# Доклад по предмету «Основы безопасности бизнеса»

# БЕЗОПАСНОСТЬ БИЗНЕСА В СТРАНАХ СЕВЕРНОЙ ЕВРОПЫ

В силу своего географического положения, традиций, обычаев и довольно близких языковых систем и норм законодательства в странах Северной Европы отмечается достаточно много общих подходов к организации частной правоохранительной деятельности, которые и будут предметом изучения в данном разделе.

## ФИНЛЯНДИЯ

### 1. ЧАСТНЫЕ ОХРАННО-СЫСКНЫЕ БЮРО

1.1. Нормативная база. В Финляндии органами законодательной власти определены весьма четкие правовые границы для деятельности частных сыскных и охранных бюро. Это нашло отражение в двух основных законодательных актах: Законе о частном сыске и Законе о частных телохранителях.

Для открытия частных охранно-сыскных бюро требуется разрешение соответствующих органов исполнительной власти. Если деятельность бюро предполагается осуществлять в пределах административных границ одной губернии (области), то такое разрешение выдается губернатором.

Если с момента открытия бюро планирует проводить охранно-сыскные мероприятия одновременно в нескольких административных центрах (областях), то разрешение на открытие бюро выдается центральным исполнительным органом страны – правительством Финляндии.

1.2. Профессиональная подготовка кадров. Действующим законодательством Финляндии определены также общие требования к сотрудникам частных охранно-сыскных бюро, которые должны иметь:

* полицейское или юридическое образование;
* практический опыт работы в местных спецслужбах либо полиции;
* высокие моральные качества и благонадежность.

Все эти требования должны быть документально подтверждены кандидатом документами об образовании и состоянии здоровья, справкой с последнего места работы в государственном правоохранительном органе и, желательно, рекомендательным письмом с благоприятным для кандидата содержанием от уважаемого гражданина Финляндии либо известного местного эксперта по вопросам сыска, охраны или безопасности.

Кроме того, как отмечалось в предыдущих разделах, отделы кадров приступают после получения всех необходимых документов к их тщательной проверке, которая может сопровождаться продолжительными беседами с кандидатом по всем вопросам, требующим уточнений.

### 2. КОММЕРЧЕСКИЕ И ПРОМЫШЛЕННЫЕ СЛУЖБЫ БЕЗОПАСНОСТИ

Режимные меры по обеспечению сохранности коммерческой тайны и научно-технических секретов в отдельных фирмах и банках обеспечивают в Финляндии частные службы безопасности, которые в последние годы укреплены высококвалифицированными кадрами из числа бывших сотрудников полиции и контрразведки страны (СУПО).

2.1. Тактика деятельности. Для Финляндии характерен весьма высокий уровень взаимодействия СУПО с частными службами безопасности. Например, в соответствии с инструкцией, разработанной СУПО для частнопредпринимательских кругов, бизнесмен Финляндии после первой же встречи с иностранным коммерческим и иным представителем обязан:

* доложить о характере имевшей место беседы;
* указать, кто явился инициатором беседы, встречи или письменного запроса;
* охарактеризовать манеру поведения иностранного представителя;
* высказать собственные предположения относительно вероятных задач иностранного представителя при организации встречи;
* указать точное место и время контакта с иностранцем своему непосредственному руководителю или заместителю фирмы по кадровым вопросам;
* последний, в свою очередь, должен в течение суток связаться с СУПО.

В результате анализа ситуации сотрудники контрразведки Финляндии дают указание либо о прекращении контакта, либо о его продолжении, но уже под контролемСУПО. Согласно этой же инструкции после поездки в Россию сотрудники и специалисты частных фирм и служащие государственных учреждений Финляндии обязаны собственноручно подготовить по разработанномуСУПО вопроснику подробную справку, которая передается в контрразведку.

2.2. Подготовка кадров. Сотрудники фирм Финляндии, работающие, в первую очередь в так называемых «восточных» департаментах и отделах безопасности, обязаны проходить соответствующую стажировку в США, знакомиться с опытом американских коллег в частном правоохранительном секторе, а также с деятельностью государственных спецслужб, в частности ФБР, по контрразведывательному обеспечению объектов, располагающих экономическими и техническими секретами.

В последние годы некоторые фирмы Финляндии все чаще стали использовать в качестве своих представителей или посредников для ведения переговоров с российскими внешнеэкономическими организациями бывших советских граждан, среди которых выявлены лица, подозреваемые в связях с СУПО.

2.3. Функции сотрудника по вопросам безопасности, работающего в совместном с иностранным партнером обществе. Весьма активно соответствующие специалисты Финляндии осуществляют меры безопасности в совместных российско-финляндских обществах.

Так, в обществе «Тебойл» вопросами безопасности ведает квалифицированный местный сотрудник, который подозревается в связях с СУПО. Этот работник стремится взять под свой контроль любые контакты российских представителей в Финляндии как с местными гражданами, так и иностранцами. Он же стремится выявлять и возможные контакты граждан Финляндии в Российской Федерации, других государствах СНГ и в Прибалтике в случае выезда представителей этой страны за рубеж для коммерческих и иных переговоров.

На основе изученных оперативных материалов и опроса соответствующих специалистов автором разработана **методика обеспечения сохранности на совместном обществе (предприятии) коммерческой и производственной тайны,** а также проведения иных режимных и профилактических мероприятий, осуществляемых, как правило, специально выделенным для этих целей офицером (инспектором) но вопросам безопасности и режима.

Итак, помимо уже вышеизложенных в функции сотрудника данной категории входят также следующие задачи:

* контроль за выдачей служащим обществ любой информации в отношении местных фирм;
* выявление причин, природы и регулярности подобных запросов:
* наблюдение и опрос местных сотрудников обществ о периодичности, характере и особенностях контактов иностранных представителей, а также бизнесменов других стран с местными предпринимателями.

### 3. ВОПРОСЫ ПРАВОВОЙ ЗАЩИТЫ КОМПЬЮТЕРНЫХ ПРОГРАММ

В Финляндии в 90-е годы в связи с бурным развитием рынка компьютерных услуг приступили к решению проблем защиты прав авторов на компьютерные программы.

3.1. Роль предпринимательских организаций в совершенствовании законодательства о защите программного обеспечения компьютеров. Государственная промышленная палата Финляндии поставила перед правительством страны вопрос о неотложном совершенствовании законодательства об авторских правах на компьютерное программное обеспечение. Сформулированы основные аспекты компьютерного законодательства, которые необходимо внести в новый нормативный акт, регулирующий взаимоотношения между авторами программ и их пользователями по вопросу установления фактической собственности на программное обеспечение. В настоящее время вопрос о том, кто имеет право на владение программным обеспечением – разработчик или пользователь, остается открытым.

Высказано предложение о предоставлении составителям программ для компьютеров таких же авторских прав, как, например, писателям. Для разработки соответствующего нормативного акта изучены аналогичные законы, действующие в США, Франции, Великобритании, Японии, ФРГ и Швеции.

3.2. Перспективы юридической защиты интеллектуальной собственности в компьютерной сфере. Согласно данному предложению авторские права на программы сохраняются в течение того периода, который определяют сам разработчик и пользователи. Считается необходимым в связи с этим изменить действующее законодательство по авторским правам, в соответствии с которым право на патент или изобретение сохраняется в течение 50 лет после смерти изобретателя. Подобные сроки признаются, однако, многими юристами и экспертами неприемлемыми, поскольку даже самые универсальные программы теряют актуальность через несколько лет или даже месяцев.

В нормативном акте рассмотрены и такие важные аспекты, как обеспечение права собственности фирмы-пользователя на компьютерные программы в случае ее банкротства с тем, чтобы иметь возможность продать программу другому пользователю для погашения долга.

Предполагается, что в случае объединения усилий всех заинтересованных служб и ведомств новый Закон об авторском праве на компьютерные программы будет функционировать до конца нынешнего десятилетия.

Очевидно, что частные службы безопасности будут ориентироваться на эти нормы права и одним из вероятных направлений их деятельности в ближайшие годы станет выявление каких-либо нарушений авторских прав создателей компьютерных программ.

Кстати, автор не располагает какой-либо достоверной информацией о подобной деятельности российских детективных фирм и частных служб безопасности и не сталкивался пока с практикой частного расследования нарушений авторского права в нашей стране.

## ШВЕЦИЯ И ДАНИЯ

## 1. ЧАСТНЫЕ ОХРАННО-СЫСКНЫЕ БЮРО

В этих странах частные сыскные и охранные бюро относятся к категории частных предприятий. При этом имеется в виду то, что их учреждение, регистрация, финансирование, налогообложение и взаимоотношения с другими частными компаниями и государственными организациями, а также правовое положение и деятельность регламентируются общими основами действующего законодательства.

## 2. КОММЕРЧЕСКИЕ И ПРОМЫШЛЕННЫЕ СЛУЖБЫ БЕЗОПАСНОСТИ

В Швеции контрразведывательную работу в отношении совместных шведско-иностранных обществ и защиту государственных промышленных и коммерческих секретов осуществляет шведская полиция безопасности – СЕПО, которая стремится тесно взаимодействовать в этом вопросе с частными промышленными службами безопасности.

2.1. Особенности работы промышленных служб безопасности. В странах Северной Европы местные правоохранительные органы весьма активно действуют через влиятельные национальные союзы предпринимателей, а также самостоятельно в крупных фирмах. Уполномоченные сотрудники спецслужб на предприятиях совместно с кадровым аппаратом и службой промышленной безопасности обязаны:

* проводить квалифицированную спецпроверку лиц, допускаемых к работе с секретными документами и материалами;
* создавать агентурно-осведомительную сеть;
* распространять среди персонала служб промышленной безопасности опыт контрразведывательного обеспечения закрепленных за ними объектов.

В Швеции и Норвегии частными службами безопасности введен строгий контроль за технической и коммерческой документацией, передаваемой местными фирмами иностранным специалистам, которых разрешено знакомить лишь с материалами, имеющими особую отметку. Сотрудникам ряда шведских фирм вменено в обязанность под угрозой увольнения после любых контактов с иностранными гражданами представлять в администрацию письменные отчеты о характере имевших место бесед.

Выявлена тенденция к расширению функций государственных и ведомственных спецслужб по обеспечению безопасности коммерческой деятельности за рубежом частнопредпринимательских организаций и содействию в формировании в них собственных групп и служб безопасности. В 90-е годы на некоторые государственные спецслужбы стран Северной Европы возложены определенные задачи по защите интересов и обеспечению безопасности национальных корпораций за рубежом.

В одной из инструкций СЕПО об агентурно-оперативной работе и контактах со служащими шведских фирм за границей органам контрразведки прямо предписывается устанавливать агентурные отношения с представителями «восточных» отделов, регулярно выезжающими в Россию, страны СНГ и Прибалтику. Выполнение отдельных оперативных заданий поручается без разглашения существа всей операции сотрудникам служб промышленной безопасности крупных фирм.

2.2. Меры общей профилактики экономической преступности. С целью проведения общепрофилактических мероприятий в частном секторе сотрудниками СЕПО подготовлен в начале 90-х годов и настойчиво распространялся в среде деловых кругов страны меморандум на тему: «Промышленный шпионаж – угроза национальной безопасности Швеции», в котором приведены некоторые, правда, довольно устаревшие, данные о добывании в Швеции некоторыми иностранными спецорганами промышленных и экономических секретов.

2.3. Режимные меры. Несмотря на определенное улучшение военно-стратегической обстановки в мире, спецслужбы стран Северной Европы продолжают уделять пристальное внимание борьбе с утечкой информации. В частности, осуществляются дорогостоящие мероприятия по обеспечению секретности всех важных переговоров в государственных учреждениях и частных фирмах и банках, выявлению подслушивающих устройств криминальных структур и иностранных разведок.

При этом государственные спецслужбы и службы безопасности в частном секторе придерживаются концепции создания так называемой «чистой зоны», в соответствии с которой место, отведенное для секретных переговоров, оборудуется специальными устройствами, поглощающими электромагнитные излучения.

К каждому предмету интерьера помещения, в котором происходит секретное совещание, прикрепляется трудноснимаемый датчик (так называемое «охранное кольцо»), способный обнаруживать подслушивающие устройства и передавать соответствующий сигнал на контрольный пункт.

По заключению экспертов, однако, указанная аппаратура не может по техническим причинам быть использована для обеспечения секретности выездных совещаний. В этой связи специалистами частных фирм ведутся работы по модификации всего комплекса охранных средств и мер для таких совещаний. Предполагаемые расходы на осуществление подобных мер безопасности составят около 270 тыс. дол.

В целях повышения бдительности и ограничения контактов секретоносителей с иностранными гражданами СЕПО в последние годы резко усилила работу с промышленными службами безопасности, созданными на предприятиях и в фирмах, являющихся подрядчиками Министерства обороны. Разработаны и внедрены комплексные и многоступенчатые процедуры проверки и оценки контактов шведских бизнесменов с иностранными представителями.

По некоторым данным, СЕПО ежегодно по запросам государственных органов, частных организаций, фирм и банков выдает более 100 тыс. справок относительно политической благонадежности отдельных граждан.

2.4. Функции офицера безопасности в промышленной фирме (банке). Во многих шведских фирмах, предприятиях, учреждениях, выполняющих государственные заказы, официально введены должности офицеров безопасности. Повышенное внимание уделяется упорядочению контактов государственных служащих и сотрудников частнопредпринимательских структур, связанных с секретными работами, иностранными представителями:

* введены дополнительные ограничения в передвижении, в том числе при выездах за рубеж;
* усилены режимные меры в работе с документами;
* разработаны и внедрены новые правила и инструкции поддержания контактов и отчетности о них.

2.5. Роль общественных организаций и союзов предпринимателей в предупреждении утечки из страны научно-технических секретов. Значительное место в воспитательно-профилактической работе, направленной на предупреждение несанкционированного разглашения важных для экономики страны научно-технических сведений, занимают некоторые шведские организации предпринимателей. Например, специалистами Союза шведских промышленников в начале 90-х годов подготовлены рекомендации по защите национальных научно-технических секретов и обеспечению безопасности шведских предприятий в связи с резким расширением их деловых контактов со странами Восточной Европы.

В рекомендациях союза, подготовленных совместно со шведской контрразведкой и некоторыми военными контрразведывательными органами НАТО, отмечалось, что «разведывательная деятельность в сфере науки, техники и экономики осуществляется странами Восточной Европы в «децентрализованном варианте», но тем не менее достаточно смело и агрессивно».

Это, по мнению шведских экспертов, объясняется, во-первых, потребностью данных стран в создании достаточно конкурентных производств, что весьма затруднительно без регулярного доступа к новинкам западной техники и технологии, во-вторых, массовым переходом кадровых офицеров разведки и контрразведки в частнопредпринимательский сектор.

В результате активизировались вербовочные подходы к шведским коммерсантам с явно разведывательными целями со стороны бизнесменов из стран Восточной Европы.

В качестве наиболее характерных методов работы иностранных государственных спецслужб и частных разведывательно-информационных органов шведские эксперты называют следующие:

* внедрение в исследовательские отделы шведских фирм через многочисленные совместные предприятия;
* получение информации методами выведывания, опроса, интервьюирования, анкетирования, собеседования, наблюдения;
* проведение прямых вербовочных бесед с предложе­нием о сотрудничестве на материальной основе.

В рекомендациях особо подчеркивается, что при дальнейшем продвижении стран Восточной Европы к рыночной экономике потребуются значительные усилия для повышения конкурентоспособности практически всех видов производимой в этих странах продукции, но особенно машинотехнических товаров. Это, естественно, обернется для стран Общего рынка и Западной Европы в целом «шквалом промышленного шпионажа с Востока».

В качестве меры защиты эксперты по безопасности рекомендуют:

* усиление профилактической работы с персоналом шведских компаний;
* расширение использования услуг детективно-охранных агентств, специализирующихся в вопросах промышленной безопасности.

Анализ свидетельствует о значительной информированности за рубежом относительно усилий некоторых российских предпринимателей ликвидировать техническое отставание в промышленности посредством якобы форсирования разведывательной деятельности.

Такая осведомленность и практически уже разработанная программа профилактических мероприятий (в программе не упомянуто, кстати, совсем о мерах пресечения такой деятельности), во-первых, настораживают, во-вторых, однозначно указывают на источник ее происхождения – специальные службы. Составителям таких программ, безусловно, хотелось бы затормозить деловое сотрудничество, сохранить за своими ведущими производителями многие сегменты мирового рынка товаров и услуг.

Такой подход, однако, сегодня встречает на Западе довольно резкий отпор самих предпринимателей, воспринимается ими как анахронизм прежних лет, как атавистическое мышление периода холодной войны.

2.6. Административные меры контроля за экспортом технологий «двойного» назначения. Шведское правительство еще в начале 80-х годов уполномочило Управление материально-технического обеспечения Швеции оказывать национальным фирмам, импортирующим американскую технологию «двойного» использования, помощь в усилении режима секретности, осуществлять периодические инспекции и выдавать им свидетельства об уровне безопасности. С середины 80-х годов только при предъявлении такого свидетельства Министерство торговли США разрешает американской компании заключать контракт на поставку наукоемкой продукции шведской фирме.

### 3. ПРОБЛЕМЫ БОРЬБЫ В ШВЕЦИИ С КОМПЬЮТЕРНОЙ ПРЕСТУПНОСТЬЮ

3.1. Оценка безопасности компьютерных сетей. Шведские эксперты по вопросам безопасности в последние годы уделяют повышенное внимание борьбе с компьютерными преступлениями.

Так, в начале 90-х годов опубликованы материалы отчета шведских специалистов о состоянии безопасности данных в государственной информационной сети. Согласно отчету, озаглавленному «Компьютерная безопасность Швеции», национальные компьютерные сети слабо защищены от случайных или преднамеренных выводов из строя, что может привести в нерабочее состояние большую часть систем информационного обеспечения страны.

Шведские исследователи, изучая вопрос о возможных последствиях непредвиденного или преднамеренного вмешательства в работу информационных систем и вывода их из строя, пришли к выводу, что руководство многих министерств, ведомств и отдельных фирм, выполняющих государственные заказы, практически не имеет понятия о существующих правилах обеспечения безопасности компьютерных сетей.

3.2. Некоторые предложения по предупреждению компьютерной преступности. В ряде случаев действующие законодательные нормы, направленные на борьбу с компьютерной преступностью, настолько несовершенны, что создают серьезные препятствия в работе сотрудников, обслуживающих эти системы. Кроме того, порой они вступают в противоречие с положениями служебных инструкций.

Так, например, согласно Закону по обеспечению компьютерной безопасности некоторые документы после ознакомления с ними ограниченного круга лиц должны быть уничтожены, в то время как в инструкции по ведению делопроизводства рекомендуется хранить подобные документы в архивах.

Не решен также вопрос о том, должны ли быть закрытыми пожарные выходы из машинных залов, где обрабатывается конфиденциальная информация. Служебными инструкциями предусмотрено оставлять их открытыми для эвакуации в случае пожара, тогда как согласно предписаниям полицейских служб они должны быть запертыми в целях исключения возможности несанкционированного проникновения.

Важной с точки зрения обеспечения безопасности является проблема организации деятельности полицейского информационного центра. В целях предотвращения возможности незаконного доступа лиц к массивам данных, поступающих из различных полицейских управлений страны, руководство центра приняло решение о сокращении рабочего дня его сотрудников с 9 до 17 ч с ужесточением контроля за сотрудниками на рабочих местах, в том числе посредством скрытого видеонаблюдения.

Поэтому лица, задержанные полицией после 17 ч в связи с невозможностью проверки личности по картотеке, хранящейся в памяти центрального компьютера, должны находиться в участке до утра. Произвести проверку личности задержанного по обычной картотеке представляется невозможным из-за неукомплектованности полицейских учетных подразделений сотрудниками.

Кроме того, отсутствует надежная защита от вторжения «хэккеров» в компьютерные системы, обслуживающие таможенные и патентные государственные органы и связанные с ними частные компании и университеты. В связи с этим предполагается внести существенные изменения в работу государственной компьютерной системы, а также усовершенствовать действующие законодательные нормы по обеспечению безопасности в частном секторе.

## НОРВЕГИЯ

В начале 90-х годов в Норвегии государственная комиссия рассмотрела деятельность контрразведывательной службы страны (ПОТ) и подготовила предложения о ее структурной реорганизации, корректировке задач и методов работы. Предусмотрено существенное расширение функций центрального управления в Осло.

## 1. КОММЕРЧЕСКИЕ И ПРОМЫШЛЕННЫЕ СЛУЖБЫ БЕЗОПАСНОСТИ

Приоритетное значение в деятельности ПОТ в последнее время получили задачи борьбы с промышленным и коммерческим шпионажем. При этом основное внимание уделяется защите в частном секторе технологической информации, имеющей военное значение, а также повышению режима секретности. Все это обусловило повышенное внимание к разработке юридических норм учреждения и функционирования частных служб безопасности, определению статуса и методов деятельности офицеров безопасности, формулированию более четких правил и процедур проведения профилактических мероприятий.

1.1. Особенности тактики. Тенденция к укреплению в фирмах и банках агентурно-оперативных позиций служб безопасности характерна для большинства торговых партнеров России. Более того, некоторые, например норвежские фирмы, только приступая к переговорам и начиная проработку контракта, уже стремятся с помощью спецслужб создать на своих объектах контрразведывательный аппарат.

1.2. Специфика формирования экспортных отделов и «буферных» фирм. Тенденция к изоляции иностранных представителей от прямых контактов с производственно-промышленными объектами и их персоналом затронула даже те фирмы, которые поддерживают весьма незначительные торговые связи с нашей страной. В Норвегии, например, со стороны спецслужб ряду местных фирм («Конгсберг вопенфабрик», «Ра-уфосс амунитунс фабрик», «Сканвест ринг», «Микрон») даны следующие рекомендации:

* разделить гражданское и военное производство;
* создать отдельно «буферные фирмы»;
* «замкнуть» на эти фирмы иностранных представителей.

1.3. Подготовка персонала. В Швеции и Норвегии осуществляется Программа специальной подготовки управленческого аппарата и персонала служб безопасности компаний для принятия профессиональных мер по борьбе с потенциальной угрозой иностранных разведок и криминальных структур: сотрудников фирм, в первую очередь работающих за рубежом, обучают методам реагирования на подходы со стороны лиц, заинтересованных в секретной экономической и научно-технической информации.

Контрразведывательная служба Швеции (СЕПО) организовала курсы для сотрудников Таможенной службы и персонала транспортно-экспедиторских отделов частных компаний по вопросам противодействия иностранным разведкам. На занятиях слушателей:

* знакомят с методами иностранных спецслужб по изучению и привлечению к сотрудничеству местных граждан;
* инструктируют о необходимости информировать СЕПО о всех контактах местных фирм с иностранными представителями;
* раскрывают возможности поддержания дальнейшего контакта с иностранцем, но уже под контролем контрразведывательных органов.

### 2. ПРОБЛЕМЫ БОРЬБЫ С КОМПЬЮТЕРНОЙ ПРЕСТУПНОСТЬЮ

2.1. Причины компьютерных преступлений. Большинство компьютерных преступлений, совершаемых в стране, остается практически не известным органам полиции, поскольку государственные компании и частные фирмы, заботясь о своей репутации, редко заявляют о случаях несанкционированного доступа к их компьютерным системам.

При совершении компьютерного преступления фирмы проводят служебное расследование с помощью сотрудников частного сыска, а лица, признанные виновными, как правило, увольняются.

Однако, поступив на работу в другие учреждения, они продолжают свои противоправные деяния. В связи с этим в управлении уголовной полиции создано специальное подразделение по расследованию преступлений в коммерческой и промышленной сферах. Большое внимание сотрудники этого подразделения уделяют вопросам борьбы с компьютерными преступлениями и промышленным шпионажем, масштабы и опасность которых в настоящее время недооцениваются руководством местных фирм.

2.2. Меры борьбы с компьютерной преступностью. Главное управление уголовной полиции считает необходимым проводить мероприятия по широкому разъяснению представителям компаний и фирм величины того риска, с которым они сталкиваются, и мер по предотвращению этой опасности.

В свою очередь, страховые агентства при выплате страховых сумм фирмам, потерпевшим убытки в результате совершения компьютерных преступлений, обязаны ставить полицию в известность о данных правонарушениях. Это помогает полиции создать реальную картину состояния преступности в сфере экономики и разработать эффективные меры борьбы с нею. Полиция постоянно призывает руководство фирм и компаний к тесному сотрудничеству с правоохранительными органами в целях повышения эффективности работы по предупреждению компьютерных преступлений, а также случаев промышленного шпионажа.

# Заключение

## ОСНОВНЫЕ ТЕНДЕНЦИИ СОВЕРШЕНСТВОВАНИЯ РЕЖИМ НО ПРОФИЛАКТИЧЕСКИХ МЕР ОБЕСПЕЧЕНИЯ СОХРАННОСТИ ПРОМЫШЛЕННОЙ И КОММЕРЧЕСКОЙ ТАЙНЫ В СТРАНАХ СЕВЕРНОЙ ЕВРОПЫ

В конце 80-х – в 90-е годы в странах Северной Европы выявлена тенденция к созданию в банках, фирмах, предприятиях специальных отделов безопасности, которые нацелены на выявление несанкционированных контактов своих сотрудников с иностранными гражданами. В крупных промышленно-торговых фирмах Финляндии, Норвегии, Дании, Швеции сформированы достаточно мощные службы безопасности, которые поддерживают регулярные контакты со спецслужбами стран НАТО, и их руководство укомплектовано в основном сотрудниками разведки и контрразведки.

Основная функция служб безопасности – выявление несанкционированных контактов местных сотрудников и пресечение утечки секретной коммерческой и научно-технической информации. Введение во многих фирмах института офицеров безопасности дополнило режимные меры по упорядочению контактов секретоносителей с иностранными представителями.

Эти режимно-профилактические меры ограничивают международные контакты, научно-технические и экономические обмены, вызывают аргументированную критику со стороны деловых кругов, в том числе российских предпринимателей, которые продолжают сталкиваться с определенными проявлениями дискриминации при налаживании сотрудничества с зарубежными партнерами.