные компании.

После совершения сделки фирмы-однодневки за бесценок продают первому попавшемуся лицу, при этом привлечь его к ответственности или заставить выплатить налоги практически невозможно. Зато в суде присутствует добросовестный приобретатель. Но жертве рейдера от этого не легче, поскольку изъять имущество у такого покупателя чрезвычайно сложно. Как правило, к ответственности не удается привлечь ни самих рейдеров, ни подкупленных ими руководителей организации.

Для этого пострадавшая сторона должна иметь веские доказательства, но, как правило, их не удается предоставить. Участники захвата никогда не признаются в сговоре. А некомпетентность директора, из-за которой пострадала организация не повод для привлечения к уголовной ответственности.

Еще один действенный метод рейдеров – завладение контрольным пакетом акций. Акции скупаются небольшими долями на физических лиц.

Типичные методы действия рейдеров заключаются в создании системы двойного менеджмента и «параллельных» советов директоров, применении силовых методов на основании определений различных судов (желательно – максимально удаленных от места событий), оспаривании итогов приватизации по искам акционеров, создании двойного реестра и списании акций со счетов законных владельцев с их последующей продажей добросовестным

приобретателям. Эффективны «каскадные атаки», когда проблемы защищающихся все время меняются, мешая создать эффективную защиту: за «акционерным» каскадом следует «арбитражный», затем «уголовный», «надзорный», «информационный» (с привлечением СМИ), «регистрационный», «имущественный». Есть даже «каскад надежды», когда вдруг возникшие доброхоты предлагают жертве купить у нее обреченное предприятие (хотя и существенно дешевле) или провести переговоры с захватчиками.

Обязательные элементы рейдерской тактики: привлечение властного ресурса (включая судебный), фальсификация документов (почти всегда), скорость проведения операций. Рейдер действует быстро. Если не получается, с каждым днем затея становится все менее выгодной. Неудавшиеся захваты переходят в разряд вялотекущих корпоративных конфликтов и тогда уже попадают в прессу.

Проблема серьезная, и законными методами с рейдерами бороться сложно: они стараются избегать прямых (доказуемых) нарушений норм права. Этим занимаются высококлассные специалисты, ими отработаны специальные процедуры и технологии. Рейдерский захват – мероприятие очень выгодное и, по оценке специалистов, составляет 10-20 % реальной стоимости имущественного комплекса. За последние годы отработаны технологии, процесс поставлен на поток. Захватывается все: от небольших компаний до огромных холдингов. Круг интересов профессиональных рейдеров постоянно расширяется. Меняются способы, стратегия и регионы действий компании-агрессора.

Среди основных тенденций в сфере рейдерства[1] можно выделить следующие:

- смещение активности из Московского и Петербургского регионов России из-за дефицита «свободных объектов для захвата». Как известно, цель любого захвата – завладение недвижимым имуществом организации либо самим бизнесом. В регионах рейдеров привлекает именно бизнес, поскольку объекты недвижимости не представляют большого интереса, в то время как в столице больший интерес вызывают именно активы поглощаемых компаний;
- установление контроля над акциями (долями) перестает быть доминирующим способом недружественного поглощения компаний. На первый план выходит фальсификация документов, например подделка реестров акционеров, протоколов общего собрания акционеров;
- разделение рейдерских компаний на две группы: первая использует преимущественно законные способы перехвата управления компанией, а вторая специализируется на криминальных способах захвата;
- проведение псевдорейдерских атак, когда компания-агрессор имитирует попытку захвата с целью дестабилизации деятельности компании-цели. Последняя в такой ситуации часто идет на уступки в переговорах о продаже бизнеса.

[1] Анализ антирейдерского законодательства / Пушкин А. // Управление компанией. – № 1. – 2007.

Рейдерство наносит ущерб не только отдельным компаниям, но и экономике России в целом. Непрозрачность бизнеса, дискредитация судебной системы являются негативными факторами в глазах иностранных инвесторов. Их осторожность понятна, ведь и их компании становятся объектом рейдерских атак. Использование государства, его административных и судебных ресурсов в качестве прикрытия для проведения захватов таит в себе и общественную опасность, так как не только наносит ущерб экономике государства, но и дискредитирует его.

Борьба с недружественными поглощениями осложняется из-за отсутствия эффективных механизмов защиты компании от вторжения рейдеров, которые активно используют нормы корпоративного и процессуального права а также мощный административный и судебный ресурс для проведения захвата. Рост недружественных поглощений вынуждает государственные структуры разрабатывать и принимать *законы и иные правовые акты, направленные на снижение активности корпоративных конфликтов.*

В 2006 г. принят Федеральный закон «О внесении изменений в Федеральный закон "Об акционерных обществах» и некоторые другие законодательные акты Российской Федерации», который существенно изменил правовое регулирование поглощения акционерного общества путем приобретения его акций. В закон включена новая глава, посвященная порядку приобретения крупного пакета акций. В частности, регламентируется процедура направления добровольного, обязательного и конкурирующего предложения при приобретении более 30 % акций открытого акционерного общества. Также определен порядок выкупа оставшихся акций при приобретении 95 % его акций. Кроме того, законом предусматривается установление государственного контроля за приобретением акций, ответственность органов управления общества за убытки, причиненные их действиями, порядок раскрытия информации при подаче предложений о выкупе акций общества. Новый механизм приобретения крупного пакета акций должен, по мнению законодателя, повысить прозрачность процедуры приобретения акций любыми лицами, сделать процесс слияний и поглощений более цивилизованным.

Помимо указанного закона стоит назвать несколько постановлений Пленума ВАС РФ. Поскольку суды часто используются в качестве инструмента захвата, Пленум ВАС РФ вынужден постоянно давать разъяснения по применению арбитражно-процессуального законодательства. Один из последних документов ВАС РФ, посвященных данной проблеме, – Постановление Пленума ВАС РФ от 12.10.2006 г. № 54 «О некоторых вопросах подсудности дел по искам о правах на недвижимое имущество», направленное на борьбу с инициированием рейдерами дел, связанных с недвижимостью, в удобных для себя судах.

В соответствии со ст. 38 ч. 1 АПК РФ иски о правах на недвижимое имущество предъявляются в арбитражный суд по месту нахождения данного имущества. Однако на практике это общее правило нередко обходится. Поэтому Пленум ВАС в своем постановлении недвусмысленно указал, что

любые дела по спорной недвижимости рассматриваются арбитражными судами исключительно по месту ее нахождения.

В постановлении приводится перечень исков о правах на недвижимое имущество с целью исключить принятие их судами не по месту нахождения имущества. К таким искам отнесены: иски об истребовании имущества из чужого незаконного владения; об устранении нарушений права, не связанных с лишением владения; об установлении сервитута; о разделе имущества, находящегося в общей собственности; о признании права; об установлении границ земельного участка; об освобождении имущества от ареста. По месту нахождения недвижимого имущества также рассматриваются дела, в которых удовлетворение заявленного требования и его принудительное исполнение повлечет необходимость государственной регистрации возникновения, ограничения (обременения), перехода, прекращения прав на недвижимое имущество или внесения записи в Единый государственный реестр прав в отношении сделок, подлежащих государственной регистрации. Если арбитражный суд установил, что дело неподсудно данной судебной инстанции, то исковое заявление возвращается на основании п. 1 ст. 129 ч. 1 АПК РФ.

Не менее важным стало принятие Пленумом ВАС РФ Постановления от 12.10.2006 г. № 55 «О применении арбитражными судами обеспечительных мер», ограничивающего категории дел, в рамках которых могут приниматься обеспечительные меры, только имущественными спорами. В Постановлении подчеркивается, что обеспечительные меры допускаются на любой стадии арбитражного процесса, в том числе в период приостановления производства по делу. В этот период лица, участвующие в деле, вправе обратиться с ходатайством об отмене обеспечительных мер, замене одной обеспечительной меры другой, истребовании встречного обеспечения.

Заявление об обеспечении иска рассматривается арбитражным судом в день поступления или не позднее, чем на следующий день после его поступления в арбитражный суд. В соответствии с п. 5 ст. 92 ч. 2 АПК РФ заявитель должен обосновать причины обращения с требованием о применении обеспечительных мер. При этом необходимо представление заявителем доказательств наличия оспоренного или нарушенного права, а также его нарушения. В решении о применении обеспечительных мер либо об отказе в их применении арбитражный суд должен дать оценку обоснованности доводов заявителя о необходимости принятия таких мер. В частности, суд учитывает разумность и обоснованность требования заявителя о применении обеспечительных мер, вероятность причинения заявителю значительного ущерба в случае непринятия таковых, обеспечение баланса интересов заинтересованных сторон, предотвращение нарушения публичных интересов и интересов третьих лиц при принятии обеспечительных мер. Кроме того, рассматривая заявление, суд оценивает, насколько истребуемая заявителем конкретная обеспечительная мера связана с предметом заявленного требования, соразмерна ему и каким образом она обеспечит фактическую реализацию поставленных целей.

Самостоятельным основанием применения обеспечительных мер (в отсутствие прочих оснований) не может служить предоставление заявителем

встречного обеспечения, например банковской гарантии. Обеспечительные меры, применяемые арбитражным судом, и суммы встречного обеспечения должны быть соразмерны имущественным требованиям, в обеспечение которых они применяются.

Однако несколькими законами и постановлениями проблему недружественных захватов полностью не решить. Поэтому следующим шагом стала *разработка поправок к корпоративному законодательству* в соответствии с одобренной Правительством РФ Концепцией развития корпоративного законодательства на период до 2008 г. Она была разработана Минэкономразвития России в 2004-2005 гг.

В настоящее время в Государственной Думе подготовлены поправки в законы «Об акционерных обществах» и «Обществах с ограниченной ответственностью», направленные на противодействие рейдерским атакам, в частности касающиеся процедуры смены руководителя общества[1].

Нововведения предусматривают:

- в обществах с числом акционеров 50 и менее (и для всех обществ с ограниченной ответственностью) должен нотариально удостоверяться факт регистрации акционеров на собрании, в повестку дня которого включен вопрос об избрании исполнительного органа общества, досрочном прекращении его полномочий, избрании совета директоров, передаче полномочий единоличного исполнительного органа управляющей организации или управляющему. Данное положение не будет применяться в случае, если функции счетной комиссии на таком собрании акционеров будет выполнять регистратор;

-в обществах с числом акционеров более 50 функции счетной комиссии сможет осуществлять только регистратор;

-необходимо нотариально удостоверять факт присутствия на заседании совета директоров его членов, если на этом заседании будет рассматриваться вопрос об избрании исполнительного органа общества или досрочном прекращении его полномочий. А подлинность подписи председательствующего на заседании должна быть нотариально засвидетельствована.

В законе «Об акционерных обществах» теперь прописаны процедуры, которые необходимо соблюдать при скупке акций. Однако этого явно недостаточно. Нужно комплексное одномоментное изменение законодательства для того, чтобы корпоративные конфликты в целом и недружественное поглощение в частности перестали быть инструментом отъема собственности. И главное здесь – соблюсти баланс между регламентацией процедур и смысловой совокупностью совершаемых действий.

Например, упомянутая процедура скупки акций ограничивает в действиях аффилированных лиц. Однако уже существующая практика корпоративных конфликтов дает достаточно материала для понимания того, что признаки аффилированности из-за их формальности можно достаточно легко обойти. Поэтому при рассмотрении подобных дел в арбитражном суде и/или

[1] Защита по закону / Серебряный А. // Управление компанией. – № 5. – 2007.

антимонопольном органе было бы разумно не ограничиваться только формальными признаками аффилированности лиц, осуществлявших скупку акций, но и исследовать их возможную фактическую связь друг с другом (один из возможных примеров – координация действий по скупке акций из единого центра и финансирование скупки акций из одного источника).

Один из ключевых вопросов, на котором основывается рейдерство, – приобретение акций атакованной компании третьими лицами у лиц, завладевших акциями в результате неправомерных действий, являвшихся составной частью рейдерской атаки. Совершив несколько сделок купли-продажи с акциями между своими компаниями, рейдер продает акции конечному покупателю, который становится добросовестным приобретателем.

Ситуация может еще больше осложниться, если акции в процессе перепродаж тасовались, то есть для каждой последующей продажи формировался пакет акций из пакетов, приобретенных у разных продавцов. За счет такой техники и из-за того, что акции обращаются в бездокументарной форме, становится невозможно определить путь каждой конкретной акции от первой продажи до конечного покупателя.

При распутывании этих ситуаций владелец акций компании, которая подверглась рейдерской атаке, будет считать вопрос урегулированным только после возврата ему всех акций. Конечный же их покупатель, со своей стороны, будет считать ситуацию урегулированной после возврата уплаченных за акции денег. Возможно ли достичь этих двух целей одновременно? На бумаге – да, фактически – вряд ли.

В процессе перепродажи акций, скорее всего, будут участвовать подставные компании, поэтому взыскивать с них необходимо, поскольку цепочка банковских переводов должна привести следствие к деньгам. Но если подставные компании будут оперативно ликвидированы, этот путь возврата денег станет тупиковым.

Так как в основе рейдерства лежит уголовно наказуемое деяние: одно или несколько, то проблему рейдерства нельзя решить предложенным законодателем путем: утяжеление процедур в акционерном законодательстве не может заменить неотвратимость уголовного наказания для лиц, преступивших закон.

Передел рынка в различных отраслях экономики – нормальное явление, поэтому в будущем недружественное поглощение компаний останется, однако оно должно перестать быть рейдерством. Для этого из процесса недружественного поглощения должна уйти уголовно наказуемая составляющая. Подобное произошло некоторое время назад с процедурой банкротства организации. Напомним, что перед рейдерством именно банкротство организаций использовалось как «легальный» способ отъема бизнеса. Однако после изменения в законодательстве банкротство перестало быть пригодным для этого.

Пересечение гражданского и уголовного процессов может стать существенным препятствием для решения поставленной задачи возврата акций законному владельцу. Практика и опыт, накопленные арбитражными судами в ходе разрешения корпоративных конфликтов, должны быть осознаны (желательно в короткое время) судами общей юрисдикции.

4.3. Противостояние рейдерству (захватнической политике)

Принято считать, что основные войны по поводу собственности уже отгремели в конце прошлого века, а теперь наступил период некоего порядка и здравомыслия[1]. К сожалению, это не совсем так. Процессы насильственного перераспределения собственности не только не прекратились – они даже не замедлились. Изменились только способы и средства противоправного присвоения имущества. И если раньше, на стадии «первоначального накопления капитала», имели место в основном прямо противозаконные методы, а несколько позже использовались процедуры банкротства, то в настоящее время наиболее актуальный способ передела собственности – корпоративный захват. И эффективное противодействие подобному сложному, многоаспектному явлению современной российской хозяйственной и правовой действительности предполагает разработку и последовательную реализацию целого комплекса мер, стратегических и тактических способов защиты.

Чтобы эффективно выстроить систему защиты от враждебного нападения, в первую очередь необходимо определить возможные способы поглощения, которые могут быть применены к компании[2].

Наиболее распространенными в современной России способами враждебного поглощения стали:

- консолидация (скупка) мелких пакетов акций;
- рейдер организует скупку акций компании с целью последующего ее захвата;
- допэмиссия (компания-агрессор, будучи миноритарным акционером компании, инициирует дополнительную эмиссию акций, затем выкупает выпущенные акции, чем увеличивает свою долю); такая схема чаще всего применяется в компаниях, где главный акционер – государство, так как чиновника легче заинтересовать голосовать за допэмиссию. В результате после ее выкупа рейдером доля государства снижается до нескольких процентов;
- высокоинтеллектуальное вымогательство, приводящее к захвату активов предприятий – гринмэйл[3] (корпоративный шантаж). Первые упоминания о

---

[1] Корпоративное плутовство: анатомия проблемы / Шалапугин А. // Управление компанией. – № 6. – 2006.

[2] Защита от враждебного поглощения «по-русски» – управленческие аспекты / Никитин Л. // Управление компанией. – № 7. – 2004.

[3] Отцом-основателем гринмэйла принято считать американского бизнесмена Кеннета Дарта.

враждебных корпоративных действиях с целью получения отступных в отношении акционерных компаний в Великобритании относятся к XIX столетию, но термин «гринмэйл» получил широкое распространение только в 80-х годах прошлого столетия и такого определения мошеннической деятельности, как гринмэйл, нет ни в одном официальном разрешенном перечне. Россия познакомилась с этим явлением в середине 1990-х вместе с либерализацией экономики и уже к 2004 г. только в Москве из 37 организаций легкой промышленности, где за последние три года сменились собственники, 20 прекратили свою деятельность; в машиностроении ликвидировано 15 организаций, в пищевой промышленности – 5[1];

- контроль над менеджментом: рейдер путем подкупа или угроз вносит в устав компании изменения, позволяющие сформировать управления – наблюдательный совет или правление, где большинство руководящих должностей получают представители рейдера или доверенные;

- реприватизационный захват (компания-агрессор спекулирует темой «защиты государственных интересов»): будучи миноритарным акционером ОАО, компания-агрессор добивается в судах отмены приватизации, в результате которой контрольный пакет может перейти к другому собственнику;

- юридический террор (зачастую целью такой операции является получение «отступных»): компания-агрессор организует иски к организации по любым поводам – начиная от экологической обстановки в организации и заканчивая «неправильным» увольнением того или иного работника, организует «проблемы» в прокуратуре, МЧС, санэпидстанции и т. д.;

- захват с помощью регистратора (если независимый регистратор ОАО находится под контролем компании-агрессора): с помощью юридических манипуляций она может препятствовать проведению собрания акционеров ОАО, попытаться собрать свое собрание, даже если у нее всего 10 % акций. В результате длительных тяжб компания-агрессор либо устанавливает контроль над ОАО, либо вынуждает выкупить у него пакет акций за цену, превышающую их реальную стоимость в несколько раз;

- долговой захват (в случае если организация имеет кредиторскую задолженность перед компанией-агрессором или же если компания-агрессор скупила кредиторскую задолженность организации): под предлогом невыплаченного или просроченного кредита компания-агрессор получает решение суда о санации, таким образом, входит в органы управления или же просто забирает организацию с ее имущественным комплексом за долги с помощью силового захвата;

- силовой захват: получив незаконное решение суда, компания-агрессор привлекает для его исполнения исполнительную службу, милицию, спецподразделения МВД, а также собственные охранные структуры, с помощью которых захватывает имущественный комплекс, называет «своего» директора и устанавливают контроль над компанией. Однако в таком «чистом» виде силовой захват встречается редко;

[1] Маетная Е., Шипицина Н. «Московский комсомолец».

- информационной террор, целью которого чаще всего является также получение «отступных»: компания-агрессор организует информационные кампании в прессе против собственника и митинги возле организации по любым поводам.

Приведем обзорную характеристику системного подхода к защите предприятия.

Системный подход предполагает планомерное использование сочетания нескольких способов защиты, в частности постановку на пути врага оптимального (с точки зрения соотношения «эффективность защиты/затраты на защиту») количества «рогаток» и их использование в зависимости от намерений и действий потенциальных и реальных агрессоров.

Стратегические способы защиты – это способы, предусмотренные долгосрочным планом развития компании. Их применение обусловливает серьезные организационные изменения в системе управления бизнесом (например, переход к холдинговой структуре). Такие способы используются при планомерной организации защиты бизнеса, как правило тогда, когда нападение еще не началось и реальная, зримая угроза поглощения отсутствует.

Тем не менее, большинство активных и динамично развивающихся российских бизнес-структур при формировании своей стратегии развития обязательно учитывают фактор защиты бизнеса.

К *стратегическим способам защиты* относятся, главным образом, мероприятия организационно-управленческого характера: выстраивание корпоративной структуры (структуры организаций, входящих в холдинг, группу компаний), формирование системы внутреннего контроля, организация эффективной системы мотивации топ-менеджеров и др.

Тактические способы защиты используются тогда, когда поглощение уже началось, или тогда, когда угроза нападения стала очевидной. Они не требуют серьезных стратегических и организационных новаций. Как правило, это мероприятия юридического характера.

Управленческие способы защиты требуют серьезных организационных новаций. Это и переход к холдинговой структуре, и использование сервисных компаний (например, лизинговых). Другие же в революционных изменениях не нуждаются, но требуют формирования регулярной системы менеджмента. Остановимся подробнее на наиболее существенных аспектах регулярного менеджмента, ориентированного на защиту от враждебного поглощения.

Успех превентивной защиты зависит от четкости и слаженности работы компании в целом, ее органов управления и менеджеров как основной движущей силы, преодолевающей любые посягательства. Внутренняя бесконтрольность, нечеткость в разграничении полномочий или излишняя инертность в принятии решений сами по себе могут привести к отрицательным последствиям, а если они присутствуют в период атаки агрессора, то корабль пойдет ко дну, даже не успев дать бой.

Юридической основой защиты компании должны стать скрупулезно разработанные внутренние документы (Устав, Положения об органах управления и т. п.), соответствующие выбранной стратегии защиты. Зачастую к

этим документам относятся как к неприятной формальности, повторяя в них императивные нормы корпоративного законодательства. Собственники бизнеса нередко не принимают во внимание, что при угрозе враждебного поглощения им может просто не хватить времени на устранение противоречий в документах и внесение дополнений, необходимых для организации защиты.

В этой связи целесообразно говорить о принятии в обществе защищающего от поглощения устава. Единого рецепта защищающего устава на все случаи жизни и для любого общества быть не может. Однако имеются общие принципы, лежащие в основе разработки такого документа. Начинать надо с определения организационно-правовой формы предприятия. По своей правовой конструкции закрытые акционерные общества и общества с ограниченной ответственностью изначально имеют большую степень защиты от враждебных поглощений, чем открытые акционерные общества, так как заранее известен и численно ограничен круг акционеров (участников), имеется преимущественное право выкупа акций или отказа в приеме нового участника. Встречаются также достаточно экзотические варианты создания народных предприятий и автономных некоммерческих организаций, однако в этих случаях их «творцы» попадают в зависимость от выбранной организационно-правовой формы предприятия.

В защищающем уставе четко прописывается порядок осуществления сделок с акциями общества, порядок выбора и прекращения (включая досрочное прекращение) полномочий лиц, выступающих от имени общества, порядок внесения изменений в устав. Также исключаются неурегулированные вопросы (например, определение кворума общего собрания или совета директоров по вопросам, относящимся исключительно к их компетенции), закрепляется порядок конвертации привилегированных акций в обыкновенные, облигаций в акции, устанавливается порядок приобретения акций и порядок выкупа акций.

В обществах, где наличие совета директоров не обязательно, возможно введение этого органа и передача ему части полномочий единоличного исполнительного органа (генерального директора). Формирование совета директоров и правления позволяет использовать такой тактический способ защиты, как разумная бюрократизация порядка принятия решений в обществе. Процедурные вопросы принятия стратегически важных для общества решений следует четко регламентировать в положениях об органах управления. В этих документах должны определяться не только полномочия этих органов, но и порядок формирования повестки дня коллегиальных органов управления, порядок представления на рассмотрение выносимых вопросов и информации, порядок принятия решений (в том числе и путем заочного голосования), другие процедурные вопросы.

Разумная бюрократизация системы управления проводится и через регламентацию основных бизнес-процессов компании и наиболее значимых управленческих процедур. Вопросы построения логичных и прозрачных для топ-менеджмента и основных акционеров регламентов управления по направлениям «Продажи и сервис», «Закупки», «Производство и обеспечение

качества», «Финансы и экономика», «Инвестиции» сегодня одни из самых актуальных для большинства российских динамично развивающихся компаний.

Важное значение в регламентации управленческих процессов имеет тщательная разработка Положения о порядке заключения договоров. Правильное выстраивание процедуры заключения договора и четкие правовые конструкции наиболее распространенных в компании договоров позволяют в большинстве случаев избежать угрозы совершения работниками компании невыгодных для компании действий.

Современные реалии таковы, что кража или разглашение коммерческой информации могут нанести серьезный ущерб бизнесу, повлечь за собой утечку производственно-технологической информации и «ноу-хау», привести к корпоративным конфликтам, перехвату третьими лицами контроля над компанией, понижению рыночной стоимости не только акций или иных ценных бумаг, но и самой компании и даже к ее банкротству[1].

Коммерческая тайна – важный элемент бизнеса, ее охрана целиком и полностью зависит от своевременно проведенных мероприятий по предотвращению утечки важной информации. Одним из них, безусловно, является установление режима коммерческой тайны. Главное – правильно определить информацию, в отношении которой следует применять данный режим, а также цели, для которых он вводится.

Среди средств *защиты компании от поглощения до публичного объявления о сделке можно* выделить следующие меры, наиболее часто используемые на мировом рынке слияний и поглощений:

а) внесение изменений в устав компании («противоакульи» поправки к уставу – shark repellents). Среди таких изменений выделяют следующие:

- ротация совета директоров: совет делится на несколько частей, при этом каждый год избирается только одна часть;

- сверхбольшинство: утверждение сделки слияния сверхбольшинством акционеров;

- справедливая цена: ограничивает слияния акционерами, владеющими более чем определенной долей акций в обращении, если не платится справедливая цена (определяемая формулой или соответствующей процедурой оценки);

б) изменение места регистрации компании. Учитывая разницу в законодательстве отдельных регионов, выбирается то место для регистрации, где можно проще провести противозахватные поправки к уставу и облегчить себе судебную защиту;

в) «ядовитая пилюля» (poison pill)[2]. Подобные меры применяются компанией в целях уменьшения своей привлекательности для потенциального захватчика. Например, существующие акционеры наделяются правами,

[1] Мазавина А. Отражение рейдерских атак // Управление компанией. – № 8. – 2006.

[2] Способ был изобретен корпоративным юристом Мартином Липтоном (Martin Lipton), который впервые его опробовал в 1982 г. с целью защиты компании <Эль Пасо Электрик> (El Paso Electric) от поглощения со стороны Дженерал Американ Ойл (General American Oil).

которые в случае покупки значительной доли акций захватчиком могут быть использованы для приобретения обыкновенных акций компании по низкой цене – обычно за половину рыночной цены;

г) выпуск акций с более высокими правами голоса. Распространение обыкновенных акций нового класса с более высокими правами голоса позволяет менеджерам компании-«мишени» получить большинство голосов без владения большей долей акций;

д) выкуп с использованием заемных средств – покупка компании или ее подразделения группой частных инвесторов с привлечением высокой доли заемных средств. Акции компании, которую выкупают таким способом, больше не продаются свободно на фондовом рынке. Если при выкупе компании группу инвесторов возглавляют ее менеджеры, такую сделку называют выкупом компании менеджерами.

Защита компании после публичного объявления о ее поглощении может выражаться в следующем:

а) защита Пэкмена (Pac-Man defense) – контрнападение на акции захватчика;

б) судебная тяжба. Предполагает судебное разбирательство против захватчика за нарушение антимонопольного законодательства или законодательства о ценных бумагах;

в) слияние с «белым рыцарем» (white knight). Предусматривают объединение с дружественной компанией, которую обычно называют «белым рыцарем».

г) «зеленая броня» (greenmail), заключается в предложении группе инвесторов, угрожающих захватом, об обратном выкупе с премией, то есть предложение о выкупе компанией своих акций по цене, превышающей рыночную (а также, как правило, цену, которую уплатила за эти акции данная группа);

д) заключение контрактов на управление со своим управленческим персоналом, в которых предусматривается высокое вознаграждение за работу руководства. Это служит эффективным средством увеличения цены поглощаемой компании, так как стоимость «золотых парашютов» (golden parachutes) в этом случае существенно возрастает;

е) реструктуризация активов – покупка активов, которые не понравятся захватчику или создадут антимонопольные проблемы;

ж) реструктуризация обязательств – выпуск акций для дружественной третьей стороны или увеличение числа акционеров, выкуп акций с премией у существующих акционеров.

Перечисленные средства защиты от враждебных поглощений, – это лишь часть применяемых в мировой практике. Приведем еще некоторые из них:

а) «макаронная оборона» (macaroni defense) эффективна, когда компания-«мишень» выпускает на большую сумму облигации, которые по условию выпуска должны быть погашены досрочно по более высокой цене в случае поглощения компании. Следовательно, стоимость погашения облигаций возрастает, когда над компанией нависает угроза поглощения (подобно тому,

как макароны разбухают во время варки), делая поглощение чрезмерно дорогим;

б) «политика выжженной земли» (scorched-earth policy). Метод, используемый компанией-«мишенью» для того, чтобы сделаться менее привлекательной для покупателя. Например, она может согласиться на продажу наиболее привлекательных частей своего бизнеса, называемых «драгоценностями короны» (crown jewels), или назначить выплату всех задолженностей немедленно после слияния компаний;

в) «белая броня» (whitemail). Суть этого метода заключается в том, что компания-«мишень» продает большое число своих акций дружественной компании по цене ниже рыночной. Это ставит потенциального «захватчика» в положение, когда он должен будет купить примерно столько же акций, но по «вздутой» цене, чтобы захватить контроль над компанией. Этот метод помогает действующему руководству компании сохранять свое положение;

г) «белый кавалер» (white squire) – брокер, приобретающий меньше акций, чем в контрольном пакете компании.[1]

Многие агрессоры при скупке наиболее интересных активов действуют по принципу: «Зачем покупать компанию, если можно купить ее менеджмент?». Действительно, если в компании не построена действенная система независимого мониторинга ее финансово-хозяйственной деятельности (иначе говоря, система экономической безопасности бизнеса, система внутреннего контроля), реализовать этот принцип агрессору будет не так уж и сложно.

Система мониторинга традиционно реализуется через создание собственно службы текущего мониторинга (службы экономической безопасности) и контрольно-ревизионной службы, к задачам которой относится проведение комплексных проверок соблюдения установленных в компании процедур управления.

Создавая систему защиты, следует избегать тотальной бюрократизации процедур и жесткого контроля за их соблюдением, надо всегда помнить, что сама по себе система не может обеспечить действенной защиты бизнеса. Так как в основе любой системы управления коллективом в бизнесе лежит *правильная мотивация – менеджеров и ведущих специалистов,* то одним из действенных механизмов защиты бизнеса будет создание системы мотивации, ориентирующей менеджмент компании на рост стоимости и эффективности бизнеса. В западном бизнес-сообществе широко распространены схемы партнерского участия топ-менеджеров и ключевых специалистов в бизнесе (опционы, механизмы отложенного дохода, «парашюты»). В современной России эти механизмы почти не применяются, а это свидетельствует скорее о недостаточном развитии культуры корпоративного управления, чем о принципиальной невозможности использования этих схем на отечественной почве[2].

---

[1] Заикин В., Калашников Г. Механизмы защиты компаний / Заикин В., Калашников Г. // Управление компанией. – № 7. – 2004.

[2] Подробнее см.: Асаул, А.Н. Культура организации: проблемы формирования и

Российская практика корпоративных слияний и поглощений формировалась на фоне неразвитой правовой базы в области корпоративного права и отсутствия исторически сложившихся, эволюционных экономических отношений, что и сделало враждебные поглощения наиболее эффективным методом корпоративной стратегии в России. По сути, методы враждебных поглощений и соответствующие меры защиты, применяемые в России на начальном этапе становления государственности, претерпели определенные изменения только благодаря развитию корпоративного законодательства. Исключительно в связи с этим процессом некоторые средства, применяемые для защиты от враждебных поглощений, уже не могут быть столь же эффективными, как на заре становления корпоративного рынка России. В результате новых законодательных изменений средства защиты от враждебных поглощений, применяемые в России, перестали носить исключительно административный характер и приближаются к средствам защиты, широко используемым во всем мире.

Ниже мы рассмотрим наиболее распространенные в России экономические и правовые методы сопротивления потенциальному захватчику, которые используются руководством (акционерами) компании-«мишени»:

а) покупка акций компаниями, принадлежащими руководству, или выкуп компанией собственных акций, в том числе с последующей их продажей работникам и администрации (принадлежащих ей компаний) для увеличения доли «инсайдеров» в ущерб внешним акционерам. Такая стратегия получила широкое распространение в России во второй половине 1990-х гг.

б) контроль за реестром акционеров, а также ограничение доступа к реестру акционеров или манипуляции им, что эффективно при комплексных мерах защиты. Использование этого метода без каких-либо дополнительных средств не может предотвратить поглощение, но благодаря комплексным мероприятиям, в число которых входит и жесткий контроль реестра акционеров может предотвратить поглощение;

в) изменение размера уставного капитала компании посредством целенаправленного уменьшения («разводнения») доли конкретных «чужих» акционеров путем размещения акций новых эмиссий на льготных условиях среди администрации и работников, а также дружественных внешних и псевдовнешних акционеров. Этот метод широко применяется в первую очередь с целью консолидации, создания максимально управляемой корпоративной структуры. Таким образом, уменьшается риск поглощения за счет слаженных действий всех структурных подразделений компании;

г) привлечение местных властей для введения административных ограничений деятельности «чужих» посредников и компаний, скупающих акции работников бюджетообразующей компании – объекта атаки;

д) судебные иски о признании недействительными определенных сделок с акциями, поддерживаемые местными властями. В качестве примера можно

управления / Асаул А.Н., Асаул М.А., Ерофеев П.Ю., Ерофеев М.П. – СПб: Гуманистика, 2006. – 216с.

назвать корпоративные войны, развернувшиеся за крупнейшие лесопромышленные объекты России.

Список используемых в России средств защиты от враждебного поглощения не ограничивается мерами, перечисленными выше, так как арсенал методов поглощения постоянно пополняются. Следует еще раз подчеркнуть российские особенности средств защиты:

а) «шантаж» местных властей руководством в случае, если компания является бюджетообразующей;

б) введение различных материальных и административных санкций по отношению к работникам-акционерам, намеревающимся продать свои акции «постороннему» покупателю;

в) формирование двоевластия в компании (два общих собрания, два совета директоров, два генеральных директора);

г) вывод активов или реорганизация компании с выделением ликвидных активов в отдельные структуры и т. д.

На данном этапе развития российского рынка корпоративных слияний и поглощений очевидна национальная составляющая, отражающая особенности развития рыночных отношений в стране. Большинство средств защиты от враждебных поглощений, применяемых в России, не могут быть однозначно квалифицированы в соответствии с признанными мировыми институтами корпоративного поглощения, так как не только спектр средств получения контроля над компанией-«мишенью», но и средства защиты от такого поглощения не подпадают под стандартные критерии, принятые в международной практике. Тем не менее, необходимо отметить безусловно позитивный сдвиг в российском корпоративном законодательстве.

4.4. Информационная безопасность

Под информационной безопасностью понимается защищенность информации и поддерживающей инфраструктуры от случайных или преднамеренных воздействий естественного или искусственного характера, чреватых нанесением ущерба владельцам или пользователям информации и поддерживающей инфраструктуры. С методологической точки зрения правильный подход к проблемам информационной безопасности начинается с выявления субъектов и интересов субъектов, связанных с использованием информационных систем.

Информационная безопасность не сводится исключительно к защите информации. Субъект информационных отношений может пострадать (понести убытки) не только от несанкционированного доступа, но и от поломки системы, вызвавшей перерыв в обслуживании клиентов. Более того, для многих открытых организаций (например, учебных) собственно защита информации не стоит на первом месте.

Для того чтобы освоить основы обеспечения информационной безопасности, необходимо владеть понятийным аппаратом. Раскрытие

некоторых ключевых терминов не самоцель, важно формирование начальных представлений о целях и задачах защиты информации.

Под безопасностью информации понимается такое ее состояние, при котором исключается возможность просмотра, изменения или уничтожения информации лицами, не имеющими на это права, а также утечки за счет побочных электромагнитных излучений и наводок, специальных устройств перехвата (уничтожения) при передаче между объектами вычислительной техники.

Под защитой информации понимается совокупность мероприятий, направленных на обеспечение конфиденциальности и целостности обрабатываемой информации, а также доступности информации для пользователей.

Конфиденциальность – сохранение в секрете критичной информации, доступ к которой ограничен узким кругом пользователей (отдельных лиц или организаций).

Целостность – свойство, при наличии которого информация сохраняет заранее определенные вид и качество.

Доступность – такое состояние информации, когда она находится в том виде и месте, какие необходимы пользователю, и в то время, когда она ему необходима.

Целью защиты информации является сведение к минимуму потерь в управлении, вызванных нарушением целостности данных, их конфиденциальности или недоступности информации для потребителей.

Приведенная совокупность определений достаточна для формирования общего, пока еще абстрактного взгляда на построение системы информационной безопасности. Для уменьшения степени абстракции и формирования более детального замысла необходимо знание основных принципов организации системы информационной безопасности.

Принципы построения системы информационной безопасности. Современный опыт решения проблем информационной безопасности показывает, что для достижения наибольшего эффекта при организации защиты информации необходимо руководствоваться рядом принципов.

Первым и наиболее важным является *принцип непрерывности совершенствования и развития системы информационной безопасности*. Суть этого принципа заключается в постоянном контроле функционирования системы, в выявлении ее слабых мест, возможных каналов утечки информации и несанкционированного доступа, обновлении и дополнении механизмов защиты в зависимости от изменения характера внутренних и внешних угроз, обосновании и реализации на этой основе наиболее рациональных методов, способов и путей защиты информации. Таким образом, обеспечение информационной безопасности не может быть разовым мероприятием.

Вторым является *принцип комплексного использования всего арсенала имеющихся средств защиты во всех структурных элементах производства и на всех этапах технологического цикла обработки информации*. Комплексный характер защиты информации обусловлен действиями злоумышленников. Здесь

правомерно утверждение, что оружие защиты должно быть адекватно оружию нападения.

Кроме того, наибольший эффект достигается в том случае, когда все используемые средства, методы и мероприятия объединяются в единый, целостный механизм – *систему информационной безопасности*. Только в этом случае появляются системные свойства, не присущие ни одному из отдельных элементов системы защиты, а также возможность управлять системой, перераспределять ее ресурсы и применять современные методы повышения эффективности ее функционирования.

Можно определить систему информационной безопасности как *организованную совокупность органов, средств, методов и мероприятий, обеспечивающих защиту информации от разглашения, утечки и несанкционированного доступа*.

Важнейшими условиями обеспечения безопасности являются законность, достаточность, соблюдение баланса интересов личности и организации, высокий профессионализм представителей службы информационной безопасности, подготовка пользователей и соблюдение ими всех установленных правил сохранения конфиденциальности, взаимная ответственность персонала и руководства, взаимодействие с государственными правоохранительными органами.

Без соблюдения этих условий никакая система информационной безопасности не может обеспечить требуемого уровня защиты. С позиций системного подхода для реализации приведенных принципов процесс и сама система защиты информации должны отвечать некоторой совокупности требований.

Защита информации должна быть:

централизованной: необходимо иметь в виду, что процесс управления всегда централизован, в то время как структура системы, реализующей этот процесс, должна соответствовать структуре защищаемого объекта;

плановой: планирование осуществляется для создания взаимодействия всех подразделений организаций в интересах реализации принятой политики безопасности; каждая служба, отдел, направление разрабатывают детальные планы защиты информации в сфере своей компетенции с учетом общей цели организации;

конкретной и целенаправленной: защите подлежат абсолютно конкретные информационные ресурсы, представляющие интерес для конкурентов;

активной: защищать информацию необходимо с достаточной степенью настойчивости и целеустремленности. Это требование предполагает наличие в составе системы информационной безопасности средств прогнозирования, экспертных систем и других инструментов, позволяющих реализовать наряду с принципом «обнаружить и устранить» принцип «предвидеть и предотвратить»;

надежной и универсальной, охватывать весь технологический комплекс информационной деятельности объекта: методы и средства защиты должны надежно перекрывать все возможные каналы утечки информации и противодействовать способам несанкционированного доступа независимо от

формы представления информации, языка ее выражения и вида носителя, на котором она закреплена;

нестандартной (по сравнению с другими организациями), разнообразной по используемым средствам;

открытой для изменения и дополнения мер обеспечения безопасности информации;

экономически эффективной: затраты на систему защиты не должны превышать размеры возможного ущерба.

Наряду с основными требованиями существует ряд устоявшихся рекомендаций, которые будут полезны создателям систем информационной безопасности:

средства защиты должны быть просты для технического обслуживания и «прозрачны» для пользователей;

каждый пользователь должен иметь минимальный набор привилегий, необходимых для работы;

возможность отключения защиты в особых случаях, например, когда механизмы зашиты реально мешают выполнению работ;

независимость системы защиты от субъектов защиты;

разработчики должны учитывать враждебность окружения (то есть предполагать, что пользователи имеют наихудшие намерения, будут совершать серьезные ошибки и искать пути обхода механизмов защиты);

в организации не должно быть излишней информации о существовании механизмов защиты.

Все перечисленные позиции следует положить в основу формирования системы защиты информации.

Теперь, владея основными концептуальными положениями, необходимо освоить механизм выработки детальных предложений по формированию политики и построению системы информационной безопасности.

Последовательность действий при разработке системы обеспечения информационной безопасности объекта. Прежде чем приступать к разработке системы информационной безопасности, необходимо определить, что же для организации (физического лица) является интеллектуальной собственностью.

С точки зрения делового человека, интеллектуальной собственностью являются информационные ресурсы, знания, которые помогают ему эффективно разрабатывать и изготавливать новую продукцию, выгодно продавать товар или каким-то другим образом увеличивать свою прибыль. Способ управления производством, технологический процесс, список клиентов, профиль научных исследований, анализ конкурентоспособности – вот лишь некоторые примеры.

Незнание того, что составляет интеллектуальную собственность, есть уже шаг к потерям финансовым, моральным и материальным. Именно с этого надо начинать создание системы защиты информации. Затем, вне зависимости от размеров организации и специфики ее информационной системы, необходимо:

определить границы управления информационной безопасностью объекта;

провести анализ уязвимости;

выбрать контрмеры, обеспечивающие информационную безопасность;
определить политику информационной безопасности;
проверить систему защиты;
составить план защиты;
реализовать план защиты (управление системой защиты).

Определение границ управления информационной безопасностью объекта. Целью этого этапа является определение всех возможных «болевых точек» объекта, которые могут доставить неприятности с точки зрения безопасности информационных ресурсов, представляющих для организации определенную ценность.

Для работ на данном этапе должны быть собраны следующие сведения:

1. Перечень сведений, составляющих коммерческую или служебную тайну.
2. Организационно-штатная структура организации.
3. Характеристика и план объекта, размещение средств вычислительной техники и поддерживающей инфраструктуры.

На плане объекта указывается порядок расположения административных зданий, производственных и вспомогательных помещений, различных строений, площадок, складов, стендов и подъездных путей с учетом масштаба изображения.

Дополнительно на плане указываются структура и состав автоматизированной системы, помещения, в которых имеются технические средства обработки критичной информации с учетом их расположения. Указываются также контуры вероятного установления информационного контакта с источником излучений по видам технических средств наблюдения с учетом условий среды, по времени и месту.

4. Перечень и характеристика используемых автоматизированных рабочих мест, серверов, носителей информации.
5. Описание информационных потоков, технология обработки информации и решаемые задачи, порядок хранения информации. Для решаемых задач должны быть построены модели обработки информации в терминах ресурсов.
6. Используемые средства связи (цифровая, голосовая и т. д.). Знание элементов системы дает возможность выделить критичные ресурсы и определить степень детализации будущего обследования. Инвентаризация информационных ресурсов должна производиться исходя из последующего анализа их уязвимости. Чем качественнее будут проведены работы на этом этапе, тем выше будет достоверность оценок на следующем.

В результате должен быть составлен документ, в котором зафиксированы границы системы, перечислены ресурсы, подлежащие защите, дана система критериев для оценки их ценности. В идеале такой документ должен включать информационно-логическую модель объекта, иллюстрирующую технологию обработки критичной информации с выделением вероятных точек уязвимости, по каждой из которых необходимо иметь полную характеристику. Такая модель является базой, а ее полнота – залогом успеха на следующем этапе построения системы информационной безопасности.

Анализ уязвимости**.** По сути, это самый главный этап во всей работе. От того, насколько полно и правильно будет проанализировано состояние защищенности информационных ресурсов, зависит эффективность всех последующих мероприятий.

Необходимо рассмотреть все возможные угрозы и оценить размеры возможного ущерба.

Под угрозой (риском) следует понимать реальные или возможные действия или условия, приводящие к хищению, искажению, изменению или уничтожению информации в информационной системе, а также приводящие к прямым материальным убыткам за счет воздействия на материальные ресурсы.

Анализируемые виды угроз следует выбирать из соображений здравого смысла, но в пределах выбранных видов необходимо провести максимально полное рассмотрение.

Оценивая вероятность осуществления угроз, целесообразно учитывать не только среднестатистические данные, но и специфику конкретных информационных систем.

Для проведения анализа уязвимости исследователю целесообразно иметь в своем распоряжении модели каналов утечки информации и несанкционированного доступа, методики определения вероятности информационного контакта, модель нарушителя, перечень возможностей информационных инфекций, способы применения и тактико-технические возможности технических средств ведения разведки, методику оценки информационной безопасности.

Анализ уязвимости начинается с выбора анализируемых объектов и определения степени детальности их рассмотрения.

На этом этапе большую помощь может оказать разработанная инфологическая структура объекта.

Для определения объектов защиты удобно рассматривать АСУ как четырехуровневую систему.

Внешний уровень характеризуется информационными, главным образом сетевыми, сервисами, предоставляемыми данной системой, и аналогичными сервисами, запрашиваемыми другими подсистемами. На этом уровне должны отсекаться как попытки внешнего несанкционированного доступа к ресурсам подсистемы, так и попытки обслуживающего персонала АСУ несанкционированно переслать информацию в каналы связи.

Сетевой уровень связан с доступом к информационным ресурсам внутри локальных сетей. Безопасность информации на этом уровне обеспечивается средствами проверки подлинности пользователей и разграничением доступа к ресурсам локальной сети (идентификация, аутентификация и авторизация).

Защите системных ресурсов должно уделяться особое внимание, поскольку несанкционированный доступ к ним может сделать бессмысленными прочие меры безопасности.

На каждом уровне определяются уязвимые элементы. Уязвимым является каждый компонент информационной системы. Но в сферу анализа невозможно включить каждый байт. Приходится останавливаться на некотором уровне

детализации, отдавая себе отчет в приближенности оценки. Для новых систем предпочтителен детальный анализ. Старая система, подвергшаяся небольшим модификациям, может быть проанализирована только с точки зрения оценки влияния новых элементов на безопасность всей системы.

Следующим шагом на пути анализа уязвимости является моделирование каналов утечки информации и НСД.

Любые технические средства по своей природе потенциально обладают каналами утечки информации. Под каналом утечки информации принято понимать физический путь от источника конфиденциальной информации, по которому возможна утечка охраняемых сведений, к злоумышленнику. Для возникновения (образования, установления) канала утечки информации необходимы определенные пространственные, энергетические и временные условия, а также соответствующие средства приема и фиксации информации на стороне злоумышленника.

Применительно к практике каналы утечки информации можно разделить на следующие группы:

визуально-оптические;

акустические (включая и акустико-преобразовательные);

электромагнитные (включая магнитные и электрические);

материально-вещественные (бумага, фото-, магнитные носители, производственные отходы различного вида).

Основная задача моделирования каналов утечки информации и соответствующих способов несанкционированного доступа к источникам конфиденциальной информации на конкретном объекте защиты – это выявление особенностей, характеристик, условий возникновения каналов и, в результате, получение новых знаний, необходимых для построения системы защиты информации.

Основное требование к модели – адекватность, то есть степень соответствия разработанной модели реально протекающим процессам. Любая модель канала утечки информации должна показывать не только сам путь, но и возможность (вероятность) установления информационного контакта. Вероятность установления информационного контакта – численная величина, определяемая пространственными, временными и энергетическими условиями и характеристиками средства наблюдения. Условия установления информационного контакта можно представить в виде обобщенной модели.

Разнообразие источников конфиденциальной информации, способов несанкционированного доступа к ним и средств реализации несанкционированного доступа в конкретных условиях требует разработки частных моделей каждого варианта информационного контакта и оценки вероятности его возникновения. Имея определенные методики, можно рассчитать возможность такого контакта в конкретных условиях.

Главная ценность подобных методик заключается в возможности варьирования аргументов функции (мощность излучения, высота и коэффициент концентрации антенны и т. п.) в интересах достижения минимальных значений вероятности установления информационного контакта,

а значит, и в поиске совокупности способов снижения ее значений. Для анализа уязвимости информационных ресурсов необходимо выявить каналы утечки информации, хорошо представлять облик нарушителя и вероятные способы его действий, намерения, а также возможности технических средств получения информации по различным каналам. Только совокупность этих знаний позволит адекватно среагировать на возможные угрозы и, в конце концов, выбрать соответствующие средства защиты.

Сами же действия нарушителя во многом определяются надежностью системы защиты информации, так как для достижения своих целей он должен приложить некоторые усилия, затратить определенные ресурсы. Если система защиты достаточно надежна, его затраты будут чрезмерно высоки и он откажется от своего замысла.

Поэтому представляется целесообразным разработать наиболее вероятный сценарий осуществления противоправных действий по доступу к информации в конкретной системе, одной из важнейших составляющих которого и является модель нарушителя. Наличие такого сценария, который должен постоянно корректироваться на основе новых знаний о возможностях нарушителя, после изменений в системе защиты и на основе анализа причин произошедших нарушений, позволит либо повлиять на сами причины нарушения, либо точнее определить требования к системе защиты от данного вида нарушений.

Основные контуры модели нарушителя определены в руководящем документе Гостехкомиссии России «Концепция защиты средств вычислительной техники и автоматизированных систем от несанкционированного доступа к информации».

Кроме уровня знаний нарушителя, его квалификации, подготовленности к реализации своих замыслов, для формирования наиболее полной модели нарушителя необходимо определить:

категорию лиц, к которой может принадлежать нарушитель;

мотивы действий нарушителя (преследуемые нарушителем цели);

техническую оснащенность и используемые для совершения нарушения методы и средства;

предполагаемые место и время осуществления незаконных действий нарушителя;

ограничения и предположения о характере возможных действий.

Результаты исследований причин нарушений (по данным Datapro Information Services Group и других организаций) говорят об одном: главный источник нарушений – внутри самой автоматизированной системы: 75-85 % нарушений совершаются самими служащими организации, имеющими доступ к ее системе, и только 15-25 % нарушений совершаются лицами со стороны.

Внутренними нарушителями могут быть: пользователи (операторы) системы; персонал, обслуживающий технические средства (инженеры, техники и т. п.); сотрудники отделов разработки и сопровождения программного обеспечения (прикладные и системные программисты); технический персонал, обслуживающий здания и имеющий доступ в помещения; руководители различных уровней.

Внешними нарушителями могут быть: клиенты (представители сторонних организаций, граждане); представители организаций, с которыми осуществляется взаимодействие; лица, случайно или умышленно нарушившие пропускной режим; любые лица за пределами контролируемой зоны.

При формировании модели нарушителя и оценке риска от действий персонала необходимо дифференцировать всех сотрудников по возможности доступа к системе и, следовательно, по потенциальному ущербу от каждой категории пользователей. Например, оператор или программист автоматизированной банковской системы может нанести несравненно больший ущерб, чем обычный пользователь, тем более непрофессионал.

Таким образом, каждый пользователь в соответствии со своей категорией риска может нанести больший или меньший ущерб системе. Необходимо учитывать, что пользователи различных категорий различаются не только по степени риска, но и по тому, какому элементу системы они угрожают больше всего. Так можно оценить степень риска данной категории пользователей относительно данного элемента системы и представить результаты анализа в виде таблицы соответствий.

Приведенный подход к категорированию персонала системы по степени риска должен использоваться для определения возможностей каждого типа нарушителя по незаконному доступу к информации, циркулирующей в АСУ. Наличие такой информации, безусловно, облегчит дальнейшую работу по проектированию системы и ее эксплуатации.

При формировании модели нарушителя следует уделять особое внимание личности нарушителя. Это поможет разобраться в побудительных мотивах и принять соответствующие меры для уменьшения вероятности совершения нарушений.

В целях овладения конфиденциальной информацией нарушители широко используют современные технические средства, обеспечивающие реализацию рассмотренных способов несанкционированного доступа к объектам и источникам охраняемых сведений.

По технической оснащенности и используемым методам и средствам нарушители подразделяются:

на применяющих пассивные средства (средства перехвата без модификации компонентов системы);

на использующих только штатные средства и недостатки системы защиты для ее преодоления (несанкционированные действия с использованием разрешенных средств);

на применяющих методы и средства активного воздействия (модификация и подключение дополнительных технических средств, подключение к каналам передачи данных, внедрение программных закладок и использование специальных инструментальных и технологических программ).

Приведенная классификация предусматривает постоянное обновление информации о характеристиках технических и программных средств ведения разведки и обеспечения доступа к информации.

Незаконные действия нарушитель может осуществлять:

в разное время (в процессе функционирования, во время работы компонентов системы, во время плановых перерывов в работе, в нерабочее время, в перерывы для обслуживания и ремонта и т. п.);

с разных мест (из-за пределов контролируемой зоны; внутри контролируемой зоны, но без доступа в выделенные для размещения компонентов помещения; внутри выделенных помещений, но без доступа к техническим средствам; с доступом к техническим средствам и с рабочих мест конечных пользователей; с доступом в зону данных, архивов и т. п.; с доступом в зону управления средствами обеспечения безопасности).

Учет места и времени действий злоумышленника также позволит конкретизировать его возможности и учесть их для повышения качества системы защиты информации.

Определение значений возможных характеристик нарушителей в значительной степени субъективно. Модель нарушителя, построенная с учетом особенностей конкретной предметной области и технологии обработки информации, может быть представлена несколькими вариантами его облика.

Совокупность моделей действий нарушителя может быть полезной с точки зрения прогнозирования возможных событий во всем разнообразии складывающихся ситуаций, для предотвращения действий нарушителя, построения надежной системы защиты информации, использования современных средств интеллектуальной поддержки для управления системой защиты.

Теперь в руках исследователя есть все исходные данные для оценки потерь (возможного ущерба). Желательно, чтобы эта оценка была количественной. Для оценки потерь могут быть использованы как точные методы современной математики, так и методы экспертных оценок, которые весьма широко используются при решении подобных задач.

Оценивая тяжесть ущерба, необходимо иметь в виду: непосредственные расходы на замену оборудования, анализ и исследование причин и величины ущерба, восстановление информации и функций АС по ее обработке; косвенные потери, связанные со снижением банковского доверия, потерей клиентуры, подрывом репутации, ослаблением позиций на рынке.

Естественно, информационные потери требуют расходов на их восстановление, что приводит к временным задержкам, вызывающим соответствующие претензии пользователей, потерю интересов, а иногда и финансовые санкции.

Для оценки потерь необходимо описать сценарий действий трех сторон: нарушителя – по использованию добытой информации, службы информационной безопасности – по предотвращению последствий и восстановлению нормального функционирования системы и третьей стороны.

Оценив потери по каждой из вероятных угроз, необходимо определить стратегию управления рисками. При этом возможно несколько подходов:

уменьшение риска (многие риски могут быть существенно уменьшены путем использования весьма простых и дешевых контрмер);

уклонение от риска (от некоторых классов рисков можно уклониться; например, вынесение Web-сервера организации за пределы локальной сети позволяет избежать риска несанкционированного доступа в локальную сеть со стороны Web-клиентов);

изменение характера риска (можно принять некоторые меры, например страхование отдельных рисков);

принятие риска (не все риски могут быть уменьшены до пренебрежимо малой величины). Возможна ситуация, когда для уменьшения риска не существует эффективных и приемлемых по цене мер. В этом случае приходится поднимать планку приемлемого риска и переносить центр тяжести на смягчение последствий и выработку планов восстановления после аварий, стихийных бедствий и иных происшествий.

На практике, после принятия стандартного набора контрмер, ряд рисков уменьшается, но остается все еще значимым. Необходимо знать остаточную величину риска. Если какие-либо риски оказались недопустимо высокими, необходимо реализовать дополнительные защитные меры.

Проведение анализа рисков и оценки потерь требует глубоких системных знаний и аналитического мышления во многих смежных областях зашиты информации. Без таких знаний невозможно будет впоследствии построить надежную систему информационной безопасности на выделенные средства и в заданные сроки.

По результатам работ, на этапе анализа уязвимости должно быть подготовлено экспертное заключение о защищенности информационных ресурсов на объекте, включающее в себя:

модели каналов утечки информации и несанкционированного доступа;

методики определения вероятностей установления информационного контакта для внешних нарушителей;

сценарии возможных действий нарушителя по каждому из видов угроз, учитывающие модель нарушителя, возможности системы защиты информации и технических средств разведки, а также действия нарушителя после ознакомления с информацией, ее искажения или уничтожения.

Руководство предприятия или организации, как правило, ожидает точной количественной оценки защищенности информационных ресурсов на объекте. Не всегда удается получить такие оценки, однако можно вычленить наиболее уязвимые участки и сделать прогноз о возможных проявлениях описанных в отчете угроз.

4.5. Защита информационных ресурсов и повышение информационной безопасности

Предпринимаемые меры защиты должны быть адекватны вероятности осуществления данного типа угрозы и потенциальному ущербу, который может быть нанесен в том случае, если угроза осуществится (включая затраты на защиту от нее).

Необходимо иметь в виду, что многие меры защиты требуют достаточно больших вычислительных ресурсов, что в свою очередь существенно влияет на процесс обработки информации. В связи с этим, современный подход к решению этой проблемы заключается в применении в АСУ принципов ситуационного управления защищенностью информационных ресурсов. Суть такого подхода заключается в том, что требуемый уровень безопасности информации устанавливается в соответствии с ситуацией, определяющей соотношение между ценностью перерабатываемой информации, затратами (снижением производительности АСУ, дополнительным расходом оперативной памяти и др.), которые необходимы для достижения этого уровня, и возможными суммарными потерями (материальными, моральными и др.) от искажения и несанкционированного использования информации.

Необходимые характеристики защиты информационных ресурсов определяются в ходе ситуационного планирования при непосредственной подготовке технологического процесса защищенной обработки информации с учетом сложившейся ситуации, а также (в сокращенном объеме) во время процесса обработки. Выбирая защитные меры, приходится учитывать не только прямые расходы на закупку оборудования и программ, но и расходы на внедрение новинки, на обучение и переподготовку персонала. Важным обстоятельством является совместимость нового средства со сложившейся аппаратно-программной структурой объекта.

Зарубежный опыт в области защиты интеллектуальной собственности и отечественный опыт в защите государственных секретов показывает, что *эффективной может быть только комплексная защита, сочетающая в себе такие направления защиты, как правовое, организационное и инженерно-техническое*.

Правовое направление предусматривает формирование совокупности законодательных актов, нормативно-правовых документов, положений, инструкций, руководств, требования которых являются обязательными в рамках сферы их деятельности в системе защиты информации.

Организационное направление – это регламентация производственной деятельности и взаимоотношений исполнителей на нормативно-правовой основе таким образом, что разглашение, утечка и несанкционированный доступ к конфиденциальной информации становятся невозможными или существенно затрудняются за счет проведения организационных мероприятий.

По мнению специалистов, организационные мероприятия играют большую роль в создании надежного механизма защиты информации, так как возможности несанкционированного использования конфиденциальных сведений в значительной мере обусловлены не техническими аспектами, а злоумышленными действиями, нерадивостью, небрежностью и халатностью пользователей или персонала защиты.

К *организационным* мероприятиям относятся:

– мероприятия, осуществляемые при проектировании, строительстве и оборудовании служебных и производственных зданий и помещений;

– мероприятия, осуществляемые при подборе персонала;

– организация и поддержание надежного пропускного режима, охраны помещений и территории, контроля за посетителями;

– организация хранения и использования документов и носителей конфиденциальной информации;

– организация защиты информации;

– организация регулярного обучения сотрудников.

Одним из основных компонентов организационного обеспечения информационной безопасности компании является Служба информационной безопасности (СИБ – орган управления системой защиты информации). Именно от профессиональной подготовленности сотрудников службы информационной безопасности, наличия в их арсенале современных средств управления безопасностью во многом зависит эффективность мер по защите информации. Ее штатная структура, численность и состав определяются реальными потребностями компании, степенью конфиденциальности ее информации и общим состоянием безопасности.

Основная цель функционирования СИБ: используя организационные меры и программно-аппаратные средства, избежать или хотя бы свести к минимуму возможность нарушения политики безопасности, в крайнем случае, вовремя заметить и устранить последствия нарушения.

Для обеспечения успешной работы СИБ необходимо определить ее права и обязанности, а также правила взаимодействия с другими подразделениями по вопросам зашиты информации на объекте. Численность службы должна быть достаточной для выполнения всех возлагаемых на нее функций. Желательно, чтобы штатный состав службы не имел обязанностей, связанных с функционированием объекта защиты. Службе информационной безопасности должны быть обеспечены все условия, необходимые для выполнения своих функций.

Ядром *инженерно-технического направления* являются программно-аппаратные средства защиты информации, к которым относятся механические, электромеханические, электронные, оптические, лазерные, радио- и радиотехнические, радиолокационные и другие устройства, системы и сооружения, предназначенные для обеспечения безопасности и защиты информации.

Под программным обеспечением безопасности информации понимается совокупность специальных программ, реализующих функции защиты информации и режима функционирования.

Сформированная совокупность правовых, организационных и инженерно-технических мероприятий выливается в соответствующую политику безопасности.

Политика безопасности определяет облик системы защиты информации в виде совокупности правовых норм, организационных (правовых) мер, комплекса программно-технических средств и процедурных решений, направленных на противодействие угрозам с целью исключения или минимизации возможных последствий проявления информационных воздействий. После принятия того или иного варианта политики безопасности

необходимо оценить уровень безопасности информационной системы. Естественно, что оценка защищенности производится по совокупности показателей, основными из которых являются стоимость, эффективность, реализуемость.

Задача оценки вариантов построения системы защиты информации достаточно сложная, требующая привлечения современных математических методов многопараметрической оценки эффективности, к ним относятся: метод анализа иерархий, экспертные методы, метод последовательных уступок и ряд других.

Когда намеченные меры приняты, необходимо проверить их действенность, то есть убедиться, что остаточные риски стали приемлемыми. Если это на самом деле так, то можно намечать дату ближайшей переоценки. В противном случае, придется проанализировать допущенные ошибки и провести повторный сеанс анализа уязвимости с учетом изменений в системе зашиты.

После того как сформирован возможный сценарий действий нарушителя, возникает необходимость проверки системы защиты информации. Такая проверка называется «тестирование на проникновение». Цель – предоставление гарантий того, что для неавторизованного пользователя не существует простых путей обойти механизмы защиты.

Один из возможных способов аттестации безопасности системы – приглашение хакеров для взлома без предварительного уведомления персонала сети. Для этого выделяется группа из двух-трех человек, имеющих высокую профессиональную подготовку. Хакерам предоставляется в распоряжение автоматизированная система в защищенном исполнении, и группа в течение 1–3 месяцев пытается найти уязвимые места и разработать на их основе тестовые средства для обхода механизмов защиты. Наемные хакеры представляют конфиденциальный доклад по результатам работы с оценкой уровня доступности информации и рекомендациями по улучшению защиты.

Наряду с таким способом используются программные средства тестирования.

На этапе *составления плана зашиты,* в соответствии с выбранной политикой безопасности разрабатывается план его реализации. План защиты является документом, вводящим в действие систему защиты информации, который утверждается руководителем организации.

Планирование связано не только с наилучшим использованием всех возможностей, которыми располагает компания, в том числе выделенных ресурсов, но и с предотвращением ошибочных действий, могущих привести к снижению эффективности предпринятых мер по защите информации.

План защиты информации на объекте должен включать:

– описание защищаемой системы (основные характеристики защищаемого объекта: назначение объекта, перечень решаемых задач, конфигурация, характеристики и размещение технических средств и программного обеспечения, перечень категорий информации (пакетов, файлов, наборов и баз данных, в которых они содержатся), подлежащих защите, и требований по обеспечению доступа, конфиденциальности, целостности этих категорий

информации, список пользователей и их полномочий по доступу к ресурсам системы и т. п.);

– цель защиты системы и пути обеспечения безопасности автоматизированной системы и циркулирующей в ней информации;

– перечень значимых угроз безопасности автоматизированной системы, от которых требуется зашита, и наиболее вероятных путей нанесения ущерба;

– политику информационной безопасности;

– план размещения средств и функциональную схему системы защиты информации на объекте;

– спецификацию средств зашиты информации и смету затрат на их внедрение;

– календарный план проведения организационных и технических мероприятий по защите информации, порядок ввода в действие средств защиты;

– основные правила, регламентирующие деятельность персонала по вопросам обеспечения информационной безопасности объекта (особые обязанности должностных лиц, обслуживающих автоматизированную систему);

– порядок пересмотра плана и модернизации средств защиты.

Пересмотр плана защиты осуществляется при изменении следующих компонентов объекта:

– кадровые изменения;

– изменения архитектуры информационной системы (подключение других локальных сетей, изменение или модификация используемых средств вычислительной техники или ПО);

– изменения территориального расположения компонентов автоматизированной системы.

В рамках плана защиты необходимо иметь план действий персонала в критических ситуациях. Такой план называется *планом обеспечения непрерывной работы и восстановления информации* и содержит следующие пункты:

– цель обеспечения непрерывности процесса функционирования автоматизированной системы, восстановления ее работоспособности и пути ее достижения;

– перечень и классификация возможных кризисных ситуаций;

– требования, меры и средства обеспечения непрерывной работы и восстановления процесса обработки информации (порядок создания, хранения и использования резервных копий информации, ведения текущих, долговременных и аварийных архивов; состав резервного оборудования и порядок его использования и т. п.);

– обязанности и порядок действий различных категорий персонала системы в кризисных ситуациях, при ликвидации их последствий, минимизации наносимого ущерба и по восстановлению нормального функционирования системы.

Если организация осуществляет обмен электронными документами с партнерами по выполнению единых заказов, то необходимо в план защиты включить договор о порядке организации обмена электронными документами, в котором отражаются следующие вопросы:

– разграничение ответственности субъектов, участвующих в процессах обмена электронными документами;

– определение порядка подготовки, оформления, передачи, приема, проверки подлинности и целостности электронных документов;

– определение порядка генерации, сертификации и распространения ключевой информации (ключей, паролей и т. п.);

– определение порядка разрешения споров в случае возникновения конфликтов.

Исходя из того, что план защиты информации представляет собой пакет текстуально-графических документов, необходимо отметить, что наряду с приведенными компонентами этого пакета в него могут входить:

– положение о коммерческой тайне, определяющее перечень сведений, составляющих коммерческую тайну, и порядок его определения, а также обязанности должностных лиц по защите коммерческой тайны;

– положение о защите информации, регламентирующее все направления деятельности по реализации политики безопасности, а также ряд дополнительных инструкций, правил, положений, соответствующих специфике объекта защиты.

Реализация плана защиты (управление системой зашиты) предполагает разработку необходимых документов, заключение договоров с поставщиками, монтаж и настройку оборудования и т. д. После того как сформирована система защиты информации, решается задача ее эффективного использования, а значит, управления безопасностью.

Управление – *процесс целенаправленного воздействия на объект, осуществляемый для организации его функционирования по заданной программе*.

Управление информационной безопасностью должно быть:

– устойчивым к активным вмешательствам нарушителя;

– непрерывным, обеспечивающим постоянное воздействие на процесс защиты;

– скрытым, не позволяющим выявлять организацию управления защитой информации;

– оперативным, обеспечивающим возможность своевременно и адекватно реагировать на действия злоумышленников и реализовывать управленческие решения к заданному сроку.

Кроме того, решения по защите информации должны быть обоснованными с точки зрения всестороннего учета условий выполнения поставленной задачи, применения различных моделей, расчетных и информационных задач, экспертных систем, опыта и любых других данных, повышающих достоверность исходной информации и принимаемых решений.

Показателем эффективности управления защитой информации является время цикла управления при заданном качестве принимаемых решений. В цикл управления входит сбор необходимой информации для оценки ситуации, принятие решения, формирование соответствующих команд и их исполнение. В качестве критерия эффективности может использоваться время реакции системы защиты информации на нарушение, которое не должно превышать времени устаревания информации исходя из ее ценности.

Как показывает разработка реальных АСУ, ни один из способов (мер, средств и мероприятий) обеспечения безопасности информации не является надежным, а максимальный эффект достигается при объединении всех их в целостную систему защиты информации. Только оптимальное сочетание организационных, технических и программных мероприятий, а также постоянное внимание и контроль над поддержанием системы защиты в актуальном состоянии позволят с наибольшей эффективностью обеспечить решение постоянной задачи.

Методологические основы обеспечения информационной безопасности являются достаточно общими рекомендациями, базирующимися на мировом опыте создания подобных систем. Задача каждого специалиста по защите информации – адаптировать абстрактные положения к своей конкретной предметной области (организации, банку), в которой всегда найдутся свои особенности и тонкости этого непростого ремесла.

Анализ отечественного и зарубежного опыта убедительно доказывает необходимость создания целостной системы информационной безопасности компании, увязывающей оперативные, оперативно-технические и организационные меры защиты. Причем система безопасности должна быть оптимальной с точки зрения соотношения затрат и ценности защищаемых ресурсов. Необходима гибкость и адаптация системы к быстро меняющимся факторам окружающей среды, организационной и социальной обстановке в учреждении. Достичь такого уровня безопасности невозможно без проведения анализа существующих угроз и возможных каналов утечки информации, а также без выработки политики информационной безопасности на предприятии. В итоге должен быть создан план защиты, реализующий принципы, заложенные в политике безопасности.

Целью проведения работ по анализу риска и выработке рекомендаций является определение правильного (с точки зрения организации) способа использования вычислительных и коммуникационных ресурсов, а также разработка мер по предотвращению и ликвидации последствий нарушений режима безопасности. Чтобы достичь данной цели, необходимо учитывать специфику конкретной организации. Кто принимает участие в проведении работ по исследованию информационной защищенности? Вопросы приема, передачи и обработки информации могут касаться большей части сотрудников организации. Однако реально оказать влияние на информационную защищенность может технический персонал, способный понять все аспекты политики безопасности и ее реализации, а также руководители, способные влиять на проведение политики в жизнь. Реально это чаще всего сотрудники

службы безопасности (информационной) и службы, отвечающей за автоматизацию процессов обработки информационных потоков.

При проведении работ могут применяться разнообразные методы: экспертно-документальный метод, метод интервьюирования персонала, имеющего отношение к доступу и обработке конфиденциальной информации, измерение и оценка уровней излучения для отдельных технических средств и каналов утечки информации; проверка функций или комплекса функций защиты информации с помощью тестирующих средств, а также путем их пробного запуска и наблюдения за их выполнением, попытки «взлома» систем защиты информации. Выполнение работ по анализу риска лучше всего поручить профессионалам: собственным профессиональным службам или фирмам, специализирующимся на деятельности в этой области. Успешное их проведение возможно при владении вышеописанными методами, при наличии квалифицированных специалистов и инструментария. Но существуют и другие сложности и «подводные камни», на которые обязательно нужно обратить внимание. Это проблемы, выявленные на практике и слабо поддающиеся формализации: проблемы не технического или технологического характера, которые так или иначе решаются, а проблемы социального и политического характера.

Проблема 1. Отсутствие понимания у персонала и руководителей среднего и нижнего ранга необходимости проведения работ по повышению уровня информационной безопасности.

Дело в том, что на этой ступеньке управленческой лестницы, как правило, не видно стратегических задач, стоящих перед организацией. Вопросы безопасности при этом могут вызывать даже раздражение – они создают «ненужные» трудности.

Как правило, приводятся следующие аргументы против проведения работ и принятия мер по обеспечению информационной безопасности:

появление дополнительных ограничений для конечных пользователей и специалистов подразделений, затрудняющее пользование автоматизированной системой организации;

необходимость дополнительных материальных затрат как на проведение таких работ, так и на расширение штата специалистов, занимающихся проблемой информационной безопасности.

Указанная проблема является одной из основных. Все остальные вопросы так или иначе выступают в качестве ее следствий. Для ее преодоления важно решить следующие задачи: 1) повысить квалификацию персонала в области защиты информации путем проведения специальных собраний, семинаров; 2) повысить уровень информированности персонала, в частности о стратегических задачах, стоящих перед организацией.

Проблема 2. Противостояние службы автоматизации и службы безопасности организаций. Это вечная проблема, которая обусловлена родом деятельности и сферой влияния и ответственности этих структур внутри предприятия. Суть проблемы в том, что реализация системы защиты – в руках технических специалистов, а ответственность за ее защищенность лежит на

службе безопасности. Специалисты службы безопасности хотят во что бы то ни стало ограничить при помощи межсетевых экранов весь трафик. Но люди, работающие в отделах автоматизации, не желают решать дополнительные проблемы, связанные с обслуживанием специальных средств. Такие разногласия не лучшим образом сказываются на уровне защищенности всей организации.

Решается эта проблема, как и большинство подобных, чисто управленческими методами. Важно, во-первых, иметь в организационной структуре фирмы механизм решения подобных споров. Например, две «враждующие» службы могут иметь единое начальство, которое будет решать проблемы их взаимодействия. Во-вторых, технологическая и организационная документация должна четко и грамотно делить сферы влияния и ответственности подразделений.

Проблема 3. Личные амбиции и взаимоотношения на уровне руководителей среднего и высшего звена. Взаимоотношения между руководителями могут быть разными: и хорошими, и плохими, и «никакими». Бывает, что при проведении работ по исследованию информационной защищенности то или иное должностное лицо видит личную заинтересованность в результатах этих работ. И оказывается прав: действительно, исследования – это достаточно сильный инструмент для решения собственных проблем и удовлетворения амбиций. Выводы и рекомендации, записанные в отчете, используются как руководство к дальнейшим действиям. Они имеют большой вес, в особенности если работы проводились независимыми экспертами. Таким образом, после завершения работ и включения «нужных» выводов в отчет, появляется хорошая возможность опереться на него при случае. Возможна также и «вольная» трактовка выводов отчета в сочетании с проблемой 5, описанной ниже. Такая ситуация является крайне нежелательным фактором, так как искажает смысл проведения работ и требует своевременного выявления и ликвидации на уровне высшего руководства предприятия. Наилучшим вариантом являются деловые взаимоотношения, когда во главу угла ставятся интересы организации, а не личные.

Проблема 4. Низкий уровень исполнения намеченной программы действий по созданию системы защиты информации. Это достаточно банальная ситуация, когда стратегические цели и задачи теряются на уровне исполнения. Все может начинаться идеально. Генеральный директор принимает решение о необходимости совершенствования системы информационной безопасности. Нанимается независимая консалтинговая фирма, выполняющая аудит существующей системы защиты информации. По окончании формируется отчет, включающий все необходимые рекомендации по защите информации, доработке существующего документооборота в области информационной безопасности, по внедрению технических средств защиты информации и организационных мер, дальнейшей поддержке созданной системы. План защиты включает краткосрочные и долгосрочные мероприятия. Далее рекомендации передаются на исполнение в одно из подразделений. И здесь важно, чтобы они не утонули в болоте бюрократии, личных амбиций,

нерасторопности персонала и десятке других причин. Исполнитель может быть плохо проинформирован, недостаточно компетентен или просто не заинтересован в выполнении работ. В интересах того же генерального директора проконтролировать выполнение намеченного плана, дабы не потерять, во-первых, средства, вложенные в безопасность на начальном этапе, во-вторых, чтобы не понести потери в результате отсутствия этой безопасности.

Проблема 5. Низкая квалификация специалистов по защите информации. Данный аспект можно не считать серьезным препятствием, если он не является преградой на пути создания системы защиты информации. Дело в том, что в план защиты, как правило, включается такое мероприятие, как повышение квалификации специалистов в области защиты информации в компании. Для специалистов других служб могут проводиться семинары по основам организации защиты информации. Нужно верно оценивать реальную квалификацию сотрудников, занимающихся исполнением плана защиты. Зачастую неверные выводы или неумение применять методы защиты на практике приводят к сложностям при реализации рекомендованных мероприятий. При намеке на такие обстоятельства самым правильным выходом будет повышение квалификации специалистов по защите информации в специально созданных для этого центрах обучения.

В принципе, процесс повышения квалификации должен быть непрерывным, так как меняется уровень технологических решений в автоматизированные системы, меняются подходы к обеспечению безопасности и, что особенно важно, меняется политика безопасности конкретной фирмы по мере ее развития.

В заключение, приведем основные выводы данной главы. Практическая деятельность в области повышения экономической и информационной безопасности наглядно демонстрирует, что создание реально действующей системы защиты информации оказывается в сильной зависимости от своевременного решения перечисленных проблем. Однако накопленный опыт подсказывает, что все рассмотренные вопросы успешно решаются при условии плотной совместной работы представителей заказчика и фирмы-исполнителя. Главное – осознать важность проведения таких работ, своевременно выявить существующие угрозы и применить адекватные меры противодействия, которые, как правило, специфичны для каждого конкретного предприятия. Наличие желания и возможностей является достаточным условием для плодотворной работы, целью которой стало бы создание комплексной системы обеспечения безопасности организации.