УДК 334.02:65.011.56

Источники возникновения и последствия реализации угроз информационной безопасности промышленных предприятий

Канд. экон. наук, доцент **Балановская А.В.** balanovskay@mail.ru
Самарский государственный экономический университет
443090, РФ, г. Самара, ул. Советской армии 141

В статье дана характеристика современному состоянию угроз информационной безопасности предприятий. Особое внимание уделено проблеме утечки информации. Проанализированы тенденции, характерные для утечки информации в современных условиях функционирования промышленных предприятий. Выявлены источники утечки информации и наиболее часто используемые нарушителями каналы утечки информации. Приведена сравнительная характеристика видов информации, в отношении которой наиболее часто осуществляются преступные действия с ожидаемыми опасениями руководства или собственника. Изучены особенности и свойства информации промышленных предприятий, обладающей набором определенных свойств, которые следует учитывать в процессе разработки модели управления угрозами с целью обеспечения информационной безопасности. В качестве основополагающего свойства информации выделена конфиденциальность. В целях сохранении данного свойства особое внимание уделено рассмотрению внешних угроз, связанных с разведывательной деятельностью ряда субъектов. Рассмотрены основные структурные элементы шпионажа и их взаимосвязь, изучены методы промышленного шпионажа. Подробно отражена оценка эффективности применения различных методов промышленного шпиона в современных условиях. Также затронут такой важный аспект проблемы обеспечения информационной безопасности как возможные последствия влияния информационных угроз на деятельность промышленных предприятий.

Ключевые слова: информация; информационная безопасность; информационная система; информационные угрозы; утечка информации; промышленный шпионаж; система информационной безопасности.

Sources of emergence and consequence of realization of threats of information security of the industrial enterprises

Ph.D. **Balanovskaya A.V.** balanovskay@mail.ru
Samara State University of Economics
Samara 443090 Russia 141 Sovetskoi Armii St.

In article the characteristic is given to a current state of threats of information security of the enterprises. The special attention is paid to an information leakage problem. Tendencies, characteristic for information leakage in modern operating conditions of the industrial enterprises are analysed. Sources of information leakage and channels of information leakage which are most often used by violators are revealed. The comparative characteristic of types of information concerning which criminal acts with the expected fears of the management or the owner are most often carried out is provided. Features and properties of information of the industrial enterprises possessing a set of certain properties which should be considered in the course of development of model of management of threats for the purpose of ensuring

information security are studied. As fundamental property of information confidentiality is marked out. For preservation of this property the special attention is paid to consideration of the external threats connected with prospecting activity of a number of subjects. The basic structural elements of espionage and their interrelation are considered, methods of industrial espionage are studied. The assessment of efficiency of application of various methods of the industrial spy is in detail reflected in modern conditions. Also will mention such important aspect of a problem of ensuring information security as possible consequences of influence of information threats on activity of the industrial enterprises.

Keywords: information; information security; information system; information leakage; industrial espionage; information threats; information security system.

Стратегия развития промышленных предприятий приводит к необходимости диверсификации производства, проникновению на новые для предприятия рынки сбыта, решению вопросов повышения эффективности взаимодействия с поставщиками и потребителями, созданию различных подразделений в структуре самой организации, что в итоге порождает постоянное усложнение и совершенствование информационной системы с необходимостью применения новых информационных технологий (ИТ). Наравне с построением современной автоматизированной информационной системы существенно возрастает вероятность различного рода угроз, которые являются источником нарушения и направлены на подрыв информационной безопасности (ИБ) промышленного предприятия.

Под информационной угрозой предприятия понимают потенциально существующую опасность случайного (непреднамеренного) или преднамеренного нарушения качества информации, обусловленного особенностями ее хранения, обработки и использования. Информация в основном хранится и обрабатывается при помощи автоматизированных информационных систем, а значит, результат деятельности промышленного предприятия находится в зависимости от устойчивости функционирования этих систем и защищенности от действий злоумышленников и конкурентов. Так, 73% руководителей специализированных служб (ИТ- и ИБ-службя) и более 77% сотрудников данных служб выразили сомнение относительно надежности организационных систем обеспечения информационной безопасности, которые в настоящее время функционируют на их предприятиях. Данное мнение подтверждается также и статистикой. В 2014 году официально подтверждено (в СМИ и других источниках) и зарегистрировано Аналитическим центром InfoWatch 1395 случаев утечки конфиденциальной информации, что на 22 п.п. превышает число утечек, зарегистрированных в 2013 году, тогда как по России данное увеличение составило 73 п.п. [11]. Динамика роста количества утечек приведена на рис. 1.

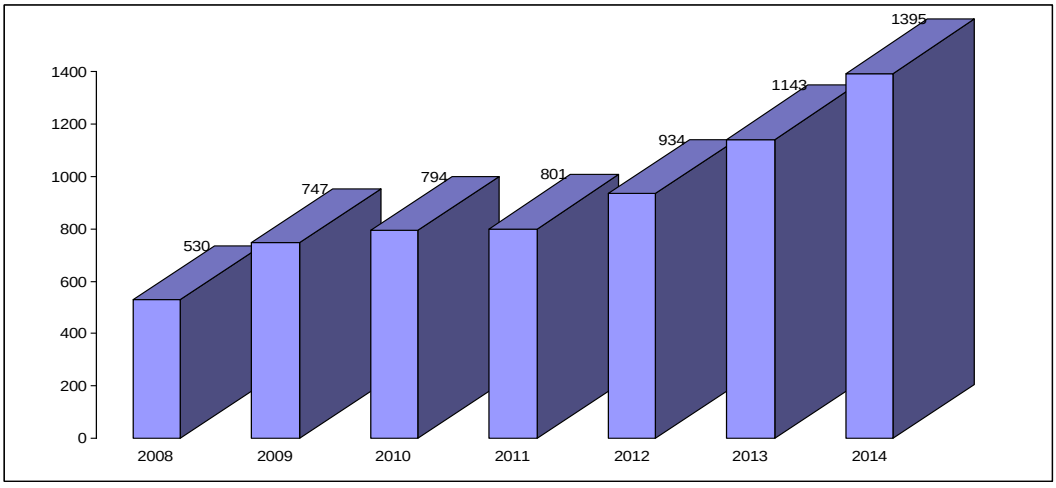

Рис. 1. Количество случаев утечки конфиденциальной информации, ед.

За последние пять лет количество случаев утечки конфиденциальной информации увеличилось более чем на 75 п.п. На сегодняшний день угрозы информационной безопасности очень разнообразны. Однако при систематизации всех потенциальных угроз безопасности выделяют два основных класса: естественные (объективные) и искусственные (субъективные). Естественные угрозы - это угрозы, вызываемые воздействием на информационную систему промышленного предприятия и ее компоненты объективных физических процессов или стихийных природных явлений, независящих от субъекта (человека). Искусственные угрозы – это угрозы, вызванные деятельностью человека. Среди искусственных угроз по мотивам к действию выделяют: непреднамеренные (случайные, неумышленные) угрозы, которые вызваны различными возможными ошибками в проектировании информационной системы, в программном обеспечении, в действии персонала и т.п.; преднамеренные (умышленные) угрозы, связанные с корыстными, идейными и другими устремлениями людей (нарушителей).

Безусловно, наибольшую опасность представляют искусственные угрозы. Ежедневно экспертами Лаборатории Касперского обрабатывается около 315 тысяч образцов вредоносного программного обеспечения. По результатам проведенного «Лабораторией Касперского» опроса только 4% респондентов имеют объективное представление о количественных оценках ежедневных новых образцов, 5% переоценили данную угрозу и, следовательно, более 90% респондентов существенно ее недооценивают [10].

С позиции возможного ущерба наиболее опасными и самыми частыми исследователями называются непреднамеренные ошибки постоянных сотрудников. Именно такие ошибки очень часто и создают уязвимые места для действия различных внешних угроз. Непреднамеренные ошибки, в среднем, по мнению экспертов приносят 60-65% потерь. Тогда как на долю стихийных бедствий приходится не более 13% всех потерь от угроз информационной безопасности.

Самым распространенным последствие реализации информационных угроз становится утечка конфиденциальной информации. Распределение утечек по долям выглядит следующим образом (рис. 2)

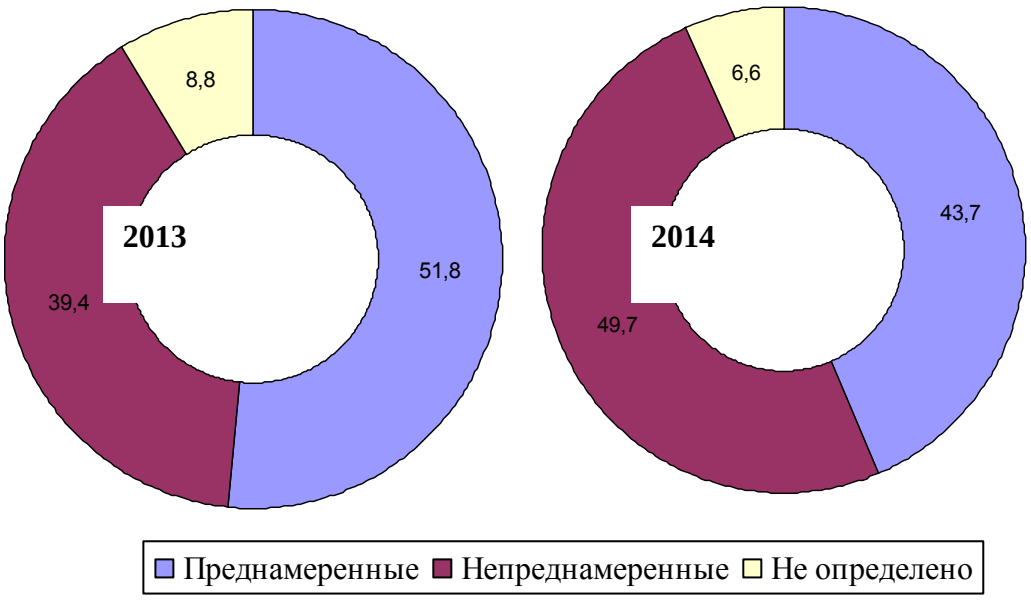

Рис. 2. Распределение утечек информации по долям, %

Значительную угрозу представляют так называемые «обиженные» сотрудники, работающие в данный момент на предприятии или уволенные. Поскольку бывшие работники знакомы с организацией работы на предприятии, то важным при увольнении является аннулирование права доступа к

информации для этих сотрудников. Очень часто они имеют возможность удаления каких-либо данных, порчи оборудования или встраивания так называемой «бомбы», которая в результате приводит или к разрушению данных программ, или получению контроля над системой, или внедрению другого вредоносного программного обеспечения.

Распределение источников утечек информации представлено на рис. 3

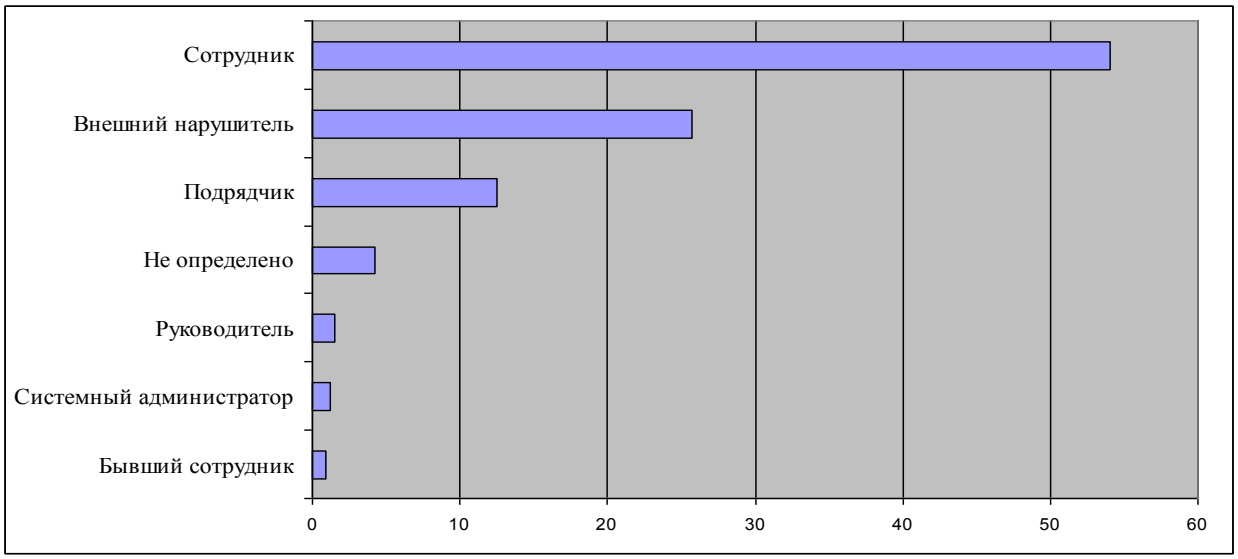

Рис. 3. Распределение источников утечек информации на предприятии, %

Больше чем в половине случаев виновниками утечки информации становились реальные (54%) или бывшие сотрудники (1%) предприятия. Достаточно большая доля (4%) утечек приходилась на подрядчиков, чей персонал имел доступ к конфиденциальной информации и по сути утечка происходила на стороне подрядчика. Зафиксирована и вина высшего и среднего руководства предприятий (топ-менеджмент, руководители отделов и подразделений). Аналогичный вклад вносят и системные администраторы, являющийся пользователями с расширенными правами доступа к информации.

В распределении по характеру действий нарушителей основная доля приходится на «классическую» утечку, заключающуюся в потере контроля над информацией. Однако 7,8% случаев зарегистрированных инцидентов классифицированы как нарушения, сопряженные с получением несанкционированного доступа к информации и 12% классифицированы как мошенничество с использованием данных [11].

По типу информации, в отношении которой совершаются мошеннические действия и информацией, которую предприятие в большей степени опасаются утратить, наблюдается ряд отличий.

Виды информации, которую чаще всего крадут нарушители представлены на рис. 4.

Рис. 4. Информация, в отношении которой совершают действия нарушители, %

По опросу проведенному Лабораторией Касперского, предприятия чаще всего вынуждены утратить свою внутреннюю операционную информацию, о чем указали 56% респондентов. Остальные категории информации, которые становятся объектом действий нарушителей, это персональные данные сотрудников, информация о клиентах и финансовая информации. Они указывались респондентами в 25% случаев.

Виды информации, которую предприятия опасаются утратить представлены на рис. 5.

Рис. 5. Виды информации, с наибольшей степенью опасения утраты

Российские предприятия наиболее опасаются утратить клиентскую базу и прочую информацию о клиентах и заказчиках, по мнению 21% респондентов. Немного менее опасаются потерять финансовую информацию (19%), внутреннюю операционную информацию (15%). При этом следует отметить, что внутренняя операционная информация фактически становится объектом кражи в значительно большем количестве случаев [10].

В целом следует отметить, что опасения предприятий вполне совпадают с фактическими угрозами. Предприятия относительно адекватно оценивают риски информационной безопасности. В

результате, принятие своевременных защитных мер в отношении той или иной категории информации приводит к существенным структурным сдвигам при рассмотрении данного аспекта в динамике.

Особенно важном является изучение утечек в разрезе каналов потери информация (рис. 6).

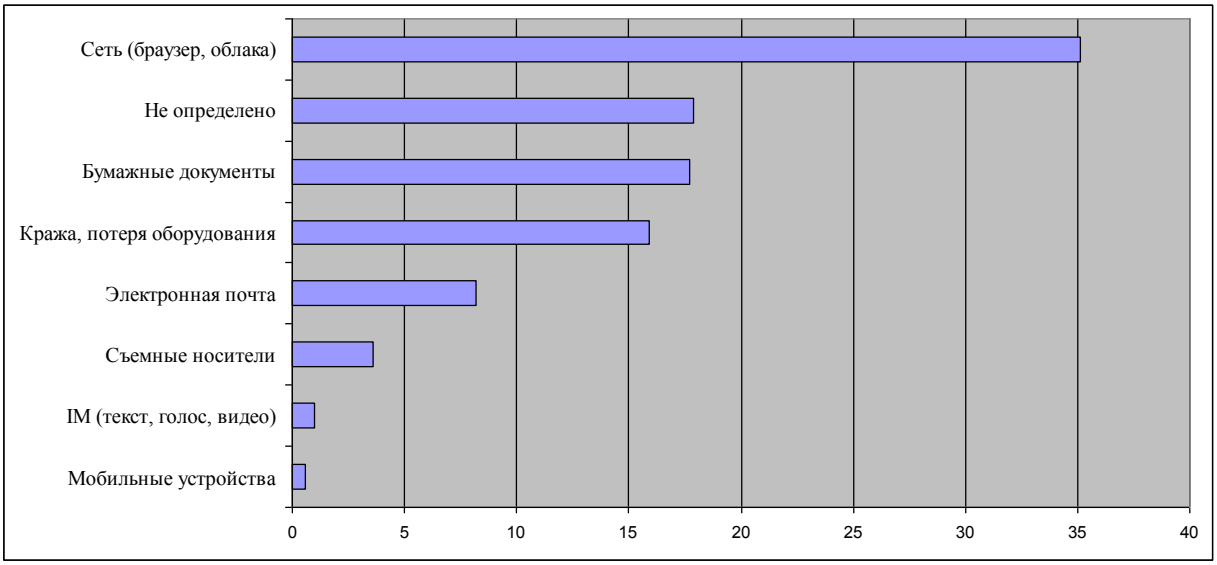

Рис. 6. Каналы утечки информации

В динамике наметилась тенденция все меньшего использования «традиционных» каналов. Нарушители такие каналы перестали использовать в связи с высокой эффективностью функциональных возможностей защитных решений, используемых на предприятиях, о которых они хорошо осведомлены. Основная доля утечек в 2014 году приходилась на три основных канала: Интернет (35%), бумажные документы (18%) и кража, потеря оборудования (16%). Через Интернет как правило происходят преднамеренные утечки. А непреднамеренные утечки происходят при потере, краже документов или оборудования.

Подробное исследование возможных каналов утечек информации носит сугубо практическое значение, т.к. с большой эффективностью помогает выявить уязвимые места, определить и внедрить набор средств защиты [11],

Как правило, на промышленных предприятиях в защите нуждаются два типа информации, которая подпадает под категорию служебной или коммерческой тайны:

- информация, составляющая научно-технологические сведения, связанные непосредственно с конструкторской и технологической документацией, сведения об используемых материалах, а также описание методов и способов производства новых изделий, уникальный программный продукт;
- информация, составляющая деловые сведения о деятельности учреждения: финансовая документация, перспективные планы развития, направления модернизации производства, аналитические материалы об исследованиях конкурентов и эффективности работы на рынках товаров и услуг, различные сведения о партнерах и др.

Именно эти два типа сведений становятся чаще всего объектом компьютерных преступлений. Под этим термином понимаются преступления в области компьютерной информатики. История их ведется примерно с 1960-х гг. с выявления в США первых случаев компьютерных преступлений, совершенных с использованием ЭВМ. В РФ эти преступления впервые были предусмотрены Уголовным Кодексом в 1996 г. В научный оборот вошли такие термины как информационные преступления, компьютерные преступления в сфере компьютерной информации.

Мещеряков В.А. классифицировал следующим образом информационные преступления [12]: а) неправомерное завладение информацией или нарушение исключительного права ее использования; б) неправомерная модификация информации; в) разрушение информации; г) действие или бездействие по созданию информации с заданными свойствами; д) действия, направленные на создание препятствий пользования информации законным пользователем.

Из года в год увеличивается количество преступлений в сфере информационных технологий. Из них 70% связано с несанкционированным доступом к информации. На практике более часто информационные угрозы классифицируют исходя из их воздействия на основные свойства информации. Рассматривая данную проблему в качестве основных свойств информации автор выделил: значимостью, уязвимость, целостность, доступность и конфиденциальность информации [2].

Поскольку значимость информации является основным свойством, служащим предпосылкой к применению информационных ресурсов в бизнесе, то целесообразно рассматривать защиту данного свойства информации от негативных воздействий, реализующихся опосредованно через целостность, конфиденциальность и доступность. Если значимость информации теряется при изменении или уничтожении информации, то говорят, что имеется угроза целостности информации. Целостность информации можно подразделить на статическую, понимаемую как неизменность информационных объектов, и динамическую, относящуюся к корректному выполнению сложных действий. Практически все нормативные документы и отечественные разработки относятся к вопросу статической целостности, в то время как ее динамический аспект не менее важен.

Основные угрозы целостности информационных ресурсов предприятия: а) пожары, наводнения и иные стихийные бедствия (форс-мажорные обстоятельства); б) хищения, утраты и модификация документов или технических средств, поддерживающих информационную систему организации; в) сбои в работе автоматизированных систем обработки и передачи информации; г) информационный терроризм и хулиганство; д) фильтрация информации в каналах внутренних коммуникаций организации [7].

Форс-мажорные обстоятельства, хищения, утраты или модификация, нарушают безопасность носителей информации и могут являться элементом недобросовестной конкуренции, который обеспечит временное конкурентное преимущество, парализовав работу оппонента. Причиной возникновения сбоев в автоматизированных системах обработки, передачи и хранения информации этого вида угроз выступает само оборудование (машинный фактор) и персонал (человеческий фактор). Причем негативное влияние человека на целостность информации может проявляться в двух видах [14]:

– пассивные угрозы, т.е. вызванные человеческой деятельностью, носящей непреднамеренный, случайный характер (ошибки операторов автоматизированных информационных систем, обусловленные низким уровнем квалификации персонала, неграмотным и несвоевременным обслуживанием оборудования, некорректным вводом, модификацией и обработкой данных в системе;
– активные угрозы, т.е. обусловленные умышленными и преднамеренными действиями людей.

Фильтрация чаще всего касается акустической информации, т.е. информации, обращающейся в устной форме, и заключается в случайном или преднамеренном искажении содержания сведений, т.е. нарушении их целостности. Случайное искажение содержания информации возникает из-за отсутствия взаимопонимания между отправителем и получателем информации, в то же время фильтрация может носить преднамеренный характер, если пользователи информации имеют различные взгляды на ее ценность и необходимость для процесса управления. Чаще всего преднамеренная фильтрация происходит при общении между сотрудниками и руководством предприятия, когда служащие пытаются скрыть объективную информацию, которая негативно отразится на их положении на предприятии [4].

Основная угроза целостности информации заключается в ошибочных действиях ее владельцев или пользователей (52%), и лишь в 25% случаев угроза данному свойству информации исходит от нарушителя [3].

С целостностью информации тесно связано понятие актуальности и непротиворечивости информационных ресурсов. Объективно ценность информации напрямую зависит от степени ее соответствия действительности, поэтому одна из главных информационных угроз развитию предприятия – это опасность утраты актуальности информационных ресурсов. Процесс актуализации собственных информационных ресурсов представляется одной из первостепенных задач, стоящих перед службой безопасности предприятия, поскольку позволяет сохранять или увеличивать имеющееся конкурентное преимущество в экономической деятельности перед другими субъектами рынка.

В случае, когда ценность информации утрачивается при ограничении оперативности ее использования, то говорят, что имеется опасность нарушения доступности информации. Проблема обеспечения доступности информации – одна из важнейших составляющих информационной безопасности предприятия. Причина важности роли доступности информации в обеспечении устойчивого развития предприятия по информационной составляющей кроется в двух факторах:

– информация – организационный ресурс ведения бизнеса, что подразумевает ее обязательное использование в основных видах деятельности предприятия, кроме того, информация посредством процесса коммуникации позволяет руководству предприятия организовывать, планировать и контролировать финансово-экономическую жизнь предприятия. Доступность информации подразумевает ее оперативное использование для нужд предприятия, при этом сохраняется важное качество информации – актуальность;
– проблема доступности информационных ресурсов тесно связана с проблемами разграничения открытых и конфиденциальных массивов информации. Процесс обеспечения конфиденциальности информации не должен нарушать ее доступности для авторизированных пользователей.

Внутренние угрозы нарушения доступности информации могут носить процедурный характер (внедрение на предприятии необдуманно жестких систем контроля доступа к конфиденциальной информации), технический или машинный характер (нарушение доступа вследствие отказа или сбоев в работе оборудования автоматизированных информационных систем). В то же время ситуации, когда пользователь не получит доступа к законно выделенным ему службам или ресурсам, могут быть спровоцированы извне, что подразумевает умышленный агрессивный характер этих угроз.

Следующим важным моментом обеспечения информационной безопасности предприятия является обеспечение ее конфиденциальности. Угрозы конфиденциальности информации возникают при нарушении ее ценности в результате несанкционированного ознакомления с ее содержанием. Основным пространством концентрации инициаторов угроз конфиденциальности информации служит внешняя среда предприятия. Одной из главных внешних угроз массивам конфиденциальной информации предприятия в современном мире является разведывательная деятельность государств и других субъектов рынка. На рис. 7 приведены структурные элементы различных видов разведки (шпионажа) и их взаимосвязь.

Рис. 7. Основные структурные элементы шпионажа и их взаимосвязь

В основании «пирамиды» шпионажа лежит промышленный шпионаж, т.е. деятельность, направленная на овладение рынками сбыта, подделку товаров, дискредитацию или устранение конкурентов, срыв переговоров по контрактам, перепродажу фирменных секретов, шантаж определенных лиц, ущерб от которой для деятельности предприятий огромен.

Методы промышленного шпионажа различны, но их можно объединить в две основные группы: технические методы шпионажа, подразумевающие широкое применение различных технических средств съема, перехвата, ложной маршрутизации информации; шпионаж с использованием людей (сотрудников предприятия, криминальных элементов и т.д.), данный вид шпионажа предполагает подкуп или иное склонение служащих предприятия к сотрудничеству с нарушителями, а также элементарное хищение документов и других материальных носителей конфиденциальной информации [1].

Эффективность разных способов промышленного шпионажа, по данным экспертов Европейского Союза, приведена на рис. 8 [13].

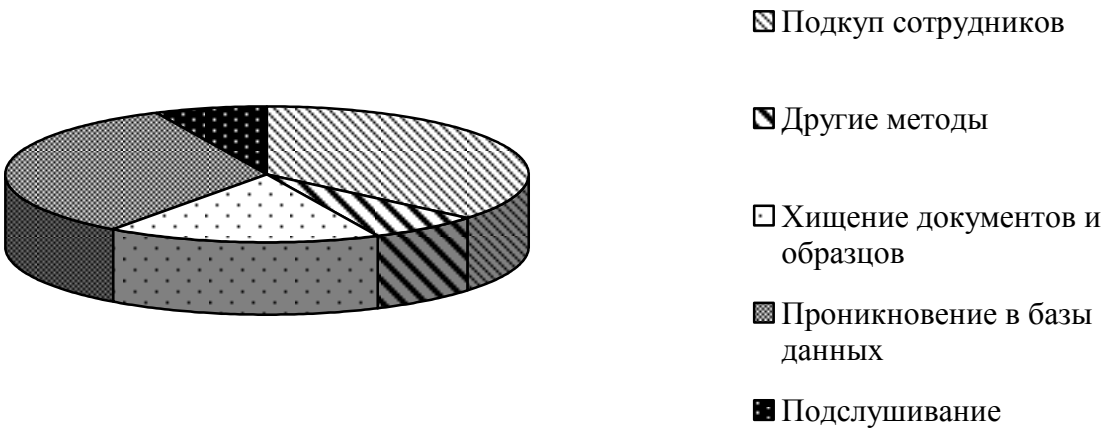

Рис. 8. Эффективность способов промышленного шпионажа

В связи с угрозой промышленного шпионажа возникает необходимость обеспечения информационной безопасности управленческой информации. Перечень и классификация возможных угроз информационной безопасности сами по себе тривиальны, давно разработаны и могут иметь тысячи названий в зависимости от степени детализации. Тем не менее, проблема формирования конкретной модели угроз является важнейшей основой для организации всей дальнейшей работы по обеспечению информационной безопасности конкретного предприятия.

Модель угроз может быть описана только после построения модели злоумышленника (нарушителя), которая, в свою очередь, определяется сутью ценности защищаемого актива, приоритетами безопасности и собственно данными субъектов угроз. Практически любой информационный комплекс легко подвергается многоуровневой вертикальной структуризации, в результате чего в системе выделяются семь уровней: физический (уровень каналов связи), сетевой, сетевых приложений, операционных систем, СУБД, приложений, бизнес-процессов. Исключительно важным при построении модели угроз является признание того, что на каждом из перечисленных уровней угрозы, их источники (в том числе нарушители), методы, средства защиты и подходы к оценке эффективности являются различными. Каждое промышленное предприятие должно определить конкретные объекты защиты на каждом из уровней информационной инфраструктуры [5].

Исключительно важным является вопрос приоритета при выборе конкретного набора актуальных угроз. Таким приоритетом в общем случае является вес, или весовой коэффициент угрозы, измеряемый вероятностью ее реализации. Именно вероятности реализации угроз являются наиболее подвижной и быстроизменяющейся составляющей проблемы, радикально влияющей на формирование политики безопасности промышленного предприятия. Сама по себе угроза не несет никакой опасности, она является, только предположением о возможной опасности и не более того.

Однако на практике дело обстоит гораздо сложнее. Защищающаяся сторона должна решить, по крайней мере, две задачи. Первая задача заключается в оценке так называемой возможности реализации предполагаемой угрозы, а вторая - в оценке возможных затрат, всегда возникающих при применении средств защиты.

Оценка возможности реализации угрозы зависит от многих факторов. Во многих источниках возможность реализации угрозы определяется как некоторая вероятность. Если бы это было так, то многие проблемы были бы сняты, так как, проведя математические расчеты и используя понятие и меру риска, ошибиться, например, на величину 0,001, можно было бы достаточно уверенно себя чувствовать в плане прогнозирования реализации угрозы. Однако на деле не все так просто. Обратим внимание на ряд определений, введенных в ГОСТ Р 51897 [8]. В этом стандарте определено понятие риска как «сочетание вероятности события и его последствий». Конечно, проблема риска и его оценки является

отдельной задачей, поэтому было бы целесообразно посмотреть, какой смысл вкладывается в понятие вероятности. В данном ГОСТ вероятность определяется как «мера того, что событие может произойти». Также делается ссылка на ГОСТ Р 50779.10 [9], в котором вероятность определяется как «действительное число от 0 до 1, относящееся к случайному событию. Число может отражать относительную частоту в серии наблюдений или степень уверенности в том, что некоторое событие произойдет». Таким образом, возможность реализации угрозы, определяемая через понятие вероятность, содержит две составляющие, одна из которых определяет частотность событий, а вторая – степень уверенности, что событие произойдет.

Первая составляющая, определяющая частотность событий, достаточно хорошо проработана в классической теории вероятностей. Пример решения такой задачи – расчет вероятности попадания хотя бы одного артиллерийского снаряда в цель при проведенном залпе при известной статистике вероятности попадания одного снаряда в цель. Как видно, это расчет, основанный на статистике. Безусловно, статистику в данном случае можно приравнять к материализации опыта, и она должна быть использована. Однако есть вторая составляющая, определяемая как степень уверенности, которую следует отнести к субъективным факторам оценки. Эта составляющая введена из-за невозможности в общем виде ориентироваться на имеющуюся статистику ввиду существенных различий сферы действий в бизнесе и разных платформ оценки риска, в рассматриваемом случае выступающей в виде оценки возможности реализации угрозы.

Гораздо глубже позиции по оценке возможностей наступления событий раскрываются в стандарте AS/NZS 436:2004 [15]. В данном стандарте понятие оценки возможности через принятие риска интерпретируется в терминах «опасности или негативных воздействий», а риск трактуется как «раскрытие последствий неопределенности или потенциальных отклонений от запланированного или ожидаемого». В связи с этим в стандарте помимо использования классического понятия вероятности как относительной величины появления событий в серии испытаний вводится новое понятие «правдоподобие» как общее описание вероятности или частоты, определяемое как качественно, так и количественно.

Можно сделать вывод о том, что угроза, являющаяся источником потенциального ущерба, а потому представляющая некоторую опасность, каким-либо образом должна быть измерена. Фактически, речь идет уже о формировании модели угроз.

Безусловно, измерение угрозы следует начать с оценки возможности ее возникновения. Такая оценка может быть сделана на основе данных по известным фактам появления угрозы, выраженным через статистическую частотность. Данную оценку можно рассматривать как оценку, основанную на имеющемся опыте эксплуатации. Кроме этого на практике имеет место как субъективная оценка, сущность которой определяется как особенностью бизнеса, так и субъективной оценкой собственником возможного проявления опасностей – угроз. Субъективизм оценки, в частности, может проистекать из изменений отношений к весомости той или иной угрозы из-за изменения среды функционирования объекта, условий работы и особенностей защищаемого объекта. Например, с 1950-х гг. до сегодняшнего дня произошли существенные изменения в практике реализации защиты входных дверей в наших квартирах. На смену незащищенным деревянным дверям с простыми замками пришли металлические двери со сложными замками. Объясняется это изменением отношения к уязвимости, в частности, вследствие роста квартирных краж, увеличения стоимости ресурсов, хранящихся в квартире, а также расширения технических возможностей взломщиков.

Вторым фактором оценки возможности реализации угрозы является оценка затрат, неизбежно возникающих при введении тех или иных средств защиты. Правильнее было бы сказать «ущерб» – урон, который понесет собственник, а не «затраты». Урон может выражаться не только экономическим ущербом, нанесенным в текущий промежуток времени, но и в виде других ущербов, например репутации, которые могут привести к более существенным уронам в будущем. При внедрении средств

защиты производятся затраты не только на приобретение средств, но и на их текущее обслуживание. Введение средств защиты снижает возможность реализации одной или группы угроз, уменьшая ущерб от реализации. Как правило, оптимальный вариант соотношения «затраты на покупку и эксплуатацию средств защиты – возможный ущерб от реализации угроз» определяется собственником. Например, возможен выбор таких защитных мер, реальные затраты на реализацию которых будут находиться на одном уровне с потерями, которые может понести собственник при реализации оставшихся угроз [6]. Превышение затрат по сравнению с оптимальным уровнем, безусловно, уменьшает возможности реализации новых угроз, но в общем балансе «ущерб – затраты» последние могут стать излишне высокими.

Над путями практического поиска этого оптимума продолжают работать и в настоящее время, однако все решения по данному вопросу носят характер общеметодологических рекомендаций. Вряд ли в ближайшее время можно ожидать точных практических рекомендаций по этому вопросу, что связано с большим числом субъективных факторов. Современная философия выбора защитных мер основана на решении собственника, который обеспечивает выбор, в частности, на базе определения опасного для себя перечня угроз, которые по его представлению могут привести к существенным потерям. На такой философии построены наиболее применяемые в настоящее время стандарты. Переход на применение строго регламентированных средств защиты, ориентируемых на определенный уровень защиты, как философия, которая продолжает функционировать в России на основе действующих руководящих документов, безусловно, существенно упрощает расчет затрат, однако такой подход в бизнес-организациях признан в мире как устаревший и непригодный. Поскольку собственники определяют опасные угрозы на основе объективных и субъективных факторов, деятельность по их оценке является неизбежной и крайне необходимой. Участие собственников в процессе признания и утверждения состава угроз крайне желательно, так как это позволит быстрее решить вопрос финансирования затрат на реализацию защитных мер.

Список литературы

1. *Ашмарина С.И., Татарских Б.Я.* Эффективность использования информационных ресурсов промышленного предприятия. Саратов: Изд-во Сарат. ун-та, 2002. 206 с.

2. *Балановская А.В.* Анализ угроз информационной безопасности деятельности промышленных предприятий // Вестник Самарск. муниц. инст. упр. №2. 2013. С. 7-18.

3. *Балановская А.В.* Модель угроз информационной безопасности промышленных предприятий // Вестник Самарск. гос. экон. ун-та. 2011. №9. С. 19-24.

4. *Балановская А.В.* Управление рисками в реализации политики информационной безопасности промышленного предприятия. Управление экономическими системами: сборник статей IV Международной научно-методической конференции. Пенза: Приволжский Дом знаний, 2012. С. 9-11.

5. *Балановская А.В., Казакова А.В.* Организационные механизмы разработки и управления информационной безопасностью промышленных предприятий. Самара: Изд-во Самар. ин-та упр., 2010. 138 с.

6. *Волкодавева А.В., Балановская А.В.* Организационно-экономические механизмы обеспечения эффективности управления информационной безопасностью промышленных предприятий. Самара, САГМУ, 2012. 248 с.

7. *Волкодаева А.В.* Проектирование эффективной системы информационной безопасности предприятия // Вестник Самарск. муниц. инст. упр. 2015. №2. С. 7-18.

8. ГОСТ Р 51897-2011 «Менеджмент риска. Термины и определения». Госстандарт России, 2002. 12 с.

9. ГОСТ Р 50779-2000. Статистические методы. Вероятность и основы статистики. Термины и определения [Электронный ресурс]. URL: http://www.gosthelp.ru (дата обращения: 20.07.2015).

10. Информационная безопасность бизнеса [Электронный ресурс]. URL: http://www.kaspersky.ru/protect-my-business/it-risk-report?icid=ru_RU:vsbdiscover (дата обращения: 15.07.2015).

11. Исследование утечек конфиденциальной информации в 2014 году. [Электронный ресурс]. URL: http://www.infowatch.ru/report2014 (дата обращения: 18.07.2015).

12. *Мещеряков В.А.* Криминалистическая классификация преступлений в сфере компьютерной информации // Конфидент. 1999. № 4-5. С. 67-72.

13. *Соловьев Э.Я.* Коммерческая тайна и ее защита. М., Ось - 89, 2001. 128 с.

14. Справочник директора предприятия / под ред. М.Г. Лапусты. М., Инфра-М, 2001. 750 с.

15. HB 436:2004. Руководство по риск-менеджменту. Справочник по AS/NZS 4360:2004. Jointly published by Standards Australia International Ltd. and Standards New Zealand, 2004.

Статья поступила в редакцию 28.07.2015 г.