"БИЗНЕС РАЗВЕДКА" № 6

оглавление

Рынок деловой разведки

Приемы и методы деловой разведки

Как делать дизайн сайта, удобный для просмотра

Как подбирать профессионала конкурентной разведки

Учебные игры для профессионалов конкурентной разведки

Информационный менеджмент

Экстранет для бизнеса

Информационные ресурсы

Забытый ресурс

Исследования. Опросы

Денис Цыпулев, О значении патентной информации

Исследование Coda Group: финансовые генералы без оружия

Конкуренция – главная проблема бизнеса Некоторые результаты опросов топ менеджеров крупнейших компаний мира

Школа деловой разведки

Безопасность бизнеса – это профессия и специальность. Интервью с директором Института безопасности бизнеса Л.М. Кунбутаевым

Учебные центры для деловой разведки

Информационная безопасность

«Человеческий фактор» в защите прав на интеллектуальную собственность

Прозрачность хороша, но в меру

Интеллектуальных преступлений становится все больше

Американское «КГБ» будет заниматься анализами

Правительсво Японии рассматривает защитные меры против промышленного шпионажа.

Промышленный шпионаж против США. Россия тоже в «черном списке»

Документы

Международная «Конвенция о киберпреступности»

Е. Волчинская, Комментарий к Конвенции о киберпреступности

Обращение общественных организаций с протестом против принятия Конвенции о киберпреступности

Этика деловой разведки

Когда говорить “нет”

Книжная полка

Craig S. Fleisher, Babette Bensoussan Strategic and Competitive Analysis: Methods and Techniques for Analyzing Business Competition.

F,W.Rustmann CIA, INC: Espionage And The Craft of Business Intelligence.

Информационные технологии

Информационные технологии: вкладывать или экономить?

В. Светозаров

Трудности, переживаемые сегодня крупным западным бизнесом в результате вяло текущей рецессии, вынуждают многих предпринимателей сокращать расходы и капиталовложения. К сожалению, нередко жертвой урезания становятся информационные технологии.

Почему? Ответ на этот вопрос в какой-то степени дают результаты опроса руководителей 46 международных корпораций, проведенный в начале текущего года лондонской исследовательской фирмой BPRI (Business Planning & Research International). Большинство респондентов ясно заявили, что дорогостоящие информационные технологии "не оправдывают возлагавшихся на них надежд и вложенных средств"(The Australian, 04.02.2002). Более всего топ менеджмент раздражает, что эффективность вложений в ИТ не поддается точным расчетам. То есть, нельзя в цифрах подсчитать, обернется ли использование информационных технологий реальной прибылью и какой именно. Обычно провайдеры таких технологий сулят усиление конкурентоспособности, снижение затрат, повышение эффективности. И, как показывает опрос, далеко не каждый пользователь убеждается в материализации этих ожиданий.

Конечно, надо иметь в виду чисто эмоциональный аспект негативных высказываний, который вполне понятен на фоне продолжающегося общеэкономического спада, время завершения которого далеко не ясно. С другой стороны, некоторые упреки выглядят весьма убедительными. Так, например, бизнесмены жалуются, что приняв на вооружение ту или иную платформу, они попадают в монопольную зависимость от ее поставщика, который требует регулярного обновления программных продуктов, отказываясь поддерживать любые другие программные версии. В целом же, проблема видится не столько в разработчиках и провайдерах информационных технологий, сколько в их потребителях, пользователях. Последние нередко ждут быстрой и автоматической отдачи там, где требуется умелая, терпеливая, кропотливая работа.

Как убедительно демонстрируют социологические опросы, подавляющее большинство предпринимателей осознают и признают, что дефицит информации, равно как и искаженная, неточная информация о конкурентах, клиентах, партнерах оборачивается большими убытками. Проведенный весной 2002 года в Англии исследовательской компанией Business Intelligence (www.business-intelligence.co.uk) опрос 120 менеджеров, работающих в отделах маркетинга и связей с клиентами крупных фирм, ориентированных на массового покупателя, показал, что 98% британских фирм понимают связь между убытками/упущенной выгодой и неточной и/или неполной информацией, имевшейся в их распоряжении. В почти каждой второй компании отсутствует отвечающий современным требованиям информационный менеджмент, а в каждой шестой фирме практически не следят за базами данных, не обновляют их, не чистят. (Были опрошены сотрудники финансовых учреждений, коммунальных служб, розничной торговли, транспортных и телекоммуникационных компаний. Вопросы касались работы с данными о клиентской базе (CRM). С отчетом можно ознакомиться на сайте www.survey@qas.com.) Есть ли возможность перевести связь между хорошим/плохим информационным менеджментом и доходами/убытками в конкретные цифры бюджета? Как было отмечено выше, отсутствие реальных цифр является главной причиной разочарования в информационном менеджменте, и это сказывается на рынке высоких технологий. К примеру, глава крупного провайдера программного обеспечения и продуктов для управления связями с клиентами «Siebel» Том Сайебель жалуется, что итоги первого квартала этого года - наихудшие за всю историю компании.

Итак, реально ли провести точные расчеты эффективности капиталовложений в информационный менеджмент? Сегодня, пожалуй, никто не может дать ясный ответ. Не более чем попыткой хоть как-то приблизиться к решению такой задачи следует назвать недавно опубликованный доклад президента и директора фирмы «Factiva» Клэр Харт (фирма является совместным предприятием Reuters и Dow Jones). Как считает Харт, крупные организации, недооценивающие важность информационного менеджмента, теряют ежегодно около 450 миллионов долларов ежегодно. При этом американские компании вместе тратят в год 107 миллиардов долларов на оплату сотрудников, работающих исключительно с внешними информационными ресурсами.

По ее мнению, нельзя уповать только на внешние источники, в том числе онлайновые. “Одностороннее увлечение порталами настораживает, - говорит К.Харт, - Мне не по душе идея больших дверей, которые вы открываете для сбора информации... В действительности необходимо другое: активный интерфейс, сочетающий адаптированные к потребителю аналитические приложения, внешние информационные ресурсы, источники внутренней, корпоративной информации, и вся эта система должна работать гармонично и постоянно, обслуживая разные информационные запросы” (Information World Review, 05.08.2002).

Убежденность главы Factiva в необходимости вкладывать деньги в управление знаниями и информационный менеджмент, в частности, мотивируется изменениями в миграции кадров. Если в 60-е годы среднестатистический сотрудник работал в одной и той же компании более 20 лет, то сейчас служащие меняют место работы (фирму) в среднем каждые 4 года. С уходом работника неизбежно утрачивается какая то часть информации, сохранить которую для фирмы могут технологии информационного менеджмента, правильно выстроенная политика управления знаниями. Харт уверена, что те предприниматели, которые сегодня экономят на этом направлении, через три или пять лет, когда спад будет преодолен и возобновится рост мировой экономики, не смогут конкурировать с более дальновидными бизнесменами. Осознавая нынешние трудности, переживаемые западной экономикой, она советует предпринимателям начать хотя бы с малого, с внутриофисного интранета: “Следите, чтобы он работал, информация была систематизирована, регулярно обновлялась и постоянно питала офисные приложения”.

Какая информация нужна инвесторам

Какая информация нужна инвесторам

Одна из причин дефицита инвестиций – неполная информация, содержащаяся в корпоративных отчетах, которые представляются потенциальным инвесторам. Даже в странах с развитой рыночной экономикой и высокой информационно-корпоративной культурой менее 20% таких отчетов удовлетворяют инвесторов.

Основная беда в том, что вся предоставляемая финансовая информация затрагивает, как правило, внутренные стороны развития предприятия или компании. В отчетах отсутствует детальный анализ конкурентной среды и основных конкурентов, анализ перспектив развития отрасли, к которой принадлежит предприятие. Нет в отчетах взгляда на правовую среду, в которой работает предприятие, видения технологий, определяющих развитие данной отрсли. Очень часто в отчетах отсутствует информация о продвиждении брэнда, об инновационных планах, о клиентской базе, интеллектуальном потенциале компании. В результате образуется разрыв между информацией, которая готовится по традиционному клише и запросами инвесторов. Отсутствие важных данных прямо и негативно влияет на стоимость акций (если компания акционирована и представлена на фондовом рынке).

Как считает партнер корпорации PricewaterhouseCoopers Стивен Слован, необходимо использовать расширенный формат коропоративных отчетов, которые бы обязавательно учитывали следующие моменты:

- **рыночный обзор**, в том числе описание конкурентов, их позиций на рынке,

макро-экономической среды и перспектив роста отрасли, правовые аспекты и технологии, которые уже влияют сегодня и будут завтра во многом определять развитие отрасли;

- **изложение стратегии** компании в целом и отдельно для его подразделений и филиалов, включая характеристику организационных структур и процессов, необходимых для реализации стратегии;

- **балансовый анализ**, который бы увязывал результаты деятельности с поставленными задачами, содержал характеристику эффективности компании в сравнении с основными конкурентами;

- **информация о нфинансовых факторах** развития, таких как инновационная деятельность внутри фирмы, интелдлектуальный потенциал, кадровый капитал.

«Предоставляя такие подробные сведения инвестору, вы поступаете правильно, ибо в рыночной экономике определенность и знание лучше догадок и предположений», заключает автор статьи в Bangkok Post от 25 июня 2002 года.

Производители программ для деловой равзедки настроены оптимистично

Производители программ для деловой разведки настроены оптимистично

В прошлом году мировой рынок программ для деловой разведки возрос на 2.2%.

Немного, но и неплохо, если сравнить в целом с продажами программного обеспечения, которые остались на уровне 2000 года. По мнению экспертов исследовательской фирмы IDC, в этом году продажи продуктов деловой разведки возрастут на 9%, в то время как вся отрасль программного обеспечения – в лучшем случае на 7.7%. Это самый оптимистичный прогноз!

Сегодня лидеры на рынке ДР: Business Objects, SAS Institute, Cognos. Они идут ноздря в ноздрю, имея каждая примерно по 10% рынка, указывает со ссылкой на IDC еженедельник Business Week (24 июня 2002). Как ожидается, продажи продукции Business Objects возрастут в 2002 году на 14%, достигнув 415 миллионов долларов. Cognos рассчитывает увеличить доходы на 10%, выйдя на отметку 540 миллионов долларов.

Относительный успех компаний - провайдеров программ для ДР (кстати, не только крупных, но и средних поставщиков) объясняется выходом на рынок интеграционным систем, которые позволяют одновременно использовать на уровне одного предприятия различные виды компьютеров, разнотипные информационные системы. Другим преимуществом продуктов ДР является их доступность даже небольшим предприятиям. К примеру, программы для отчетов по продажам и прогнозам продаж, предназначенные для малого бизнеса или отдельных структурных подразделений в рамках одной компании, стоят всего $10,000. Конечно, многофункциональные интегрированные системы управления зашкаливают за миллион, но они окупаются в считанные годы.

Business Week приводит примеры успешного использования программ ДР.

После 11 сентября отели Лас-Вегаса опустели. Все боялись летать самолетом. Компания Harrar, владеющая сетью гостиниц, провела компьютерный анализ потенциальных игроков, проживающих в радиусе, достаточном, чтобы добраться до Лас-Вегаса на автомашине. Целенаправленная реклама сделала свое дело, и вскоре отели заполнились вновь. British Airways проанализировала с использованием программ ДР жалобы клиентов на потерю багажа. И пришла к выводу, что необходимо ориентировать пассажиров относительно минимально требуемого времени для переброски багажа с одного рейса на другой. Toyota использует программы для сведения всех данных о финансах, запасных частях, готовой продукции воедино, что позволяет быстро просчитывать все операции и производственные процессы на предприятии.

Несколько рекомендаций для тех, кого интересует рынок США

Несколько рекомендаций для тех, кого интересует рынок США

Возможно, вашему бизнесу тесно или неуютно на российских просторах, и вы решили присмотреться к рынку США. В таком случае, полезно ознакомиться с рекомендациями, где и как искать информацию об американском бизнесе, которые опубликовал американский эксперт по маркетингу, управляющий партнер Amcon Marketing Strategy International Чарльз Клейн в 11 номере журнала SCIP.online. Статья так и называется: «Найти информацию о корпорациях США: справка для зарубежных компаний, нацеливающихся на рынок США».

Статья представляет собой краткий обзор информационных ресурсов и методов сбора информации. Автор рекомендует использовать как вторичные источники (файлы торгово-промышленных ассоциаций, деловую прессу, правительственные документы, материалы судов, Интернет), так и первоисточники (интервью у непосредственных участников американснкого бизнеса и рынка). «Практический опыт убеждает, что пользование только вторичными источниками и ресурсами – главная причина провала попыток занять свое место на рыгке США».

В числе первоисточников Клейн называет: служащих партнерской компании США, дистрибьютеры и агенты по продажам в интересующей отрасли, конечные пользователи аналогичной продукции или услуг, преподаватели университетов, служащие торговых ассоциаций, авторы публикаций и редакторы деловой прессы, представители конкурента партнерской (или интересующей вас) фирмы США, служащие госорганов и профсоюзов, служащие компаний-поставщиков.

Многое зависит от того, является ли объект вашего внимания, американская компания частной или публичной (т.е. акционированной и представленной на фондовом рынке). В отличие от первых, акционированные компании обязаны представлять в открытом доступе важную информацию, которую можно получить через Интернет. Частные, т.е. принадлежащие узкому кругу лиц или одному лицу фирмы, не обаны это делать. Вместе с тем, важно иметь в виду, что некоторые акционированные компании умело прячут информацию, которая вам нужна, и тогда не обойтись бе-з первоисточников.

Конечно, находясь по другую сторону океана, очень трудно находить и работать с первоисточниками. Но можно воспользоваться услугами местных консультантов, которых множество в США и которые в состоянии квалифицированно организовать опрос по интересующим вас вопросам.

Тем, кто впервые выходит на американский рынок, Клейн советует внимательно ознакомиться с двумя законодательными документами США. Это Акт об экономическом шпионаже (1996), нарушение которого грозит тюремным заключением до 10 лет и многомиллионым штрафом, а также Акт о свободе информации. Особенно важно поправка к последнему от 1996 года, ибо она требует от правительственных служб США предоставлять в возрастающем объеме несекретную информацию, в том числе экономическую, коммерческую, в цифровом виде (Интернет, CD, т.д.), что избавляет от необходимости обращаться за информацией непосредственно в соответствующие учреждения, а можно ее получить, сидя дома за компьютером.

Крах "новой экономики": почему подвели прогнозы?

Крах "новой экономики": почему подвели прогнозы?

Два года назад рухнула т.н. “новая экономика”, до того бурно развивавшаяся на базе Интернет технологий. Среди многих причин специалисты называют неспособность, неумение прогнозировать рыночную динамику. На эту тему рассуждает независимый консультант в области прогнозирования и бизнес разведки Подсэдли в журнале The Journal of Business Forecasting Methods and Systems (Весна 2002).

Он отмечает, что крушение “новой экономики” произошло, на первый взгляд, неожиданно, “непредвиденно”. Такие столпы электронного бизнеса и Интернет технологий как Cisco, Hewllett-Packard, Nortel и другие корпорации, захлебываясь от восторга фантастическими темпами роста, излучали стойкий оптимизм и строили радужные планы. Никто не был готов к резкому спаду, который произошел в 2000 году. Почему подвели прогнозы?

Отвечая на этот вопрос, автор первопричиной называет отсутствие “исторической базы” в проводившихся расчетах. “Отсутствие и/или не использование баз данных с историческим материалом делает традиционные инструменты прогноза не эффективными”. Первым делом надо было проследить развитие аналогичных ситуаций в прошлом. Так, например, сравнить динамику роста электронной почты с начальными этапами развития телефонных коммуникаций, и многое можно было бы: по мнению автора, понять и предвидеть.

Другая причина лежит в области психологии. В погоне за быстрорастущими прибылями предприниматели “новой экономики” не захотели поверить в возможность резкого перелома в рыночной тенденции, не обращали внимания на первые признаки возможного кризиса, которые подсказывали аналитические программы, широко внедрявшиеся в бизнес. Они явно недооценили зависимость производства от динамики спроса, полностью сконцентрировались на продукции, не обращая достаточного внимания изучению тенденций спроса. Это распространенная ошибка, связанная с “эгоцентрическим” подходом к анализу рыночной ситуации, когда в центре рассматриваемой проблемы стоит конкретная компания, а все остальное как бы вращается вокруг нее.

Кризис показал ненадежность традиционных методов экономического прогноза, базирующихся на статистических данных, которые нередко мало что говорят принимающим решения топ менеджерам. По мнению автора, наиболее эффективным инструментом прогноза зарекомендовал себя еще редко используемый метод “сценарного планирования”, или, как еще его называют, “сценарного прогноза”, представленный публике в 60-ые годы Германом Каном и реализованный впервые в 70-ые годы компанией Royal Dutch Shell. Он является хорошим дополнением к традиционным способам анализа ситуации, ориентирован на перспективу и потенциально более понятен руководству корпораций.

Подробнее об этой методике читатель узнает в статье **Сценарная аналитика - создание альтернатив,** которая публикуется в текущем номере, в рубрике **Приемы и методы деловой разведки.**

Сценарная аналитика - создание альтернатив

Сценарная аналитика - создание альтернатив

Как пишет крупный эксперт по конкурентной разведке Кеннет Савка (Competitive Intelligence Magazine, Sept-Oct 2001), путь к принятию оптимальных, успешных стратегических решений в бизнесе, как правило, извилист и тернист. Он пролегает через анализ множества вариантов возможных изменений рыночных условий, экономики, потребительских тенденций, действий конкурентов. Поэтому так важно использовать методологию “сценарной аналитики”, о которой идет речь в упомянутой статье американского эксперта.
К. Савка так формулирует понятие “сценарной аналитики”: “систематический метод оценки предполагаемых сценариев развития ситуации на рынке”. Методология: по его мнению, позволяет аналитикам предлагать варианты деятельности кампании при наиболее вероятных условиях развития ситуации.

Это не предсказание будущего. При высокой и постоянной изменчивости различных факторов, определяющих ситуацию на рынке, невозможно точно предсказать, как она будет развиваться в будущем. Руководство компаний и не ждет этого от службы конкурентной разведки. Но оно вправе рассчитывать на предложение рассмотрение набора обоснованных вариантов наиболее вероятного развития, предполагающих заблаговременную разработку альтернативных решений. Хорошо аргументированные сценарии позволяют своевременно создавать “запасные” вариантные планы действий. Кроме того, “сценарная аналитика” способна идентифицировать и правильно интерпретировать те или иные рыночные явления, признаки, сигнализирующие о появлении новых тенденциях, о начинающихся изменениях.

Благодаря методологии “сценарной аналитики”, профессионал конкурентной разведки может быстро и убедительно объяснить начальству мотивы поведения конкурентов, и, ссылаясь на проведенный ранее анализ, показать, какие именно элементы продуманных заранее сценариев стали воплощаться в реальность и по какой причине. Но самое главное, руководству компаний не надо терять время на проработку адекватных начавшимся изменениям действий, ибо такие планы уже есть.

Как делать дизайн сайта

Как делать дизайн сайта, удобный для просмотра

Об этом идет речь в статье Джерри МакГоверна в журнале SCIP.online (№11). Автор отмечает исключительную перегруженность информацией пользователей Интернета, который сейчас вмещает порядка 600 миллиардов разных материалов и документов. Опросы показывают, что 79% посетителей того или иного веб-сайта ограничиваются просмотром, и только 16% имеют время и терпение читать фразу за фразой. Обычно пользователи Сети читают первую фразу веб-материала, а остальной текст в лучшем случае бегло просматривают.

Учитывая эти данные, полученные в ходе разных опросов и исследований, автор рекомендует веб-дизайнерам придерживаться следующих правил:

- Структура сайта должна отвечать сложившимся стандартам с тем, чтобы читатель тратил как можно меньше времени на поиск нужного раздела. Например, большинство посетителей привыкли находить линк Home в левом верхнем углу. Если он в другом месте, потребуется время, чтобы его отыскать.

- Первая (домашняя) страничка должна содержать короткие тексты. Информация должна быть тем подробнее, чем глубже «уходит» читатель в сайт.

- Используемые термины должны быть просты и понятны всем посетителям.

- Заголовки и подзаголовки обязаны носить описательный характер, чтобы читателю было понятно, о чем в статье идет речь.

- Размещаемые на веб-сайте материалы должны быть короткими, строго по существу, не содержать громоздких, неудобоваримых предложений.

Как подбирать профессионала конкурентной разведки

Как подбирать профессионала конкурентной разведки

Итак, руководство Вашей компании решило создать службу конкурентной разведки и хочет найти специалиста, который мог бы ее возглавить. Большинство компаний не могут себе позволить держать в штате сразу нескольких сотрудников этой службы, и часто речь идет об одном специалисте КР. Каким он должен быть?

На этот вопрос отвечает эксперт Билл Флория в журнале Competitive Intelligence Magazine (September-October, 2001). Флория советует начинать с попытки ясно сформулировать цели, которые ставятся в долгосрочном плане перед новым направлением. Они должны быть достаточно амбициозными. Обычно от КР ждут помощи в прогнозировании грядущих изменений в отрасли и поведении основных рыночных фигурантов. Поэтому необходимо рассматривать результаты работы новой службы в перспективе как минимум нескольких лет, а не нескольких месяцев.

Топ менеджмент не всегда может четко определить свои потребности в КР. Чаще всего результаты КР представляют себе в виде статичных отчетов о конкурентах, которые содержат информацию “раннего предупреждения” о готовящихся конкурентами технологических новинках и действиях. В то же время конкурентная разведка - это не просто информация, а, прежде всего постоянный анализ и прогноз изменений на рынке. Поэтому специалист, который нужен компании, должен давать анализ, а не информацию, уметь выделять и концентрироваться на критически важных аспектах, уметь пользоваться информационными технологиями - работать с базами данных, веб-сайтами и т.п.

Каким опытом и навыками эксперт КР должен обладать? Ответ зависит от того, какие ставятся задачи. Если руководство ждет раннего прогнозирования возможных сюрпризов, которые готовит конкурент, то кандидат на должность директора/специалиста КР должен иметь опыт аналитической работы, уметь извлекать максимум полезного из минимума информации.

Если же руководству надо от КР поддержки в расширении продаж, то специалист КР скорее должен иметь навыки работы с телефоном, нежели способность к анализу информации.

Но в любом случае он должен быть своего рода “корпоративным провокатором”. То есть, готовить тех, кто принимает решения, к самым неожиданным возможным поворотам, предлагая обоснованные сценарии возможного поведения конкурентов и развития общей ситуации на рынке в ближайшем и долгосрочном будущем. “Что, если?” - вот ключевой вопрос, который должен звучать в его аналитических докладах.

Учебные игры для профессионалов конкурентной разведки

Учебные игры для профессионалов конкурентной разведки

Можно ли рассматривать конкуренцию как арену боевого сражения? А почему бы и нет, конечно, при условии, что конкурентная борьба ведется по правилам, без запрещенных законом и нечистоплотных с точки зрения деловой этики методами. Как и на войне, преимущество получает тот, у кого больше информации, у кого она точная и свежая. Как и военное искусство, искусство конкуренции требует продуманной и долговременной стратегии, умения хорошо ориентироваться в быстроменяющихся условиях.

В этом смысле не лишним представляется опыт ряда западных корпораций в проведении деловых игр на манер военных учений, где одна из сторон - предполагаемый «противник». Об этих играх, получивших название «военные игры», рассказывает Аллан Холл в статье лондонской газеты «The Evening Standard", опубликованной, надо заметить, 8 мая 2002 года, в день, отмечаемый на Западе как День Победы.

Война, как известно, есть продолжение политики другими средствами. То же самое, по мнению Холла, можно сказать и о большом бизнесе. Поэтому не удивительно, что некоторые топ менеджеры европейских компаний любят начинать рабочий день с чтения Клаузевица и других классических учебников по военному искусству. «Военные игры» – это по существу компонент стратегического планирования, предваряющий важное решение, связанное, например, с поглощением или слиянием.

На практике «военные игры» представляют собой широко распространенные ролевые деловые игры, где часть участников берет на себя роль противника (конкурента), придумывая за него те или иные маневры и шаги. «Это мощный инструмент прогнозирования изменений и минимизации риска», считает менеджер по конкурентной разведке фармацевтического англо-шведского гиганта AstraZeneca Джанни Пелешок. Она организовала уже дюжину «военных игр» для своей компании в Европе и Северной Америке. «Благодаря ролевым играм вы как бы встаете на место конкурентов, проникаете в их возможные замыслы, говорит Пелешок, - А это нельзя сделать при помощи традиционных инструментов менеджмента и планирования».

Во Франции корпорация Carrefour, владеющая гигантской сетью гипермаркетов, провела с помощью приглашенных экспертов деловую игру с задачей разработать сценарий действий на случай выявления коровьего бешенства в молоке традиционных поставщиков.

«Военные игры» постоянно организуются американской Академией по конкурентной разведке, основанной Фулдом, Джиладом, Херрингом.

Несколько лет назад такую игру провели руководители авиакомпании Swissair. Игра показала, что единственный способ выжить в условиях спада и кризиса – слияние с крупным конкурентом. Руководители проигнорировали выводы и результат – банкротство.

Материал подготовил В. Борисов

Экстранет для бизнеса

Экстранет для бизнеса

В отличие от «интранета» – замкнутой, защищенной от внешнего вторжения компьютерной информационной сети, «экстранет» предназначен для внешних пользователей. Обычно экстранет используется как источник дополнительной информации об услугах и продуктах. В последнее время получают распространение сети экстранет, пользователи которых используют инструменты запросов, отчетов и даже аналитики. Практически речь идет о предоставлении инструментария деловой разведки внешним потребителям информации, хранящейся в базах данных компании. Этому виду информационного обслуживания, посвящена статья Рика Вайтинга в Informationweek (05.20.2002).

Экстранеты получают распространение в бизнесе, в основном в сфере B2B. Они особенно характерны для фирм, занимающихся информационным бизнесом. NetRating Inc. оперирует экстранетом деловой разведки, предоставляя подписчикам, доступ к хранилищу информации об использовании Интернет-пространства, которая снимается и закладывается в хранилище с 200,000 веб-сайтов. Подписчики - рекламные агентства, СМИ, такие интернет компании, причем такие, как Yahoo, America Online.

Экстранеты деловой разведки создают не только информационные компании. Крупная фирма по снабжению медицинских учреждений Owens & Minor через экстранет предоставляет клиентам (больницам) подробнейшие данные обо всем, что может их интересовать - от постельного белья до сложного медицинского оборудования. Известная почтовая фирма Federal Express предоставляет транспортным компаниям, работающим с ней, интересующие их данные о своей деятельности. В автоматическом режиме пользователь может получить ответ на вопрос “Сколько почтовых отправлений поступили во Вьетнам после 17 часов такого-то дня?”.

Экстранет ДР становится популярным у финансовых, кредитных, энергетических, туристских организаций. Плюсы: снижение затрат на обслуживание клиентов (которые сами осуществляют информационный поиск), это дополнительная услуга, привлекающая новых клиентов и партнеров, это возможность для клиентов контролировать относящиеся к ним данные, это, наконец, дополнительные доходы от подписки.

Но таких открытых сетей в бизнесе относительно немного. Главное, что сдерживает их рост - это нежелание предпринимателей делиться информацией. Ведь главное условие для успешного использования экстранета деловой разведки - согласие всех партнеров открыть друг другу свои данные. Немногие на это согласны. Кроме того, играет роль боязнь нарушения конфиденциальности в работе с клиентами - ведь нет ничего хуже, когда один из клиентов (партнеров) получает информацию о других.

6-6-Забытый_ресурс информации

Забытый ресурс

Эту историю рассказал Деннис Эмерсон, владелец и директор консалтинговой фирмы по конкурентной разведке Oregon Competitive Information Services (SCIP.online, #11).

Эмерсона пригласили в фирму, занимающуюся графическим дизайном, для выступления по

проблемам конкурентной разведки. На совещании были практически все сотрудники фирмы, от младшего персонала до руководства. Выступление встретили вежливо, но с выражением скуки. Чтобы расшевелить аудиторию, Эмерсон спросил, кто из присутствующих изучал конкурентов. Двое участников подняли руку. Столько же откликнулись на вопрос о том, кто прямые конкуренты. Никто не отреагировал на вопрос о том, кто из конкурентов влияет на деятельность фирмы.

Только присутствующий здесь же директор компании сказал, что уделял внимание этому вопросу. И когда он перечислил ряд наиболее опасных конкурентных компаний, один из служащих поднялся и сказал, что если бы он знал, что в этом списке будет компания X, то смог бы собрать информацию через кузена жены: работающего там. В частности, он недавно слышал, что менеджмент X ищет кредит для выплаты текущей зарплаты.

Этот пример убедительно иллюстрирует удивительное, весьма распространенное пренебрежение к такому эффективному источнику конкурентной информации как круг знакомых людей, которые потенциально могут быть носителями ценнейшей информации. По цепочке «знакомые знакомых» можно получать важные сведения об интересующей отрасли или конкретном объекте. Не обязательно далеко ходить. Достаточно бывает опросить своих же коллег.

Поэтому, делает вывод Эмерсон, так важно, чтобы все служащие компании имели ясное понимание конкурентной среды, в которой протекает деятельность их компании. Они должны иметь представление о сильных и уязвимых сторонах своей фирмы, о перспективах и внешних угрозах, об основных конкурентах. Это необходимо не только для того, чтобы увеличить число «глаз и ушей» в процессе конкурентной разведки, но и для того, чтобы сотрудники понимали, почему принимаются те или иные важные решения и относились к ним осознанно.

О значении патентной информации

Денис Цыпулев

О значении патентной информации

Из Аттестационной работы выпускника Института безопасности бизнеса Дмитрия Цыпулева «Исследование механизмов правовой защиты интеллектуальной собственности и ее коммерциализация»

Чтобы устоять на мировом рынке, важно не только развивать свои технологии, но и знать, в каком направлении развиваются конкуренты. Помимо всего прочего, такая информация необходима для того, чтобы не нарушить законным образом оформленные права других производителей на те или иные технические и технологические решения (такое нарушение грозит большими штрафными санкциями со стороны правообладателей). Как показывает анализ патентной информации, в последние годы, например, на российском патентном рынке металлов наметилась тенденция планомерного его захвата металлургическими компаниями зарубежных стран, прежде всего, США, Японии, Кореи и др. Патенты этих компаний в корне отличаются от патентов отечественных металлургических комбинатов. В них в полной мере учтен более чем тридцатилетний опыт ведения "патентных войн" между ведущими странами мира, применена стратегия блокирования достаточно обширных областей российского патентного рынка, а также осуществлено разделение его между зарубежными компаниями. По этой причине наличие такой информации позволяет предприятию проводить эффективную патентную политику, позволяющую не только защитить свои права, но и создавать неблагоприятные условия для конкурентов.

Функции патентной информации.

В технической литературе (имеются в виду книги и периодические издания), патентная документация зачастую игнорируется. Между тем любая информация, основанная исключительно на источниках технической литературы, может быть неполной (имея в виду уровень развития в конкретной области техники).

Кроме того, зачастую патентная документация отражает уровень (или направления) развития, по которому должны идти научные исследования для решения определенной технической проблемы. Информация по уровню техники, которая может быть обнаружена в свежих патентных документах, в сочетании с конкретными научными знаниями позволит вести разработки в уже известных направлениях либо в совершенно новых направлениях, создавая прогрессивные технологии и изделия. Таким образом, использование этой информации экономит время, средства и усилия, поскольку позволяет избежать повторения работы, которая была проделана в этом направлении другими.

Патентная документация может помочь выявить альтернативные технологии, которыми можно заменить существующие с целью улучшения экономических или экологических параметров.

Другая возможность использования патентов состоит в том, что изобретения, описанные в них, предлагают более короткий или быстрый способ изготовления и, таким образом, обеспечивают более ускоренный возврат инвестированных средств и более высокую производительность.

Использование информации, возникающей в результате раскрытия изобретений, позволяет избежать напрасного дублирования работ и увеличения стоимости научно-исследовательских разработок, направленных на поиски решений технических проблем, которые могут возникнуть в обратном случае; эта информация может также действовать в качестве катализатора для дальнейших изобретении, что способствует развитию науки и техники.

Еще один способ использования патентной документации - оценка конкретной технологии, которую предполагается закупить или которая предлагается в виде лицензии. В этом смысле поиск на установление уровня техники с использованием патентных документов позволит получить информацию по различным технологиям, имеющимся на рынке или находящимся в разработке, а такая информация, естественно, позволит лучше оценить и проанализировать технологию, которая предлагается по лицензии.

Такая проблема может возникнуть, например, при планирования нового подразделения предприятия, выпускающего определенную продукцию, или при совершенствовании уже существующих способов изготовления или технологий. В этом смысле решающее значение будет иметь возможность использования местного сырья вместо импортируемого или переработка побочных продуктов существующего промышленного производства, которые до этого не использовались. В таких случаях патентная литература может дать очень ценную информацию, которая позволит заинтересованной стороне остановиться на наилучшем варианте прежде, чем начинать переговоры с фирмами, предлагающих технологии или производственные предприятия под ключ;

Поиск для установления технического уровня по патентным документам обычно помогает выявить те решения технических проблем, которые уже предлагались в прошлом. В патентной литературе очень часто указываются недостатки и трудности, которых можно избежать при использовании определенного способа производства или конструкции, или указываются преимущества и выгоды, которых можно достичь с помощью таких способов и конструкций.

В дополнение к попыткам получить даром новейшие образцы военной техники наблюдается еще одно не менее интересное явление - охота за российскими патентами. Анализ патентной информации последних лет свидетельствует, что Россия теряет исключительные права на ряд уникальных технических решений, создававшихся за государственный счет. Речь идет об изобретениях, способных определить перспективное развитие систем вооружения в первой половине XXI века.

Используя неурегулированность вопроса по соблюдению прав РФ на результаты интеллектуальной деятельности, крупнейшие мировые производители вооружений ведут беспрецедентную в международной практике работу по юридическому закреплению за

собой прав на изобретения российских авторов.

Только в США в обход российского патентного ведомства зарегистрировано несколько сотен патентов на производство продукции военного и двойного назначения, где авторами являются российские изобретатели, а обладателями патентов – американские фирмы.

Кроме того, зарубежные партнеры российского ВПК, пользуясь отсутствием необходимых мер по охране интеллектуальной собственности российской стороны, заметно активизировали процесс финансирования доступных им научно-технических разработок непосредственно в РФ.

По оценкам Российского фонда патентной информации, в период с 1993 по 1998 годы только французская компания "Аэрокоптер Франс" получила более 10 патентов РФ на перспективные технические решения, используемые в области вертолетостроения.

Учитывая тот факт, что данная фирма не может рассматривать Россию как перспективную для сбыта своей продукции в области боевых вертолетов, единственное объяснение такой "патентной активности" – создание юридических оснований для устранения конкурента в случае его появления на международном рынке.

Зарубежная компания получает юридические основания для предъявления исковых требований нарушения "своих" прав, что может создать серьезные проблемы при поставках российских боевых вертолетов, как для Вооруженных сил РФ, так и на экспорт.

В частности, патентообладателем оригинальной системы управления соосным винтом (применяемым в российском вертолете Ка-50 «Черная акула») стала отнюдь не авиационная держава из разряда оффшорных - Антильские острова. Правами на силовую установку для самолета вертикального взлета и посадки, разработанную когда-то в СССР и до сих пор непревзойденную, обладает «Локхид Корпорейшн» (США). Хозяином уникальной российской конструкции ракеты-носителя, сбрасываемой с самолета, вкупе со способом автоматического запуска двигателя в воздухе и управлением ракетой в полете, стала американская компания «Орбитал Сайенсиз Корпорейшн II». Сей грустный список, напоминающий мартиролог утраченных приоритетов, можно продолжить.

Анализ патентной ситуации

Необходимость внимательного анализа патентной ситуации при оценке новой продукции и ее сбытовых возможностей не вызывает сомнений. Для этого существует множество способов сбора данных и анализа патентной информации. Начать хотя бы с несложной методики анализа патентной активности *(Patent Hit Count by the Year),* позволяющей оценить, насколько фирме необходима новая технология; сколько потенциальных конкурентов действуют или собираются действовать в этой же сфере; растет или падает соответствующая патентная активность; нет ли на данном стратегическом направлении «узких мест» в освоении технологии, которую фирма намерена патентовать.

Статистика свидетельствует, например, о быстром развитии электронного аукционирования. Об этом часто пишут многие газеты. Но только более тщательный патентный анализ поможет раскрыть наличие нежелательных конкурентов типа *Reuterwnw Cantor Fitzgerald Securities,* уже зарегистрировавших патентные заявки и, возможно, планирующих предпринимательскую деятельность в этой сфере. Тщательное изучение чужих патентов и собственных возможностей позволит оценить шансы вступления на это уже возделываемое поле электронной торговли.

Компания *Cantor Fitzgerald уже* подала иск о нарушении ее патентных прав корпорацией *Liberty Brokerage Investment,* которая якобы воспользовалась ранее запатентованным протоколом электронного аукциона. И это - только начало столкновений в бурно развивающемся бизнесе онлайнового аукциона, поскольку объем трансакций может, согласно оценкам, достичь в 2002 г. $ 65 млрд. Небольшие начинающие фирмы и лидеры типа *IBM* и *Microsoft,* стараясь опередить друг друга, выбрасывают на рынок пакеты программ, так что аукционному бизнесу даже не приходится создавать компьютерные технологии самостоятельно.

Другим инструментом, особенно удобным для анализа участков предпринимательской

активности типа электронной торговли, служит матрица *ИС (IP Landscape Map).* С ее помощью можно охарактеризовать пространство конкуренции по разным параметрам, идентифицируя, например, распределенные во времени участки наибольших затрат на НИОКР либо выявляя отличающиеся повышенной патентной активностью зоны ускоренного технического развития во вновь появляющихся подотраслях. Одна из таких матриц позволила выявить 520 патентов, связанных с электронной почтой, из которых львиная доля (283) принадлежит компании *Pitney-Bowes, a* 8 патентов - ее начинающему конкуренту *eStamp.* Переговоры о перекрестном лицензировании не увенчались успехом, и eStamp может оказаться втянутой в дорогостоящий судебный процесс с конкурентом, рыночная стоимость которого - $ 4 млрд.

При анализе деятельности конкурентов обращаются и к отчетам о сроках обновления технических решений *(Innovation Cycle Speed reports).* Они позволяют оценить темпы разработки новых технологий конкурентами, отталкиваясь от средней ретроспективной глубины патентных ссылок на известный уровень техники, превзойденный или обойденный данным запатентованным изобретением. Если конкурент часто цитирует свои более ранние патенты, это может означать, что он освоил стержневую технологию и в ускоренном темпе создает основанную на ней новую продукцию. Если же он цитирует и чужие патенты, из этого может вытекать вероятность создания им аналогичной продукции, с которой конкурент хочет выйти на рынок первым.

При осуществлении сделок по слиянию и приобретению компаний вместе с их технологиями следует обратиться к специальным патентным базам данных. Предположим, компания *Intel* обратила внимание на новый рынок карманных информационных устройств, которые недавно считались последним словом техники. Понятно, что ее основной интерес будет обращен на разработку микропроцессоров для подобных устройств. Множество электронных приспособлений создается в небольших фирмах с капиталом до $ 100 млн. База данных *Patent Hit Count for Assignee* укажет фирмы, проводящие наиболее интенсивные работы в этой области. Последующий анализ патентов, а также производственной и финансовой деятельности отобранных фирм может высветить объект, заслуживающий приобретения.

Компания *Via Technologies* (далее -*VT),* например, создала новую линию для производства быстродействующих недорогих и Intel-совместимых микропроцессорных наборов. Однако в июне 1999 г. Intel попыталась нарушить планы VT, расторгнув лицензионное соглашение с «зарвавшимся» производителем микропроцессоров и предъявив ему иск о нарушении патентных прав. В ответ *VT* разработала план обхода блокады, предпринятой *Intel:* она приобрела отделение по производству микропроцессоров компании *National Semiconductor (NS),* имеющей лицензионное соглашение с *Intel.* Благодаря поддержке NS компания VT получила возможность агрессивного вторжения на этот быстро развивающийся и прибыльный участок рынка.

Патентный анализ помогает компании не только выявлять объекты слияния или приобретения, но и выбирать наилучшие варианты. Поэтому, изучая возможности подобных сделок, необходимо поставить ряд вопросов:

насколько технология отобранной компании совместима с вашей, заполняет ли она выявленные бреши, когда истекает срок действия соответствующих патентов, своевременно ли уплачены пошлины за поддержание их в силе во всех странах патентования, есть ли слабые места в формулировке патентных притязаний или ошибки в оценке известного уровня техники?

Приобретая компанию, обладающую передовыми технологиями, необходимо установить, не ослабевает ли ее динамика патентования в последние годы, не слишком ли велика ретроспективная глубина ссылок в патентах компании, что указывало бы на снижение темпов ее технического развития; не вовлечены ли ее патенты в ограничительные лицензионные соглашения или в патентные споры.

Российские специалисты теперь также располагают возможностью использования широкого ассортимента баз данных, обратившись к онлайновым службам таких всемирно известных информационных центров, как *STN International, Questel-Orbit, Lexis-Nexis* и др.

Найдя продавца и осуществив должную оценку соответствующих активов ИС, необходимо структурировать сделку с учетом многих правовых, налоговых и прочих преимуществ. При

этом следует учитывать возможность сопровождения сделки рядом производственных, географических и иных ограничений. Может, например, оказаться, что приобретенные патентные права допускают их использование только в Европе или что не разрешается предоставление сублицензии конкурентам продавца и т. п.

Существует возможность разграничения юридических и экономических прав на патентный портфель. Можно, например, обрести надежную защиту патентных прав в США, уплачивая относительно низкие налоги в Гонконге. Один из производителей полупроводников экономил, таким образом, на налогах более $ 10 млн. ежегодно.

Исследование Coda Group

Исследование Coda Group: финансовые генералы без оружия

Компания Coda Group, крупный провайдер финансово-разведывательных, аналитических решений, опубликовала результаты проведенного ею исследования о работе с информацией в финансовых подразделениях средних и крупных предприятий разных стран.

Опрос выявил, что более 60 % финансовых директоров международных корпораций и средних компаний не могут своевременно получать информацию, которая им необходима для проверки и контроля эффективности финансовых служб.

Основная причина – несовершенные системы бухгалтерского учета, используемые на предприятии. 98% респондентов пользуются традиционными письменными формами отчетов, которые готовятся и пополняются свежими данными вручную.

Кроме того, исследование показало, что такие отчеты представляются не чаще, чем раз в месяц.

Все это приводит к тому, что в большинстве крупных и средних компаний (западных стран) отсутствует финансовый анализ в режиме реального времени. И это несмотря на то, что 75% участников опроса признают необходимость автоматизации процесса анализа финансовой деятельности.

Приведенные “m2 Presswire” (14 июня 2002) данные об исследовании Coda Group довольно любопытны, и могут даже показаться чересчур драматизированными, если не преувеличенными. Но учитывая профиль деятельности этой компании, выпускающей в том числе программные продукты для финансового анализа, особого удивления результаты исследования не вызывают.

Конкуренция - главная проблема бизнеса

Конкуренция – главная проблема бизнеса

Некоторые результаты опросов топ менеджеров крупнейших компаний мира

Опрос 506 высших должностных лиц, возглавляющих компании стран Северной Америки, Европы и Азиатско-Тихоокеанского региона, проведенный совместно Accenture и The

Conference Board в 2001 году, показал, что вызовы конкуренции представляют для топ менеджмента главную проблему.

Первых лиц в руководстве компаний попросили назвать три наиболее важных, по их мнению, фактора, с которыми они сталкиваются в предприниматели. Чаше всего называли:

- вызовы, связанные с формой и уровнем конкуренции (41%);

- влияние Интернета (38%)*

- отраслевая консолидация (37%)

Две другие серьезные проблемы, прозвучавшие в ответах, - давление на цены (33%) и недостаток умения, современных навыков ведения бизнеса (32%).

Как отмечается в отчете о проведенном опросе, трудно выделить одну какую-либо проблему, ибо все они тесно взаимосвязаны. Их расстановка по степени важности во многом определяется регионом. Так, топ менеджеры Северной Америки испытывают головную боль, прежде всего от “недостатка умения вести бизнес”. В Европе основную проблему для себя видят в растущем влиянии на бизнес Интернета. А в АТР конкуренция является проблемой номер 1.

Как объяснить некоторое отличие в подходах? По мнению авторов отчета, “в Европе вторжение Интернета в бизнес и тенденции к консолидации - сравнительно новые проблемы по сравнению с Северной Америкой. Для экономик АТР процесс глобализации, ведущий к большей открытости рынка товаров и капиталов, требует их полной реструктуризации” (Competitive Intelligence Magazine, Sept.-Oct., 2001)

В другом исследовании, проведенном Knowledge Systems and Research, высшие менеджеры компаний определили для себя ключевые потребности конкурентной разведки:

- 87% опрошенных рассматривают в качестве самых главных вопросов “оперативный сбор разведывательной информации для поддержки стратегических решений” и “формирование победной стратегии”;

- 77% респондентов заявили, что для них наиболее значимо “повышение точности и своевременности ценового маркетинга”;

- 68% менеджеров считают ключевым фактором “налаживание круглосуточной конкурентной разведки”;

- для 76% важным является “знание, что думают клиенты о их фирме, продукции или услугах”.

Безопасность бизнеса - это профессия

Безопасность бизнеса - это профессия и специальность

Интервью с директором Института безопасности бизнеса, действительным членом Академии проблем безопасности, обороны и правопорядка Л.М.Кунбутаевым

В. Светозаров

Летнее тепло в Москву пришло в конце мая, когда в вузах столицы начались по-настоящему жаркие денечки экзаменов. Дипломные работы представляли и в Институте безопасности бизнеса Московского энергетического института/Технического университета. Второй раз за очень недолгую историю института.

Как часто бывает, идея создания такого учебного центра родилась, когда его создатель и будущий руководитель Кунбутаев Лев Магомедович встал перед выбором - чем заниматься после увольнения из Вооруженных Сил, многолетней работы начальником Факультета военного обучения МЭИ. Тогда, несколько лет назад, в России уже сложилась в общих чертах рыночная экономика, такая, какой ее знают сегодня - коррумпированная, криминализированная, с высокими рисками. Совпадение объективных потребностей и личного желания генерал-майора запаса, профессора Кунбутаева заняться образованием в этой области привела к появлению в структуре МЭИ Института безопасности бизнеса.

Идею поддержали не сразу. Кое-кто настороженно воспринял предложение, усматривая в нем причастность к секретным службам (в общем небезосновательно, если учесть что безопасность бизнеса как сегмент рынка во многом формировался и развивался усилиями бывших сотрудников МВД, военной и гражданской разведки, контрразведки). Но поддержка ректора МЭИ, подчеркнул в беседе со мной Лев Магомедович, имела решающее значение.

Важно отметить, что при фактически незначительной рекламе конкурс поданных заявлений на прием в институт составил в прошлом году более двух человек на место. План приема студентов на дневное отделение (100 человек) в 2001 году выполнен полностью. Такой же наплыв абитуриентов ожидается и этом году.

По мнению профессора Кунбутаева, это не должно вызывать удивления: "К настоящему времени всем ясно, что в условиях рыночной экономики, особенно российской, имеется множество внешних и внутренних угроз стабильному развитию бизнеса. Даже если исключить возможность совершения мошеннических действий, фирма рискует понести ущерб в результате невысокого профессионализма управленческого персонала и сотрудников, занимающихся маркетинговыми исследованиями, деловой разведкой, безопасностью бизнеса. Сюда же можно присовокупить угрозы умышленного ущерба со стороны конкурентов и коррумпированных чиновников".

Каких специалистов готовит Институт? "Мы не разрабатывали новый государственный стандарт, - подчеркивает Лев Магомедович, - а только открыли соответствующие специализации для экономистов и управленцев: управление экономической безопасностью (специальность - "экономика и управление на предприятии") и управление предпринимательскими рисками (специальность - "менеджмент организации"). Выпускники института будут иметь систематизированные знания по информационно-аналитической работе, прежде всего по конкурентной разведке. Они также будут знать, как организовать противодействие возможной утечке коммерческой информации, представлять себе в целом систему обеспечения комплексной безопасности фирм, уметь использовать психологические знания для построения правильных взаимоотношений с коллегами и внешним партнерами".

Вернемся к выпускным экзаменам. Свои работы членам экзаменационной комиссии представили слушатели вечерних курсов (профессиональной переподготовки) института. Среди выпускников были студенты дневных факультетов МЭИ. Для них учеба в ИББ дает дополнительное образование и, видимо, как-то сообразовывается с их представлением о будущей работе. Но большинство слушателей совмещали учебу с работой в своих организациях, как правило, связанной с обеспечением безопасности бизнеса. Поэтому не удивительно, что значительная часть дипломных работ посвящена структуре систем безопасности на производстве/в компании. Практически все авторы предложенных схем включили в структуру службы безопасности подразделение конкурентной разведки, которое непосредственно подчиняется руководителю службы, но не первому лицу в компании: как принято в зарубежных компаниях. Такова российская реальность. Конкурентную службу у нас обычно воспринимают с позиций обеспечения безопасности, и реже - как инструмент формирования рыночной стратегии и тактики. Хотя проблемы безопасности и доминировали, что вполне соответствует главному профилю института, ряд представленных работ имеет прямое отношение к конкурентной разведке. С этой точки зрения интересны работы "Экономическая оценка создания службы КР на малом

предприятии" Валова Л.Е., "Психологические особенности бизнеса в России" Мещеряковой Е.В., "Методы защиты от коммерческого мошенничества" Кутергина С.А..
В этом номере журнала публикуется часть дипломной работы "Исследование механизмов правовой защиты интеллектуальной собственности и ее коммерциализация" Д.Цыпулева.

Мой последний вопрос профессору Кунбутаеву о его ближайших планах и шагах.
"Следующий шаг в развитии Института и вообще данного направления в образовании видится в разработке и сертификации новой специальности по обеспечению безопасности предпринимательской деятельности. Необходимость этого шага диктуется тем, что объем учебного времени, выделяемого на дисциплины специализации государственными образовательными стандартами, достаточно мал и составляет, например, для специальности "менеджмент организации" всего 458 часов (5% от общего количества). Причем половина из них должна быть отведена на самостоятельное изучение материала, поэтому того времени, что остается на аудиторные занятия, явно недостаточно для обстоятельного изложения дисциплин по безопасности бизнеса. С другой стороны, специализация - это еще не специальность. Я надеюсь, что обоснованное мнение о необходимости введения специальности, назовем ее "Управление экономической безопасностью", найдет понимание и поддержку в Министерстве образования РФ. Но пока такой специальности нет, компании и банки могут воспользоваться услугами нашего и некоторых других вузов для повышения уровня профессионализма своих сотрудников в сфере безопасности бизнеса".

Учебные центры для деловой равзедки

Учебные центры для деловой разведки

Бизнес испытывает острый дефицит квалифицированных кадров для деловой разведки, - к такому выводу пришли в Исследовательском центре Гартнера. По словам директора центра Ф. Байтенджика, через пару – тройку лет западные компании будут иметь дело с таким мощным массивом данных, что им потребуется втрое больше аналитиков, чем они располагают сегодня, чтобы успешно управлять информацией. (Computing, 30 мая 2002).

Реально возможный рост числа подготовленных специалистов по информационному менеджменту едва ли покроет половину потребностей.

Учитывая жизненно важное значение для бизнеса современных информационных технологий, Байтенджик предлагает предпринимателям подумать о создании учебных центров подготовки специалистов деловой разведки (business intelligence competency centers).Но, понятно, немногие компании даже в развитых странах мира могут позволить себе иметь такие центры, особенно сейчас, в период затянувшейся рецессии.

«Человеческий фактор» в защите прав на интеллектуальную собственность

«Человеческий фактор» в защите прав на интеллектуальную собственность

Что делать, когда не удается публично поймать за руку тех, кто покушается на священное право интеллектуальной собственности?

Использовать «нетрадиционные методы деловой разведки», считает Алден Тэйлор, старший управляющий директор нью-йоркской компании Citigate Global Intelligence & Security.

В статье, опубликованой The Lawyers Weekly (21 июня 2002), он признает, что предлагаемые им методы сбора информации о пиратах интеллектуальной собственности «некоторые могут отнести к корпоративному шпионажу», но на самом деле, они, по его мнению, и легальны, и этичны.

Тэйлор приводит случай, когда одной компании удалось получить свидетельство о краже ее патента конкурентом: который наводнил рынок дешевыми копиями дорогостоящего продукта.

Нужные сведения были получены во время ужина со служащим пиратской компании, но этому предшествовала большая и кропотливая разработка потенциального источника информации. Сложность состояла в том, что недобросовестный конкурент представлял собой зарубежную фирму, действующую в стране с иным бизнес климатом, другим законодательством и культурой общения. Нанятые эксперты хорошо вошли в эту культурную среду, смогли установить добрые человеческие контакты со служащим конкурентной фирмы, разговорить его в неофициальной обстановке. Выданная им информация о том, каким образом фирме, где он работал, удалось приникнуть в чужие секреты, была чрезвычайно важной. Тэйлор настаивает, что использованные методы для ее получения «никоим образом не нарушили стандарты корпоративной этики и носили вполне правовой характер».

Автор подчеркивает, что человеческий фактор в деловой разведке играет определяющую роль. Это он называет «творческим персональным подходом ». И если речь идет о разведке относительно зарубежных компаний, обязательно должны учитываться особенности национальной культуры и ценностей, системы государственного управления и местного рынка.

По его словам, использование человеческого фактора в противодействии посягательствам на право интеллектуальной собственности помогает эффективно решать задачу по охране своих прав. Более того, успешная стратегия деловой разведки с использованием этого фактора нужна с профилактической точки зрения как предупреждение конкурентам, что любая попытка нарушить право интеллектуальной собственности неосмотрительна и не продуктивна.

Прозрачность хороша, но в меру

Прозрачность хороша, но в меру

Обзор по материалам международной прессы подготовлен В. Борисовым

Массовое использование западными предпринимателями Интернет пространства для рекламы, PR и работы с клиентами, партнерами, поставщиками открыло огромные возможности для поиска и нахождения конкурентной информации. Собственно, появление Всемирной Паутины во многом предопределило развитие конкурентной разведки в качестве самостоятельного вида экономической деятельности Увлечение веб-технологиями, с одной стороны, и требования прозрачности, возведенные в

фундаментальный принцип современной культуры бизнеса, - с другой, сделали многие корпорации, компании весьма уязвимыми для заинтересованного взгляда извне. По оценке некоторых экспертов, открытый Интернет и платные онлайновые информационные системы дают до 80% ценной информации, искомой конкурентами.

В этом контексте показателен случай, приведенный в Computerworld (04.01.2002). В ходе процесса поглощения компании Exodus Communications фирмой Cable & Wireless PLC. руководитель службы безопасности Exodus Билл Хэнкок привез на переговоры и представил 700 страничное досье на Cable & Wireless. Вся содержащаяся в нем информация была “накопана” в открытых источниках Интернета. Как он объяснил, возглавляемой им службе КР удалось собрать богатую информацию о структуре, персонале, доходах, клиентской базе и многом другом. Представители Cable & Wireless были неприятно удивлены масштабами и глубиной информации, которая оказалась в распоряжении Exodus. Но, по словам Хэнкока, сбор такой информации по основным конкурентам и потенциальным клиентам - дело обычное, которым его сотрудники занимались ежедневно.

Наилучший ресурс для сбора разведывательной информации - корпоративные сайты, в которых часто можно почерпнуть важную информацию о персонале, стратегии, планах, клиентах конкурирующей фирмы. Особую ценность для конкурентов представляют связанные линками информационные ресурсы других фирм - поставщиков, партнеров, дистрибьюторов и т.п.

Джей МакГональ, автор семи книг по конкурентной разведке и управляющий партнер в компании Helicon Group, приводит пример из собственной практики. Однажды по заказу провайдера программного обеспечения фирмы. А ему предстояло выяснить степень готовности ее конкурента, компании Б, выбросить на рынок рекламируемую новую веб-платформу. Внимательно просмотрев веб-сайт компании, МакГональ не нашел там ничего ценного. Тогда он занялся линками сайта и вышел, в частности, на одного консультанта, который в телефонном разговоре подтвердил, что работал над искомым проектом, но в его ранней фазе. Надо было найти специалистов, которые трудились над проектом на более поздних этапах. МакГональ стал просматривать веб-страницы компаний, специализирующихся в соответствующем сегменте технологий, стараясь выявить какую либо связь с фирмой Б. И он нашел название этой фирмы в списке клиентов одной из компаний. Остальное было делом техники и немного удачи. Телефонные звонки в компанию и осторожные расспросы о контракте с фирмой Б позволили выяснить, что объект расследования явно не готов выпустить разрекламированную продукцию в объявленные сроки. Что и требовалось узнать.
По мнению МакГонеля, урок состоит в необходимости постоянно проверять информационную уязвимость партнеров, которые имеют линки на корпоративные сайты. Кроме того, хотя бы время от времени посещать сайты не имеющих линки поставщиков и других партнеров, клиентов, и внимательно смотреть, кто и в какой связи упоминает их компанию.

Практика работы в Интернете убеждает, как важно тщательно проверять информацию, запускаемую в открытый Интернет, даже если она выглядит вполне невинно, как, скажем, объявления о вакансиях. Анализ МакГоналем подобной информации на сайте одной розничной компании в сочетании с источниками местной прессы позволили ее конкуренту с большой точностью вероятности узнать, где и сколько новых торговых точек данная компания собирается открывать. МакГонель делает вывод, что нельзя в открытом доступе давать слишком много косвенной информации, то объявление о вакансиях или другое аналогичное объявление.

Такой подход разделяет пресс-секретарь компании Кодак Герард Мечнер: “К примеру, мы каждый год предоставляем в открытом доступе информацию, сколько тратим средств на исследования (R&D), но никогда не даем разбивку с указанием, сколько денег затрачено на разработку каждого отдельного продукта” (Marketplace, 03.28.2002)

Эксперты по безопасности бизнеса в США считают, что американские компании в отличие от предпринимателей АТР и Европы, более беззаботны в этом отношении, чем и пользуются конкуренты. И дают совет: прежде чем выпускать информацию в Интернет – надо хорошенько взглянуть на нее глазами конкурентов и попытаться определить, что в ней они могут найти ценного и использовать в собственных интересах. Если этому совету последуют все компании, то, как мне кажется, для профессионалов конкурентной разведки

настанут трудные времена.

Интеллектуальных_преступлений становится все больше

Интеллектуальных преступлений становится все больше

Развитие компьютерных технологий наряду с другими факторами экономического и социального прогресса способствует росту финансовых махинаций и злоупотреблений. К такому выводу приходят американские эксперты, анализируя изменения последних лет в криминальной жизни США (The New York Times, 2 июня 2002).

Отмечается, в частности, что число убийств, ограблений и других “классических” видов покушения на здоровье имущество граждан уменьшается. В то же время резко увеличилось количество преступлений в экономической сфере - финансовые махинации, ложное банкротство, интеллектуальное пиратство, корпоративный шпионаж.

Отмеченные тенденции, полагают аналитики, связаны с изменениями, которые происходят в современном высокоразвитом обществе, в частности, с развитием компьютерных технологий, которые активно используются преступниками “в белых воротничках”. Не случайно, рекордное число финансовых преступлений фиксируется в сфере программного обеспечения и телекоммуникаций.

Распространению мошенничества и финансовых злоупотреблений способствуют также демографические изменения в американском обществе, в том числе, повышение образовательного уровня и увеличение продолжительности жизни. Поскольку считается, что преступность интеллектуального плана характерна прежде всего для людей среднего и пожилого возраста, старение общества сопровождается ростом числа именно таких преступлений.

Американское КГБ будет заниматься анализами

Американское "КГБ" будет заниматься анализами

В конгрессе проходят слушания, посвященные объединению федеральных служб безопасности под крышей нового министерства – внутренней безопасности. Одна из целей новоиспеченного ведомства – упорядочения потоков информации и достижение совместимости (interoperability) коммуникационной компьютерной технологии, используемой ФБР, ЦРУ и другими службами.

ФБР уже сегодня задыхается от информационного массива, подчеркивает эксперт в области национальной безопасности США, профессор Университета штата Джорджия Л. Джонсон (The Associated Press, 31 мая 2002). Этот океан информации представлен на разных носителях – фотографии, бумажные файлы, видео сюжеты, телефонные и радио перехваты, электронная почта. И все это надо сводить к одному формату, систематизировать, сортировать, анализировать и хранить так, чтобы любой из документов

мог быть востребован и немедленно получен. И в этом деле без помощи «Силиконовой Долины» не обойтись, отмечают наблюдатели. Действуя разрозненно, каждое из федеральных агентств неохотно делилось своей информацией с коллегами. К тому они пользуются разными компьютерными информационными системами. Одни из них не способны проводить технологически изощренный поиск, другие не могут работать с хорошо защищенными системами электронной почты. В этом смысле, крупные частные корпорации ушли далеко вперед в приобретении и использовании многофункциональных, интегрированных информационных систем.

Как отмечают высокопоставленные представители Белого Дома, новое министерство не будет заниматься сбором информации, оставив эту функцию за действующими службами. В задачу министерства, куда будет стекаться все важные сведения, касающиеся обеспечения безопасности, будет входить ее анализ и подготовка соответствующих рекомендаций оперативного и перспективного характера. Совершенно очевидно, что такой подход администрации Буша во многом учитывает разворачивающуюся в печати критику по фактам игнорирования в верхнем и среднем эшелоне власти поступивших в свое время сигналов о возможной террористической акции, которая и произошла 11 сентября прошлого года.

Любопытен еще один момент проходящих слушаний. Сенатор Беннет предложил поправку к Закону о свободе информации, которая бы позволила засекречивать поступающую от общественности (в том числе бизнеса) информацию, если она представляет интерес с точки зрения безопасности. Сторонники поправки аргументируют свою позицию тем, что требование публичного доступа к такой информации, вытекающее из упомянутого закона, не поощряет ее носителей к тому, чтобы поделиться с правительством, так как она нередко несет одновременно и коммерческий характер, а, следовательно, может быть использована конкурентами. Противники поправки возражают, подчеркивая, что она затронет основы, гарантирующие прозрачность власти и приведет к уплотнению завесы секретности, которая и без поправки достаточно надежно предохраняет от утечки информацию: связанную с национальной безопасностью.

Правительство Японии рассматривает защитные меры против промышленного шпионажа

Правительство Японии рассматривает защитные меры против промышленного шпионажа

Правительство Японии серьезно озабочено уроном, который наносит экономике страны промышленный шпионаж и планирует предпринять серьезные, прежде всего законодательные шаги с целью уменьшить эту угрозу.

Комитет по защите прав на интеллектуальную собственность, совещательный орган при кабинете министров, подготовил доклад, содержащий основные направления политики, рекомендуемые для правительства. Ключевым моментом документа является попытка распространить право защиты интеллектуальной собственности на конфиденциальную деловую информацию.

По мнению наблюдателей, нынешнее законодательство Японии в этом смысле весьма ущербно. Оно не рассматривает информацию о фирменных технологиях и других, обычно скрываемых от постороннего глаза вещах как “существенную” с точки зрения уголовного кодекса, и таким образом не трактует кражу коммерческих секретов как уголовно наказуемое деяние.

Между тем, масштабы краж коммерческих секретов из японских фирм принимают

катастрофический характер, пишет токийская газета “The Daily Yomiuri” (4 июня 2002). Проведенный осенью 2001 года опрос предпринимателей дал ошеломляющие результаты: 234 из опрошенных 289 фирм сталкиваются с фактами утечки конфиденциальной информации. Это в основном информация, связанная с технологиями, организацией и методами производства, клиентской базой, маркетинговыми исследованиями.

Самый распространенный путь “ухода” информации - через бывших сотрудников. Несмотря на корпоративно-семейные традиции японского бизнеса, лояльность служащих выглядит не столь уж безупречной, как нередко представляется со стороны.

Чтобы хоть как-то противодействовать эпидемии “увода” информации, составляющей коммерческую тайну, в правительстве рассматривают предложение о внесении поправок в действующее законодательство, предусматривающих судебное преследование за такие деяния, а также компенсацию за понесенный ущерб.

Промышленный шпионаж против США. Россия тоже в "черном списке"

Промышленный шпионаж против США. Россия тоже в "черном списке"

Обзор по американской прессе подготовил В. Светозаров

По мнению американских наблюдателей, промышленный шпионаж начинает серьезно угрожать национальным интересам мощнейшей страны мира. То, что США, где ежегодные расходы на технологические разработки и исследования достигают астрономической суммы 600 млрд. долларов, является основным объектом международного корпоративного шпионажа, не удивляет. Как считают в ФБР, в промышленном шпионаже против США участвуют правительственные секретные службы многих стран, включая ближайших союзников и партнеров. Во время слушаний в Конгрессе представители этого агентства, на которое возложены функции противодействия корпоративному шпионажу извне, огласило список 23 стран, где эта деятельность неофициально осуществляется государственными разведывательными службами. В этом списке наряду с Израилем, Англией, Германией, Францией значится и Россия (UPI, 05.15.2002).

Методы шпионажа варьируются от традиционных (кражи, подкуп) до современных, с использованием технологий. Для достижения результата применяются все мыслимые и немыслимые способы и пути, как-то: слияния и поглощения, совместные предприятия и партнерства, международные программы обменов и общественные организации. Втянутые в промышленный шпионаж государственные службы активно вербуют иностранных студентов и служащих, переводчиков, консультантов, лоббистов, журналистов и т.п. используются различные международные форумы: выставки, ярмарки, научные симпозиумы и конференции.

Принятый Конгрессом США в 1996 году Акт о промышленном шпионаже не оправдал возлагавшиеся на него надежды. За пять лет зафиксировано всего 30 случаев судебного разбирательства по этому закону – смехотворно мало с учетом огромных масштабов экономического шпионажа, ущерб от которого не поддается реальному исчислению. Самое малое 250 млрд. долларов потеряли США от кражи коммерческих секретов в 2001 году. Такую цифру назвал ведущий программы финансовых новостей CNN 20 мая 2002 Аллан Чернов в беседе с экономическими экспертами С.Финком и Дж. Сэведжем. Оба гостя программы выразили озабоченность, что правительство США, по их мнению, не уделяет проблеме достаточного внимания. Более того, начавшаяся кампания борьбы с терроризмом потребовала перераспределения сил и ресурсов федеральных служб безопасности, в первую очередь ФБР, в ущерб противодействию промышленному шпионажу. На борьбу с террористами мобилизовано до 75 процентов штатных сотрудников ФБР (С.Финк) за счет

других направлений.
Вывод: спасение утопающих – дело рук самих утопающих. Эксперты советуют бизнесменам предпринять три необходимые меры, чтобы хоть как-то защитить компанию от корпоративных шпионов. Во-первых, определить, какая производственная информация должна храниться в секрете (многие даже об этом не думают). Во-вторых, предпринять действенные шаги по охране секретов. В-третьих, разъяснить всем служащим компании, что такое коммерческая тайна, как к ней подходить и как оберегать.

Конвенция о киберпреступности

КОНВЕНЦИЯ О КИБЕРПРЕСТУПНОСТИ

Преамбула

Государства-члены Совета Европы и другие государства, подписавшие настоящую Конвенцию,

учитывая, что цель Совета Европы состоит в достижении большей степени единства между его членами;

признавая важность укрепления сотрудничества с другими государствами, подписавшими настоящую Конвенцию,

будучи убеждены в необходимости проведения в приоритетном порядке общей политики в сфере уголовного права, нацеленной на защиту общества от киберпреступности, в том числе путем принятия соответствующих законодательных актов и укрепления международного сотрудничества,

сознавая глубокие перемены, вызванные внедрением цифровых технологий, объединением и продолжающейся глобализацией компьютерных сетей,

будучи озабочены угрозой того, что компьютерные сети и электронная информация могут также использоваться для совершения уголовных преступлений и что доказательства совершения таких правонарушений могут храниться в этих сетях и передаваться по ним,

признавая необходимость сотрудничества между государствами и частным сектором в борьбе против киберпреступности и необходимость защиты законных интересов в сфере использовании и развития информационных технологий;

полагая, что для эффективной борьбы против киберпреступности требуется более широкое, оперативное и хорошо отлаженное международное сотрудничество в области уголовного права,

будучи убеждены в том, что настоящая Конвенция необходима для сдерживания действий, направленных против конфиденциальности, целостности и доступности компьютерных систем и сетей и компьютерных данных, а также против злоупотребления такими системами, сетями и данными, путем обеспечения уголовной наказуемости таких деяний, описываемых в настоящей Конвенции, и предоставления полномочий, достаточных для эффективной борьбы с такими уголовными преступлениям, путем содействия выявлению и расследованию таких уголовных преступлений и судебному преследованию за их совершение как на внутригосударственном, так и на международном уровнях, и путем разработки договоренностей относительно оперативного и надежного международного сотрудничества,

памятуя о необходимости обеспечения должного баланса между интересами поддержания правопорядка и уважением основополагающих прав человека, как это предусмотрено Конвенцией Совета Европы о защите прав человека и основных свобод от 1950 года, Международным пактом Организации Объединенных Наций о гражданских и политических правах от 1966 года и также другими применимыми международными договорами о правах человека, в которых подтверждается право каждого беспрепятственно придерживаться

своих мнений, а также право на свободное выражение своего мнения, включая свободу искать, получать и распространять всякого рода информацию и идеи, независимо от государственных границ и права, касающегося невмешательства в личную жизнь;

памятуя также о праве на охрану личных данных, предусмотренном, например, в Конвенции Совета Европы 1981 года о защите физических лиц при автоматизированной обработке данных личного характера,

учитывая положения Конвенции Организации Объединенных Наций о правах ребенка от 1989 года и Конвенции, принятой Международной Организацией Труда о наихудших формах детского труда от 1999 года,

принимая во внимание действующие конвенции Совета Европы о сотрудничестве в пенитенциарной сфере, а также аналогичные договоры, заключенные между государствами-членами Совета Европы и другими государствами, и подчеркивая, что настоящая Конвенция призвана служить дополнением к этим договорам в целях повышения эффективности уголовных расследований и процессуальных действий в отношении уголовных преступлений, связанных с компьютерными системами и компьютерными данными, а также обеспечения возможности сбора доказательств в электронной форме совершения уголовного преступления,

приветствуя события последнего времени, способствующие дальнейшему росту международного взаимопонимания и сотрудничества в борьбе с киберпреступностью, включая меры, принятые Организацией Объединенных Наций, ОЭСР, Европейским Союзом и "Группой восьми",

напоминая о Рекомендациях Комитета Министров № R (85) 10 относительно практического применения Европейской конвенции о взаимной правовой помощи по уголовным делам в том, что касается судебных поручений о перехвате телекоммуникационных сообщений, № R (88) 2 о борьбе с пиратством в области авторского права и смежных прав, № R (87) 15 о порядке использования личных данных полицией, №R(95) 4 о защите личных данных в сфере телекоммуникационных услуг, в особенности телефонных услуг, а также № R (89) 9 о преступлениях, связанных с компьютерами, в которой изложены руководящие принципы для национальных законодательных органов в отношении определения некоторых компьютерных преступлений, и №R(95) 13 по проблемам уголовно-процессуального права, связанным с информационными технологиями.

принимая во внимание Резолюцию № 1, принятую на 21-ой Конференции министров юстиции стран Европы (Прага, июнь 1997 г.),. в которой Комитету Министров было рекомендовано поддержать проводимую Европейским комитетом по проблемам преступности (ЕКПП) работу по киберпреступности, чтобы обеспечить большую согласованность положений внутреннего уголовного права и сделать возможным использование эффективных средств расследования таких правонарушений, а также принятую на 23-ей Конференции министров юстиции стран Европы (Лондон, июнь 2000 г.) Резолюцию № 3, побуждающую участвующие в переговорах стороны продолжать усилия с целью нахождения таких решений, которые позволят как можно большему числу государств стать участниками Конвенции, и подтверждающую необходимость создания оперативной и эффективной системы международного сотрудничества, должным образом учитывающей специфические потребности борьбы с киберпреступностью,

принимая во внимание также одобренный на Втором совещании глав государств и правительств Совета Европы (Страсбург, 10-11 октября 1997 г.) План действий по поиску общих мер реагирования на развитие новых информационных технологий на основе норм и ценностей, принятых в Совете Европы,

согласились о нижеследующем:

Глава I - Использование терминов

Статья 1 - Определения

Для целей настоящей Конвенции:

a. ''компьютерная система" означает любое устройство или группу взаимосвязанных или

смежных устройств, одно или более из которых, действуя в соответствии с программой, осуществляет автоматизированную обработку данных;

b. "компьютерные данные" означают любое представление фактов, информации или понятий в форме, подходящей для обработки в компьютерной системе, включая программы, способные заставить компьютерную систему выполнять ту или иную функцию;

c. ''поставщик услуг" означает:

(i) любую государственную или частную структуру, которая обеспечивает пользователям ее услуг возможность обмена информацией посредством компьютерной системы, и

(ii) любую другую структуру, которая осуществляет обработку или хранение компьютерных данных от имени такой службы связи или пользователей такой службы.

d. "данные о потоках" означают любые компьютерные данные, относящиеся к передаче информации через посредство компьютерной системы, которые генерируются компьютерной системой, являющейся составной частью соответствующей коммуникационной цепочки, и указывают на источник, назначение, маршрут, время, дату, размер, продолжительность или тип соответствующего сетевого сервиса.

Глава II - Меры, которые следует принять на национальном уровне Раздел 1 - Материальное уголовное право

Подраздел 1 - Преступления против конфиденциальности, целостности и доступности компьютерных данных и систем

Статья 2 - Противозаконный доступ

Каждая Сторона принимает такие законодательные и иные меры. которые могут быть необходимы для того, чтобы квалифицировать в качестве уголовного преступления согласно ее внутригосударственном} праву доступ, когда он является преднамеренным, к компьютерной системе в целом или любой ее части без права на это. Любая Сторона может требовать, чтобы такие деяния считались преступными, если они совершены с нарушениями мер безопасности и с намерением завладеть компьютерными данными или иным злым умыслом, или в отношении компьютерной системы, соединенной с другой компьютерной системой.

Статья 3 - Противозаконный перехват

Каждая Сторона принимает такие законодательные и иные меры, которые могут быть необходимы для того, чтобы квалифицировать в качестве уголовного преступления согласно ее внутригосударственному праву -преднамеренно осуществленный с использованием технических средств перехват без права на это - не предназначенных для общего пользования компьютерных данных, передаваемых в компьютерную систему, из нее или внутри такой системы, включая электромагнитные излучения компьютерной системы, несущей такие компьютерные данные. Любая Сторона может требовать, чтобы такое деяние считалось преступным, если оно было совершено со злым умыслом или в отношении компьютерной системы, соединенной с другой компьютерной системой.

Статья 4 - Воздействие на данные

1. Каждая Сторона принимает такие законодательные и иные меры, которые могут быть необходимы для того, чтобы квалифицировать в качестве уголовного преступления согласно ее внутригосударственному праву преднамеренное повреждение, удаление, ухудшение качества, изменение или блокирование компьютерных данных без права на это.

2. Любая Сторона может зарезервировать за собой право квалифицировать в качестве уголовного преступления только те предусмотренные пунктом 1 деяния, которые влекут за собой серьезный ущерб.

Статья 5 - Воздействие на функционирование системы

Каждая Сторона принимает такие законодательные и иные меры, которые могут быть необходимы для того, чтобы квалифицировать в качестве уголовного преступления

согласно ее внутригосударственному праву преднамеренное создание - без права на это - серьезных помех функционированию компьютерной системы путем ввода, передачи, повреждения, удаления, ухудшения качества, изменения или блокирования компьютерных данных.

Статья 6 - Противозаконное использование устройств

1. Каждая Сторона принимает такие законодательные и иные меры, которые могут быть необходимы для того, чтобы квалифицировать в качестве уголовного преступления согласно ее внутригосударственному п^аву нижеследующие деяния в случае их совершения преднамеренно и без права на это:

(a) производство, продажа, приобретение для использования, импорт, оптовая продажа или иные формы предоставления в пользование:

i. устройств, включая компьютерные программы, разработанных или адаптированных прежде всего для целей совершения какого-либо из правонарушений, предусмотренных выше в статьях 2-5;

ii. компьютерных паролей, кодов доступа или иных аналогичных данных, с помощью которых может быть получен доступ к компьютерной системе в целом или любой ее части с намерением использовать их с целью совершения какого-либо из правонарушений, предусмотренных в статьях 2 - 5; и

(b) владение одним из предметов, упомянутых в пунктах i (a) или ii (a) выше, с намерением использовать его для совершения каких-либо правонарушений, предусмотренных в статьях 2-5. Любая Сторона может требовать в соответствии с законом, чтобы условием наступления уголовной ответственности являлось владение несколькими такими предметами.

2. Настоящая статья не должна толковаться как устанавливающая уголовную ответственность в тех случаях, когда производство, продажа, приобретение для использования, импорт, оптовая продажа или иные формы предоставления в пользование или владение, упомянутые в пункте 1 данной статьи, не имеют целью совершение правонарушений, предусмотренных статьями 2-5 настоящей Конвенции, а связаны, например, с разрешенным испытанием или защитой компьютерной системы.

3. Сторона может зарезервировать за собой право не применять положения пункта 1 настоящей статьи при условии, что такая оговорка не будет касаться продажи, оптовой продажи или иных форм предоставления в пользование предметов, указанных в подпункте (a) П пункта 1.

Подраздел 2 - Правонарушения, связанные с использованием компьютерных средств

Статья 7 - Подлог с использованием компьютерных технологий

Каждая Сторона принимает такие законодательные и иные меры, которые могут быть необходимы для того, чтобы квалифицировать в качестве уголовных преступлений согласно ее внутригосударственному праву - в случае совершения преднамеренно и без права на это - ввод, изменение, стирание или блокирование компьютерных данных влекущих за собой нарушение аутентичности данных с намерением, чтобы они рассматривались или использовались в юридических целях в качестве аутентичных, независимо от того, поддаются ли эти данные непосредственному прочтению и являются ли они понятными. Любая Сторона может требовать для наступления уголовной ответственности наличия намерения совершить обман или аналогичного злого умысла.

Статья 8 - Мошенничество с использованием компьютерных технологий

Каждая Сторона принимает такие законодательные и иные меры, которые могут быть необходимы, для того чтобы квалифицировать в качестве уголовных преступлений согласно ее внутригосударственному праву - в случае совершения преднамеренно и без права на это - лишение другого лица его собственности путем:

a) любого ввода, изменения, удаления или блокирования компьютерных данных,

b) любого вмешательства в функционирование компьютерной системы, с мошенническим или бесчестным намерением неправомерного извлечения экономической выгоды для себя или для иного лица.

Подраздел 3 - Правонарушения, связанные с содержанием данных

Статья 9 - Правонарушения, связанные с детской порнографией

1. Каждая Сторона принимает такие законодательные и иные меры, которые могут быть необходимы для того, чтобы квалифицировать в качестве уголовных преступлений согласно ее внутригосударственному праву - в случае совершения преднамеренно и без права на это - следующих деяний:

a) производство детской порнографической продукции с целью распространения через компьютерную систему;

b) предложение или предоставление в пользование детской порнографии через компьютерную систему;

c) распространение или передача детской порнографии через компьютерную систему;

d) приобретение детской порнографии через компьютерную систему для себя или для другого лица;

e) владение детской порнографией, находящейся в компьютерной системе или на носителях компьютерных данных.

2. Для целей пункта 1 настоящей Статьи в понятие "детской порнографии" включаются порнографические материалы, изображающие:

(a) участие несовершеннолетнего лица в откровенных сексуальных действиях;

(b) участие лица, кажущегося несовершеннолетним, в откровенных сексуальных действиях;

(c) реалистические изображения несовершеннолетнего лица, участвующего в откровенных сексуальных действиях.

3. Для целей вышеприведенного пункта 2 термин "несовершеннолетние" означает любое лицо, не достигшее 18-летнего возраста. Однако любая Сторона может устанавливать и более низкие возрастные пределы, но не ниже 16 лет.

4. Каждая Сторона может зарезервировать за собой право не применять, полностью или частично, положения пунктов 1 d) и 1 e), а также 2 b) и 2 c).

Подраздел 4 - Правонарушения, связанные с нарушением авторского права и смежных прав

Статья 10 - Правонарушения, связанные с нарушением авторского права и смежных прав

1. Каждая Сторона принимает такие законодательные и иные меры, которые могут быть необходимы для того, чтобы квалифицировать в качестве уголовного преступления согласно ее внутригосударственному праву нарушений авторского права, как они определены в законодательстве этой Стороны во исполнение обязательств, взятых ею на себя по Парижскому от 24 июля 1971 года, пересматривающему Бернскую конвенцию об охране литературных и художественных произведений, по Соглашению о торговых аспектах прав интеллектуальной собственности и по Договору об авторском праве Всемирной организации интеллектуальной собственности (ВОИС). когда такие действия совершаются преднамеренно, в коммерческом масштабе и с помощью компьютерной системы за исключением любых моральных прав, предоставляемых этими Конвенциями.

2. Каждая Сторона принимает такие законодательные и иные меры, которые могут быть

необходимы для того, чтобы квалифицировать в качестве уголовных преступлений согласно внутригосударственному праву нарушения прав, связанных с авторским правом, как оно определено законодательством этой Стороны во исполнение обязательств, взятых ею на себя по Международной конвенции об охране интересов артистов-исполнителей, производителей фонограмм и вещательных организаций (Римская конвенция). Соглашению о торговых аспектах прав интеллектуальной собственности и Договору ВОИС об исполнителях и фонограммах, когда такие акты совершены преднамеренно, в коммерческом масштабе и с помощью компьютерной системы за исключением любых моральных прав, предоставляемых этими Любая Сторона может зарезервировать за собой права в некоторых обстоятельствах не привлекать виновных к уголовной ответственности согласно положениям пунктов 1 и 2 настоящей статьи, при условии, что имеются другие эффективные средства правовой защиты и что такая оговорка не ведет к частичному повышению Стороной своих международных обязательств, предусмотренных в международных документах, упомянутых в пунктах I и 2 настоящей статьи.

Подраздел 5 -Дополнительные виды ответственности и санкции

Статья 11 - Покушение, соучастие или подстрекательство к совершению преступления

1. Каждая Сторона принимает такие законодательные и иные меры, какие могут оказаться необходимыми для того, чтобы квалифицировать в качестве уголовных преступлений согласно ее внутригосударственному праву - в случае, когда это делается преднамеренно, - соучастие или подстрекательство к совершению любого правонарушения, предусмотренного положениями статей 2-10 настоящей Конвенции.

2. Каждая Сторона принимает такие законодательные и иные меры, какие могут потребоваться для того, чтобы квалифицировать в качестве уголовных преступлений согласно ее внутригосударственному праву - в случае, когда это делается преднамеренно, - покушения на совершение любого правонарушения, предусмотренного положениями статей 3-5, 7, 8, 91)a и 91)c настоящей Конвенции.

3. Каждое Государство может зарезервировать за собой право не применять, полностью или частично, положения пункта 2 настоящей статьи.

Статья 12 - Корпоративная ответственность

1. Каждая Сторона принимает такие законодательные и иные меры, какие могут быть необходимы для обеспечения возможности привлечения юридических лиц к ответственности за уголовное преступление, предусмотренное в соответствии с настоящей Конвенцией, которое совершается в его пользу любым физическим лицом, действующим индивидуально или как часть одного из органов соответствующего юридического лица и занимающим ведущее положение него на основании:

(a) полномочий представлять данное юридическое лицо:

(b) права принимать решения от имени этого юридического лица;

(c) права осуществлять контроль внутри этого юридического лица.

2. В дополнение к случаям, уже предусмотренным в пункте 1 настоящей статьи, каждая Сторона принимает меры, необходимые для обеспечения возможности возложения ответственности на юридическое лицо в случаях. когда отсутствие руководства или контроля со стороны физического лица, упомянутого в пункте 1, делает возможным совершение уголовного преступления, предусмотренного положениями настоящей Конвенции, в пользу этого юридического лица физическим лицом, действующим на основании данных ему полномочий.

3. В зависимости от применяемых соответствующей Стороной юридических принципов ответственность юридического лица может носить уголовный, гражданский или административный характер.

4. Такая ответственность не влечет за собой какого-либо смягчения и не снижает уголовной ответственности физических лиц, совершивших преступление.

Статья 13 - Санкции и меры

1. Каждая Сторона принимает такие законодательные и иные меры, какие могут быть необходимы для обеспечения того, чтобы к лицам совершившим уголовные преступления, предусмотренные в соответствии с положениями статей 2-11, эффективные, соразмерные и убедительные меры наказания, включая лишение свободы.

2. Каждая Сторона гарантирует, что к юридическим лицам, считающимся ответственными в соответствии с положениями статьи 12, будут применены эффективные, соразмерные и убедительные меры наказания уголовного или не уголовного характера, включая денежные санкции.

Раздел 2 - Процессуальное законодательство

Подраздел 1 - Общие положения

Статья 14 - Сфера применения процессуальных норм

1. Каждая Сторона принимает такие законодательные и иные меры, какие могут быть необходимы для установления полномочий и процедур, предусмотренных положениями настоящего Раздела в целях проведения конкретных уголовных расследований или судебного разбирательства.

2. За исключением случаев, когда положениями статьи 21 конкретно предусматривается иное, каждая Сторона применяет полномочия и процедуры, упомянутые в пункте 1 настоящей Статьи, в отношении:

(a) уголовных преступлений, предусмотренных в соответствии со статьями 2-11 настоящей Конвенции;

(b) других уголовных преступлений, совершенных при помощи компьютерной системы; и

(c) сбора доказательств в электронной форме уголовного преступления.

3. (a) Каждая Сторона может сделать оговорку о сохранении за собой права применять меры, упомянутые в статье 20, только в отношении правонарушений или категорий правонарушений, указанных в этой оговорке, при условии, что круг таких правонарушений или категорий правонарушений не более ограничен, чем круг правонарушений, к которым она применяет меры, предусмотренные в статье 21. Каждая Сторона рассматривает пути ограничения сферы действия такой оговорки, чтобы сделать возможным максимально широкое применение мер, упомянутых в статье 20. (b) В том случае, когда Сторона, ввиду ограничений в своем законодательстве, действующем на момент принятия настоящей Конвенции, не имеет возможности применить меры, предусмотренные статьями 20 и 21, к информации, передаваемой по компьютерной системе поставщика услуг, которая

i используется для обслуживания замкнутой группы пользователей, и

ii не использует общественных сетей связи, а также не соединена ни с какими другими компьютерными системами, будь то общественными или частными,

эта Сторона может зарезервировать за собой право не применять указанных мер к такой передаче информации. Каждая Сторона рассматривает пути ограничения этого права с тем, чтобы сделать возможным максимально широкое применение мер, упомянутых в Статьях 20 и 21.

Статья 15 - Условие и гарантии

1. Каждая Сторона обеспечивает, чтобы установление, исполнение и применение полномочий и процедур, предусмотренных в настоящем Разделе, осуществлялись в соответствии с условиями и гарантиями, предусмотренными нормами ее внутригосударственного права, обеспечивающими надлежащую защиту прав человека и свобод, включая права, вытекающие из обязательств, которые Сторона взяла на себя по Европейской конвенции о защите прав человека и основных свобод, принятой Советом Европы в 1950г. Международным пактом о гражданских и политических правах, принятым Организацией Объединенных Наций в 1966 г., а также другими применимыми

международными договорами по правам человека, и предусматривающими принцип соразмерности.

2. Такие условия и гарантии с учетом характера полномочии и процедур, включают, среди прочего, судебный или иной независимый надзор, основания правомочности применения, ограничение сферы и сроков действия таких полномочий или процедур.

3. В той мере, в какой это соответствует общественным интересам, в частности, обоснованному отправлению правосудия, Сторона рассматривает влияние предусмотренных в данном Разделе полномочий и процедур на права, ответственность и законные интересы третьих сторон.

Подраздел 2 - Оперативное обеспечение сохранности накопленных компьютерных данных

Статья 16 - Оперативное обеспечение сохранности хранимых компьютерных данных

1. Каждая Сторона принимает такие законодательные и иные меры, какие могут быть необходимы для того, чтобы ее компетентные органы имели возможность отдавать распоряжения или соответствующие указания об оперативном обеспечении сохранности конкретных компьютерных данных, включая данные о потоках информации, которые хранятся в компьютерной системе, в частности, когда имеются основания полагать, что эти компьютерные данные особенно подвержены риску утраты или изменения.

2. Если Сторона реализует положения приведенного выше пункта 1 посредством отдания распоряжения какому-либо лицу об обеспечении сохранности конкретных хранимых компьютерных данных, находящихся во владении или под контролем этого лица, то эта Сторона принимает такие законодательные и иные меры, какие могут быть необходимы для того, чтобы обязать данное лицо хранить эти компьютерные данные и обеспечивать их целостность в течение необходимого периода времени, не превышающего 90 дней, с тем чтобы компетентные органы могли добиться раскрытия этих компьютерных данных. Сторона может предусмотреть возможность последующего возобновления действия такого распоряжения.

3. Каждая Сторона принимает такие законодательные и иные меры, какие могут быть необходимы для того, чтобы обязать хранителя или другое лицо, которому поручено обеспечивать сохранность компьютерных данных, сохранять конфиденциальность выполнения таких процедур в течение срока, предусмотренного ее внутригосударственным правом.

4. Полномочия и процедуры, упомянутые в настоящей статье, устанавливаются в соответствии с положениями статей 14 и 15.

Статья 17 - Оперативное обеспечение сохранности и частичное раскрытие данных о потоках информации

1. Каждая Сторона принимает в отношении данных о потоках информации, сохранность которых должна быть обеспечена в соответствии с положениями статьи 16, такие законодательные и иные меры, какие могут быть необходимы для того, чтобы:

(a) гарантировать, чтобы такое оперативное обеспечение сохранности данных о потоках информации было возможным независимо от того, сколько поставщиков услуг были вовлечены в передачу соответствующего сообщения - один или более; и

(b) гарантировать оперативное раскрытие компетентным органам этой Стороны или лицу, назначенному этими органами, достаточного количества данных о потоках информации, которое позволит соответствующей Стороне идентифицировать поставщиков услуг и путь, которым передавалось данное сообщение.

2. Полномочия и процедуры, упомянутые в настоящей статье, устанавливаются в соответствии с положениями статей 14 и 15.

Подраздел 3 - Распоряжение о предъявлении

Статья 18 - Распоряжение о предъявлении

1. Каждая Сторона принимает такие законодательные и иные меры, какие могут быть необходимы для того, чтобы предоставить ее компетентным органам полномочия отдавать распоряжения:

a) лицу на ее территории - о предъявлении конкретных компьютерных данных, находящихся во владении или под контролем этого лица, которые хранятся в компьютерной системе или на том или ином носителе компьютерных данных; и

b) поставщику услуг, предлагающему свои услуги на ее территории, -о предъявлении находящихся во владении или под контролем этого поставщика услуг сведений о его абонентах.

2. Полномочия и процедуры, упомянутые в настоящей статье, устанавливаются в соответствии с положениями статей 14 и 15.

3. Для целей настоящей статьи термин "сведения об абонентах" означает любую имеющуюся у поставщика услуг информацию о его абонентах в форме компьютерных данных или любой другой форме, кроме данных о потоках или содержании информации, с помощью которой можно установить:

a) вид используемой коммуникационной услуги, принятые с этой целью меры технического обеспечения и период оказания услуги;

b) личность пользователя, его почтовый или географический адрес, номера телефона и других средств доступа, сведения о выставленных ему счетах и произведенных им платежах, имеющиеся в соглашении или договоре на обслуживание;

c) любые другие сведения о месте установки коммуникационного оборудования, имеющиеся в соглашении или договоре на обслуживание.

Подраздел 4 - Обыск и выемка хранимых компьютерных данных

Статья 19 - Обыск и выемка хранимых компьютерных данных

1. Каждая Сторона принимает такие законодательные и иные меры, какие могут потребоваться для предоставления ее компетентным огранам; полномочий на обыск или иной аналогичный доступ к:

a) компьютерным системам или их частям, а также хранящимся в них компьютерным данным; и

b) носителям компьютерных данных, на которых могут храниться

искомые компьютерные данные, на ее территории.

2. Каждая Сторона принимает такие законодательные и иные меры, какие могут быть необходимы для обеспечения того, чтобы в случае, когда ее компетентные органы производят обыск или получают аналогичный доступ к определенной компьютерной системе или ее части в соответствии с положениями пункта 1 a) и имеют основания полагать, что искомые данные хранятся в другой компьютерной системе или ее части на территории этой Стороны, и когда такие данные на законном основании могут быть получены из первой системы или с ее помощью, такие органы имели возможность оперативно распространить производимый обыск или иной аналогичный доступ на другую систему.

3. Каждая Сторона принимает такие законодательные и иные меры, к°кие могут быть необходимы для предоставления ее компетентным органам полномочий производить выемку компьютерных данных, доступ к которым был получен в соответствии с положениями пунктов 1 или *2,* или иным аналогичным образом обеспечивать их сохранность. Эти меры должны включать предоставление полномочий:

a) производить выемку компьютерной системы, ее части или носителей, используемых для хранения компьютерных данных, либо иным аналогичным образом обеспечивать их сохранность;

b) изготавливать и оставлять у себя копии соответствующих компьютерных данных;

c) обеспечивать целостность относящихся к делу хранимых компьютерных данных; и

d) делать компьютерные данные, находящиеся в компьютерной системе, доступ в которую был получен, недоступными или изымать их из нее.

4. Каждая Сторона принимает такие законодательные и иные меры, какие могут быть необходимы для предоставления ее компетентным органам полномочий требовать от любого лица, обладающего знаниями о функционировании соответствующей компьютерной системы или применяемых мерах защиты хранящихся там компьютерных данных, предоставления, в разумных пределах, необходимые сведения, которые позволяют осуществить действия, предусмотренных пунктами 1 и 2.

5. Полномочия и процедуры, упомянутые в настоящей статье, устанавливаются в соответствии с положениями статей 14 и 15.

Подраздел 5 - Сбор компьютерных данных в режиме реального времени

Статья 20 - Сбор в режиме реального времени данных о потоках информации

1. Каждая Сторона принимает такие законодательные и иные меры, которые могут быть необходимы для предоставления ее компетентным органам полномочий:

a) собирать или записывать с применением технических средств на территории этой Стороны, и

b) заставлять поставщиков услуг в пределах имеющихся у них технических возможностей:

i) собирать или записывать с применением технических средств на территории этой Стороны; или

ii) сотрудничать с компетентными органами и помогать им собирать или записывать, в реальном масштабе времени данные о потоках информации, связанные с конкретными сообщениями на территории этой Стороны, передаваемыми по компьютерной системе.

2. Если какая-либо Сторона в силу устоявшихся принципов ее системы внутригосударственного права не может принять меры, предусмотренные в пункте 1 a), то вместо этого она может принять законодательные и иные меры, какие могут быть необходимы для обеспечения сбора или записи в режиме реального времени данных о потоках информации, связанных с указанными сообщениями, на ее территории путем применения технических средств на этой территории.

3. Каждая Сторона принимает такие законодательные и иные меры, какие могут быть необходимы для того, чтобы обязать поставщика услуг соблюдать конфиденциальность самого факта осуществления любых полномочий, предусмотренных в настоящей статье, и любой информации об этом.

4. Полномочия и процедуры, упомянутые в настоящей статье, устанавливаются в соответствии с положениями статей 14 и 15.

Статья 21 Перехват данных о содержании

1. Каждая Сторона принимает такие законодательные и иные меры в отношении ряда серьезных правонарушений, подлежащих квалификации б соответствии с нормами внутригосударственного права, какие могут быть необходимы для того, чтобы наделить ее компетентные органы полномочиями:

a) собирать или записывать с применение технических средств на территории этой Стороны, и

b) заставлять поставщика услуг в пределах имеющихся у него технических возможностей

i) собирать или записывать с использованием технических средств на территории этой Стороны, или

п) сотрудничать с компетентными органами и помогать им в сборе или записи в режиме реального времени данных о содержании указанных сообщений на ее территории, передаваемых с помощью компьютерных систем.

2. Если какая-либо Сторона в силу устоявшихся принципов ее системы внутригосударственного права не может принять меры, предусмотренные в пункте 1 a), то вместо этого она может принять законодательные и иные меры, какие могут быть необходимы для обеспечения сбора или записи в режиме реального времени данных о содержании указанных сообщений на ее территории путем применения технических средств на этой территории.

3. Каждая Сторона принимает такие законодательные и иные меры, какие могут быть необходимы для того, чтобы обязать поставщика услуг соблюдать конфиденциальность самого факта осуществления любых полномочий, предусмотренных в настоящей статье, и любой информации об этом.

4. Полномочия и процедуры, упомянутые в настоящей статье, устанавливаются в соответствии с положениями статей 14 и 15.

Часть 3 - Юрисдикция

Статья 22 - Юрисдикция

1. Каждая Сторона принимает такие законодательные и иные меры, какие могут быть необходимы для установления юрисдикции в отношении любого правонарушения, предусмотренного в соответствии с положениями статей 2 -11 настоящей Конвенции, когда такое правонарушение совершено:

a) на ее территории; или

b) на борту судна, плавающего под флагом этой Стороны; или

c) на борту самолета, зарегистрированного согласно законам этой Стороны; или

d) одним из ее граждан, если это правонарушение является уголовно наказуемым в месте его совершения или если это правонарушение совершено за пределами территориальной юрисдикции какого-либо государства.

2. Каждое государство может зарезервировать за собой право не применять или применять только в определенных случаях или условиях нормы, касающиеся юрисдикции, установленные в пунктах 1 b)-l d) настоящей статьи или любой их части.

3. Каждая Сторона принимает такие меры, какие могут быть необходимы для установления юрисдикции в отношении правонарушений, упомянутых в пункте 1 статьи 24 настоящей Конвенции, в случаях, когда предполагаемый правонарушитель находится на ее территории, и она не выдает его/ее другой Стороне по получении запроса о выдаче, основываясь исключительно на его/ее гражданстве.

4. Настоящая Конвенция не исключает никакую уголовную юрисдикцию, осуществляемую в соответствии с нормами внутригосударственного права.

5. Если на юрисдикцию в отношении предполагаемого правонарушения. предусмотренного в соответствии с настоящей Конвенцией, претендует более одной Стороны, заинтересованные Стороны, по мере необходимости. проводят консультации с целью определить наиболее подходящую юрисдикцию для осуществления судебного преследования.

Глава III - Международное сотрудничество

Часть 1 - Общие принципы

Раздел 1 - Общие принципы международного сотрудничества

Статья *23* - Общие принципы международного сотрудничества

Стороны осуществляют максимально широкое сотрудничество друг с другом в соответствии с положениями настоящей главы и путем применения соответствующих международных документов о международном сотрудничестве по уголовным делам, согласованных договоренностей, опирающихся на единообразное или основанное на взаимности законодательство, а также норм внутригосударственного права в целях проведения расследований или судебного преследования в отношении уголовных преступлений, связанных с компьютерными системами и данными, или сбора доказательств по уголовному преступлению в электронной форме.

Подраздел 2 - Принципы в отношении выдачи

Статья *24* - Выдача

1. a) Настоящая статья применяется между Сторонами в отношении выдачи в связи с уголовными преступлениями, определенными в соответствии со статьями 2-11 настоящей Конвенции, при условии, что согласно законам обеих заинтересованных сторон за них предусматривается наказание в виде лишения свободы на максимальный срок не менее одного года или более суровое наказание.

b) В случаях, когда между двумя или более Сторонами действует соглашение, заключенное на основе единообразного или основанного на взаимности законодательства или договора о выдаче, включая Европейскую конвенцию о выдаче (СЕД №24), согласно которым должно применяться иное минимальное наказание, применяется положение о минимальном наказании, предусмотренное в таком соглашении или договоре.

2. Уголовные преступления, предусмотренные в пункте 1 настоящей статьи, рассматриваются как входящие в число преступлений, предполагающих выдачу, в любом двустороннем или многостороннем договоре о выдаче, существующем между Сторонами. Стороны обязуются включать такие преступления в число преступлений, предполагающих выдачу, в любые двусторонние и многосторонние договоры о выдаче, которые будет заключены между ними.

3. Если какая-либо Сторона, выдвигающая в качестве условия выдачи существование договора, получает запрос о выдаче от другой Стороны, с которой у нее нет договора о выдаче, она может рассматривать настоящую Конвенцию как юридическое основание для выдачи в связи с любым уголовным преступлением, упомянутым в пункте 1 настоящей статьи.

4. Стороны, не выдвигающие в качестве условия выдачи существование договора, в отношениях между собой признают уголовные преступления, упомянутые в пункте 1 настоящей статьи, в качестве преступлений, предполагающих выдачу.

5. Выдача осуществляется в соответствии с условиями, предусмотренными законодательством запрашиваемой Стороны или применимыми договорами о выдаче, включая основания, на которых запрашиваемая Сторона может отказывать в выдаче.

6. Если отказ в выдаче в связи с одним из уголовных преступлений, упомянутых в пункте 1 настоящей статьи, мотивируется исключительно гражданством искомого лица или тем. что, по мнению запрашиваемой Стороны, данное преступление относится к ее юрисдикции, запрашиваемая Сторона, по просьбе запрашивающей Стороны передает это дело своим компетентным органам с целью осуществления судебного преследования и своевременно сообщает запрашивающей Стороне об окончательном результате. Эти органы принимают свое решение и проводят свое расследование и судебное разбирательство также, как и в случае любого другого правонарушения сопоставимого характера согласно законам этой Стороны.

7. a) Каждая Сторона при подписании или сдаче на хранение своего документа о ратификации, принятии, одобрении или присоединении, сообщает Генеральному секретарю Совета Европы наименование и адрес каждого органа, ответственного за направление или получение запроса о выдаче или предварительном аресте при отсутствии договора.

b) Генеральный секретарь Совета Европы составляет и постоянно обновляет реестр органов, назначенных Сторонами с этой целью. Каждая Сторона обеспечивает то, чтобы в

этом реестре всегда содержались постоянные данные.

Раздел 3 - Общие принципы взаимной помощи

Статья *25* - Общие принципы взаимной помощи

1. Стороны на взаимной основе оказывают друг другу по возможности максимально правовую помощь в целях проведения расследований или судебного разбирательства в связи с уголовными преступлениями, связанными с компьютерными системами и данными, или сбора доказательств по уголовному преступлению в электронной форме.

2. Каждая Сторона также принимает такие законодательные и иные меры, какие могут быть необходимы для выполнения обязательств, изложенных в статьях 27-35.

3. Каждая Сторона может в экстренных ситуациях направлять запросы о взаимной помощи или сообщения, связанные с такими запросами, используя оперативные средства связи, включая факсимильную связь или электронную почту, в той мере, в какой такие средства обеспечивают соответствующие уровни безопасности и подтверждения подлинности (включая, если необходимо, использование шифрования), с последующим официальным подтверждением, если того требует запрашиваемая Сторона. Запрашиваемая Сторона принимает такой запрос и отвечает на него с помощью любых аналогичных оперативных средств связи.

4. За исключением случаев, когда положениями статей настоящей главы конкретно предусматривается иное, взаимная помощь оказывается на условиях, предусмотренных законодательством запрашиваемой Стороны или положениями применимых договоров о взаимной помощи, включая основания, на которых запрашиваемая Сторона может отказаться от сотрудничества. Запрашиваемая Сторона не осуществляет права на отказ во взаимной помощи в отношении правонарушений, предусмотренных статьями 2-11, исключительно на том основании, что запрос касается правонарушения, которое она рассматривает как финансовое правонарушение.

5. Когда в соответствии с положениями настоящей главы запрашиваемой Стороне разрешается выдвигать в качестве условия оказания взаимной помощи требование о том, чтобы соответствующее деяние рассматривалось как преступное обеими Сторонами, это условие считается выполненным, независимо от того, относят ли данное правонарушение ее законы к преступлениям той же категории или использует ли она для обозначения этого преступления ту же терминологию, что и запрашивающая Сторона, если деяние, лежащее в основе преступления, в связи с которым запрашивается помощь, является уголовным преступлением согласно ее законам.

Статья *26* - Внеплановая информация

1. Сторона может в пределах норм своего внутригосударственного права, направить без предварительного запроса, другой Стороне информацию, полученную в рамках своего собственного расследования, когда, по ее мнению, раскрытие такой информации могло бы помочь Стороне -получателю этой информации начать или провести расследование или судебное разбирательство в отношении уголовных преступлений, установленных в соответствии с положениями настоящей Конвенции, или могло бы повлечь за собой направление этой Стороной просьбы о сотрудничестве в соответствии с положениями настоящей главы.

2. Прежде чем предоставить такую информацию, предоставляющая Сторона может просить о соблюдении ее конфиденциальности или поставить определенные условия для ее использования. Если получающая Сторона не может выполнить такую просьбу, она уведомляет об этом предоставляющую Сторону, которая определяет затем, следует ли тем не менее предоставить такую информацию. Если получающая Сторона принимает информацию на указанных условиях, они носят для нее обязательный характер.

Подраздел 4 - Процедуры направления запросов о взаимной помощи отсутствие применимых международных соглашений

Статья *27* - Процедуры направления запросов о взаимной помощи в отсутствие применимых международных соглашений

1. В случаях, когда между запрашивающей и запрашиваемой Сторонами нет действующего договора или соглашения о взаимной помощи, основанного на единообразном или принятом на началах взаимности законодательства, применяются положения пунктов 2-9 настоящей статьи. При наличии такого договора, соглашения или законодательства положения данной статьи не применяются, если только заинтересованные Стороны не соглашается применять взамен любые или все последующие положения настоящей Статьи.

2. a) Каждая Сторона назначает центральный орган или органы, которые несут ответственность за направление запросов о взаимной помощи и ответов на них, выполнение таких запросов или их передачу органам, в компетенцию которых входит их выполнение.

b) Эти центральные органы поддерживают связь непосредственно друг с другом.

c) Каждая Сторона при подписании настоящей Конвенции или при сдаче на хранение своей ратификационной грамоты или своего документа о принятии, одобрении или присоединении сообщает Генеральному секретарю Совета Европы наименования и адреса органов, назначенных в соответствии с настоящим пунктом.

d) Генеральный секретарь Совета Европы составляет и постоянно обновляет реестр центральных органов, назначенных Сторонами. Каждая Сторона обеспечивает, чтобы в этом реестре всегда содержались достоверные сведения.

3. Запросы о взаимной помощи, направляемые согласно положениям настоящей статьи, исполняются в соответствии с процедурами, указанными запрашивающей Стороной, за исключением случаев, когда они несовместимы с законодательством запрашиваемой Стороны.

4. Запрашиваемая Сторона может в дополнение к основаниям для отказа, предусмотренным в пункта 4 статьи 25, отказать в предоставлении помощи, если:

a) запрос касается правонарушения, рассматриваемого запрашиваемой Стороной как политическое преступление или как правонарушение, связанное с политическим преступлением;

b) по ее мнению, невыполнение запроса, по всей вероятности, приведет к подрыву ее суверенитета, безопасности, общественного порядка или иных существенных интересов.

5. Запрашиваемая Сторона может отложить принятие мер по запросу, если такие меры препятствовали бы уголовным расследованиям или судебным разбирательствам, проводимым ее органами.

6. Прежде чем отказать в предоставлении помощи или отсрочить ее оказание, запрашиваемая Сторона, по мере необходимости, после консультаций с запрашивающей Стороной рассматривает возможность удовлетворения запроса частично или на таких условиях, какие она сочтет необходимыми.

7. Запрашиваемая Сторона незамедлительно информирует запрашивающую Сторону о результатах выполнения запроса о помощи. В случае отказа в выполнении запроса или отсрочки такого выполнения сообщаются причины такого отказа или отсрочки. Запрашиваемая Сторона также сообщает запрашивающей Стороне о любых причинах, по которым выполнение запроса становится невозможным или, по всей вероятности, будет осуществлено со значительной задержкой.

8. Запрашивающая Сторона может просить запрашиваемую Сторону обеспечить конфиденциальность факта и предмета любого запроса, сделанного в соответствии с положениями настоящей главы, но лишь в той степени, которая согласуется с его выполнением. Если запрашиваемая Сторона не может выполнить просьбу о сохранении конфиденциальности, она незамедлительно сообщает об этом запрашивающей Стороне, которая затем принимает решение о том, следует ли тем не менее направить запрос.

9. a) В случае крайней необходимости запросы о взаимной помощи или сообщения, связанные с такими запросами, могут направляться непосредственно судебными органами запрашивающей Стороны соответствующим органам запрашиваемой Стороны. В любых

таких случаях одновременно направляется копия центральным органам запрашиваемой Стороны через центральные органы запрашивающей Стороны.

b) Любой запрос или сообщение, упомянутые в настоящей части, могут быть направлены через Международную организацию уголовной полиции (Интерпол).

c) Когда запрос делается в соответствии с положениями подпункта a), а его рассмотрение не входит в компетенцию получившего его органа, последний направляет этот запрос в компетентный национальный орган и сообщает об этом непосредственно запрашивающей Стороне.

d) Направляемые в соответствии с положениями настоящей части запросы или сообщения, которые не предполагают принятия принудительных мер, могут передаваться компетентными органами запрашивающей Стороны непосредственно компетентным органам запрашиваемой Стороны.

e) Каждая Сторона может при подписании Конвенции или при сдаче на хранение ратификационной грамоты или документа о принятии, одобрении или присоединении сообщить Генеральному секретарю Совета Европы, что в целях обеспечения эффективности запросы. направляемые в соответствии с положениями настоящей части, должны быть адресованы ее центральным органам.

Статья 28 - Конфиденциальность и ограничения на использование информации

1. В случае отсутствия между запрашивающей и запрашиваемой Сторонами действующего договора или соглашения о взаимной правовой помощи, определяющегося на единообразное или основанное на принципе взаимности законодательство, применяются положения настоящей статьи. Положения настоящей статьи при наличии такого договора, соглашения или законодательства не применяются, если только заинтересованные Стороны не соглашаются применять вместо последних любые или все последующие положения настоящей статьи.

2. В ответ на просьбу запрашиваемая Сторона может выдвинуть следующие условия предоставления информации или материала:

a) сохранение их конфиденциальности, если без такого условия просьба о взаимной правовой помощи не могла бы быть выполнена;

b) неиспользование для других расследований или судебных разбирательств, которые не указываются в просьбе.

3. Если запрашивающая Сторона не может выполнить одно из условий, упомянутых в пункте *2,* она незамедлительно информирует об этом другую Сторону, которая затем решает, может ли быть предоставлена такая информация. Если запрашивающая Сторона соглашается выполнить эти условия, они приобретают для нее обязательную силу.

4. Любая Сторона, предоставляющая информацию или материал на упомянутых в пункте 2 условиях, может, в связи с одним из условий, потребовать от другой Стороны разъяснений относительно имевшего место использования такой информации или материала.

Раздел *2* - Конкретные положения

Подраздел 1 - Помощь в связи с предварительными мерами

Статья *29* - Неотложное обеспечение сохранности хранящихся компьютерных данных

1. Любая Сторона может попросить другую Сторону дать указание, или сделать это иным образом, неотложно обеспечить сохранность данных, хранящихся в компьютерной системе, расположенной на территории этой другой Стороны, и в отношении которых запрашивающая Сторона намеревается в рамках взаимной помощи направить просьбу об обыске или аналогичных обеспечивающих доступ действиях, выемке или аналогичном обеспечении сохранности или разглашении этих данных.

2. В просьбе об обеспечении сохранности данных, направляемой в соответствии с пунктом

1, указываются:

a) орган, добивающийся обеспечения сохранности;

b) правонарушение, которое подлежит расследованию или судебному разбирательству, и краткое изложение основных фактов;

c) хранимые компьютерные данные, подлежащие сохранению, и их связь с указанным правонарушением;

d) любая имеющаяся информация, идентифицирующая владельца компьютерных данных или местоположение компьютерной системы;

e) обоснование сохранности; и

f) сообщение, что эта Сторона намеревается в рамках взаимной помощи направить просьбу об обыске или аналогичных обеспечивающих доступ действиях, выемке или аналогичном обеспечении сохранности или разглашении этих данных.

3. По получении такой просьбы от другой Стороны запрашиваемая Сторона принимает все надлежащие меры для неотложного обеспечения сохранности указанных данных в соответствии с внутригосударственным правом. Для удовлетворения такой просьбы в качестве условия не выдвигается требование о том, чтобы правонарушение квалифицировалось как уголовно наказуемое обеими Сторонами.

4. Сторона, которая выдвигает в качестве условия удовлетворения в рамках взаимной помощи просьбы об обыске или аналогичных обеспечивающих доступ действиях, выемке или аналогичном обеспечении сохранности или раскрытии этих данных по правонарушениям, не перечисленным в статьях 2-11 настоящей Конвенции, может оставить за собой право отказывать в просьбе об обеспечении сохранности в соответствии с настоящей Конвенцией в случаях, когда у нее есть основания полагать, что в момент раскрытия условие о квалификации правонарушения как уголовно наказуемого обеими Сторонами не будет выполнено.

5. Кроме того в просьбе об обеспечении сохранности данных может быть отказано если:

a) соответствующая просьба касается правонарушения, которое запрашиваемая Сторона квалифицирует как политическое преступление или правонарушение, связанное с политическим преступлением; или

b) запрашиваемая Сторона полагает, что выполнение такой просьбы может нанести ущерб ее суверенитету, безопасности, общественному порядку или другим важным интересам.

6. Если запрашиваемая Сторона полагает, что такое обеспечение сохранности данных не обеспечит в будущем сохранность этих данных или поставит под угрозу их конфиденциальность или иным образом помешает расследованию запрашивающей Стороны, она незамедлительно информирует об этом запрашивающую Сторону, которая после этого решает, должна ли выполняться эта просьба.

7. Любое обеспечение сохранности данных, предпринятое в ответ на упомянутую в пункте 1 просьбу, производится на срок не менее 60 дней, чтобы запрашивающая Сторона могла направить просьбу об обыске или аналогичных обеспечивающих доступ действиях, выемке или аналогичном обеспечении сохранности или разглашении данных. После получения такой просьбы такие данные продолжают сохраняться до принятия решения в отношении этой просьбы.

Статья 30 — Неотложное раскрытие сохраненных данных о потоках информации

1. Если в ходе предпринятого в соответствии со статьей 29 исполнения просьбы об обеспечении сохранности данных о потоках в связи с конкретным сообщением запрашиваемая Сторона установит, что поставщик услуг в другом государстве участвовал в передаче этого сообщения, запрашиваемая Сторона оперативно раскрывает запрашивающей Стороне достаточный объем данных о потоках, чтобы идентифицировать этого поставщика услуг и путь, по которому было передано это сообщение.

2. Просьба о раскрытии данных потоков в соответствии с пунктом 1 может быть отозвана только в случаях, если:

a) просьба касается правонарушения, которое запрашиваемая Сторона квалифицирует в качестве политического преступления; или

b) запрашиваемая Сторона полагает, что исполнение этой просьбы может нанести ущерб ее суверенитету, безопасности, общественному порядку или другим важным интересам.

Подраздел 2 - Взаимная помощь в связи со следственными полномочиями

Статья 31 - Взаимная помощь в связи с оценкой хранящихся электронных данных

1. Сторона может попросить другую Сторону произвести обыск или аналогичные обеспечивающие доступ действия, выемку или аналогичное обеспечение сохранности и раскрытие хранящихся с помощью компьютерной системы данных, находящейся на территории запрашиваемой Стороны, в том числе данных, сохраненных в соответствии со Статьей 29.

2. Запрашиваемая Сторона отвечает на эту просьбу в соответствии с международными документами, договоренностями и законами, упомянутыми в статье 23 и согласно другим соответствующим положениям настоящей главы.

3. Ответ на просьбу дается оперативно, если:

a) есть основания полагать, что соответствующие данные особо уязвимы для потери или изменения; или

b) документы, договоренности и законы, упомянутые в пункте 2, предусматривают иное оперативное сотрудничество.

Статья 32 - Трансграничный доступ к хранящимся компьютерным данным с соответствующего согласия или к общедоступным данным

Сторона может без согласия другой Стороны:

a) получать доступ к общедоступным (открытому источнику) компьютерным данным независимо от их географического местоположения; или

b) получать через компьютерную систему на своей территории доступ к хранящимся на территории другой Стороны компьютерным данным или получить их, если эта Сторона имеет законное и добровольное согласие лица, которое имеет законные полномочия раскрывать эти данные этой Стороне через такую компьютерную систему.

Статья 33 - Взаимная правовая помощь по сбору данных о потоках в режиме реального времени

1. Стороны оказывают взаимную правовую помощь друг другу в сборе данных о потоках информации в режиме реального времени, имеющих отношение к конкретным сообщениям на их территории с помощью компьютерной системы. При соблюдении пункта 2 оказание такой помощи регламентируется условиями и процедурами, предусмотренными во внутригосударственном праве.

2. Каждая Сторона оказывает такую помощь по меньшей мере по уголовным преступлениям, для которых во внутригосударственном праве мог бы предусматриваться сбор атрибутов данных в режиме реального времени.

Статья 34 - Взаимная помощь по перехвату данных о содержании

Стороны оказывают друг другу взаимную помощь по сбору или записи в режиме реального времени содержания данных конкретных сообщений, передаваемых с помощью компьютерной системы, если это допускается их действующими договорами и внутригосударственным правом.

***Подраздел 3 - Сеть 24/7* Статья 35 - Сеть 24/7**

1. Каждая Сторона назначает контактный центр, работающий 24 часа в сутки в течении 7 дней, чтобы обеспечить оказание неотложной помощи в целях расследований или судебных разбирательств уголовных преступлений, имеющих отношение к компьютерным системам и данным или в целях сбора доказательств в электронной форме по уголовным преступлениям. Такая помощь включает содействие или, если это допускается внутригосударственным правом или практикой, непосредственное применение следующих мер:

a) оказание технической консультативной помощи;

b) обеспечение сохранности данных в соответствии со статьями 29 и 30; и

c) сбор доказательств, предоставление законной информации и установление нахождения подозреваемых лиц.

2. a) Контактный центр одной Стороны располагает возможностями для оперативного обмена сообщениями с контактным центром другой Стороны.

b) Если контактный центр, назначенный одной из Сторон не входит в состав органа или органов этой Стороны, которым поручено оказание помощи или экстрадиция, этот контактный центр принимает меры для того, чтобы он мог оперативно координировать свою деятельность с деятельностью такого органа или органов.

3. Каждая Сторона принимает меры для предоставления квалифицированного персонала и оборудования с целью облегчить функционирование такой сети.

Глава IV — Заключительные положения

Статья 36 - Подписание и вступление в силу

1. Настоящая Конвенция открыта для подписания государствами-членами Совета Европы и не являющимися его членами государствами, которые участвовали в ее разработке.

2. Настоящая Конвенция подлежит ратификации, принятию или одобрению. Ратификационные грамоты или документы о принятии или одобрении сдаются на хранение Генеральному секретарю Совета Европы.

3. Настоящая Конвенция вступает в силу в первый день месяца, следующего за истечением трех месяцев после даты, когда пять государств, включая по меньшей мере три государства-члена Совета Европы, выразят свое согласие на обязательное для них соблюдение Конвенции в соответствии с положениями пунктов 1 и 2.

4. В отношении любого подписавшего Конвенцию государства, которое в последующий период выразит согласие на обязательное для него соблюдение Конвенции, она вступает в силу в первый день месяца, наступающего по истечении трехмесячного срока, считая с даты, когда оно выразило свое согласие на обязательное для него соблюдение Конвенции в соответствии с пунктами 1 и 2.

Статья 37 - Присоединение к Конвенции

1. После вступления настоящей Конвенции в силу Комитет министров Совета Европы, после консультаций и единодушного согласия государств-участников Конвенции, может предложить любому государству, не являющемуся членом Совета и не участвовавшему в ее разработке, присоединиться к настоящей Конвенции. Такое решение принимается большинством, предусмотренным в пункте d) Устава Совета Европы, при условии единодушного согласия представителей Договаривающихся сторон, имеющих право на членство в Совете министров.

2. В отношении любого государства, присоединяющегося к Конвенции в соответствии с пунктом 1, выше, Конвенция вступает в силу в первый день месяца, наступающего по истечении трехмесячного срока, считая с даты сдачи на хранение документа о присоединении Генеральному секретарю Совета Европы.

Статья 38 - Территориальное применение

1. Любое государство при подписании или в момент сдачи на хранение ратификационной грамоты или документа о принятии, одобрении или присоединении может указать территорию или территории, на которые распространяется действие настоящей Конвенции.

2. Любая Сторона в любой последующий момент может путем заявления, направленного на имя Генерального секретаря Совета Европы, распространить действие настоящей Конвенции на любую другую территорию, указанную в заявлении. В отношении такой территории Конвенция вступает в силу в первый день месяца, наступающего по истечении трехмесячного срока, считая с даты получения заявления Генеральным секретарем.

3. Любое заявление, сделанное в соответствии с положениями двух предыдущих пунктов в отношении любой указанной в таком заявлении территории, может быть отозвано, путем уведомления, направленного на имя Генерального секретаря Совета Европы. Отзыв вступает в силу в первый тень месяца, наступающего по истечении трехмесячного срока, считая с даты получения подобного уведомления Генеральным секретарем.

Статья 39 - Последствия Конвенции

1. Цель настоящей Конвенции - дополнить соответствующие многосторонние или двусторонние соглашения или договоренности между Сторонами, включая положения:

Европейской конвенции о выдаче, открытой для подписания в Париже 13 декабря 1957 г. (СЕД № 24);

Европейской конвенции о взаимной правовой помощи по уголовным делам, открытой для подписания в Страсбурге 20 апреля 1959 г. (СЕД № 30);

Дополнительного протокола к Европейской конвенции о взаимной правовой помощи по уголовным делам, открытого для подписания в Страсбурге 17 марта 1978 г. (СЕД № 99).

2. Если две или более Сторон уже заключили соглашение или договор по вопросам, составляющим предмет настоящей Конвенции, или иным путем определили свои отношения по вопросам, или если они сделают это в будущем, они также имеют право применять указанные соглашение или договор или регулировать свои отношения в соответствии с ними. Однако, если Стороны устанавливают отношения по иным вопросам, составляющим предмет настоящей Конвенции, чем те, которые регламентирует данный документ, они делают это не нарушая целей и принципов Конвенции.

3. Ничто в настоящей Конвенции не затрагивает иные права, ограничения, обязательства и обязанности Стороны.

Статья 40 - Заявления

Путем письменного уведомления на имя Генерального секретаря Совета Европы, любое государство при подписании или в момент сдачи на хранение ратификационной грамоты или документа о принятии, одобрении или присоединении может заявить о том, что оно пользуется возможностью, чтобы потребовать включения дополнительных элементов, предусмотренных в статьях 2, 3, 6, пункте 1(b), 7, 9, пункте 3 и 27, пункте 9 (e).

Статья 41 - Положение, касающееся федеративного государства.

1. Федеративное государство может сделать оговорку о сохранении за собой права принять на себя содержащиеся в Главе II настоящей Конвенции обязательства, которые соответствуют основным принципам, регулирующим отношения между центральным правительством и субъектами Федерации или иными аналогичными территориальными образованиями при условии, что оно, тем не менее, способно осуществлять сотрудничество по Главе III.

2. Делая такую оговорку в соответствии с пунктом 1, федеративное государство не может использовать положения данной оговорки, чтобы исключить или существенно сократить обязательства по обеспечению выполнения мер, предусмотренных Главой П. Оно должно предусмотреть широкие и эффективные правоохранительные возможности для обеспечения выполнения данных мер.

3. В том, что касается положений настоящей Конвенции, выполнение которых подпадает под юрисдикцию субъектов федерации или иных аналогичных территориальных образований, которые в соответствии с конституционной системой федерации не обязаны принимать законодательные меры, федеральное правительство информирует компетентные власти таких субъектов об упомянутых положениях и своем положительном мнении, побуждая их предпринимать необходимые действия для выполнения данных положений.

Статья 42 - Оговорки

Путем письменного уведомления на имя Генерального секретаря Совета Европы любое государство при подписании или в момент сдачи на хранение ратификационной грамоты или документа о принятии, одобрении или присоединении может заявить, что оно воспользуется правом сделать оговорку(и), предусмотренную(ые) в пункте 2 статьи 4, пункте 3 статьи 6, пункте 4 статьи 9, пункте 3 статьи 10, пункте 3 статьи 11, пункте 3 статьи 14, пункте 2 статьи 22, пункте 4 статьи 29 и пункте 1 статьи 41. Никакие другие оговорки не допускаются.

Статья 43 - Статус и снятие оговорок

1. Сторона, сделавшая оговорку в соответствии с положениями статьи 42, может снять всю оговорку или ее часть путем уведомления на имя Генерального секретаря Совета Европы. Такое снятие оговорки вступая е силу в день получения соответствующего уведомления Генеральным секретарем. Если в уведомлении говорится, что снятие оговорки должно вступить в силу с момента указанной в нем даты, а такая дата наступает позже даты получения уведомления Генеральным секретарем, то снятие оговорки вступает в силу с момента указанной поздней даты.

2. Сторона, сделавшая, упомянутую в статье 42 оговорку, снимает такую оговорку или ее часть, как только позволят обстоятельства.

3. Генеральный секретарь Совета Европы может периодически запрашивать Стороны, сделавшие одну или несколько оговорок, упомянутых в статье 42, о возможностях снятия такой оговорки (оговорок).

Статья 44 - Поправки

1. Поправки к настоящей Конвенции могут предлагаться любой Стороной, и сообщаться через Генерального секретаря Совета Европы государствам-членам Совета Европы, не являющимся его членами государствам, которые участвовали в разработке этой Конвенции, а также любому государству, присоединившемуся к настоящей Конвенции или получившему предложение присоединиться к ней в соответствии с положениями статьи 37.

2. Любая поправка, предложенная одной из Сторон, направляется в Европейский комитет по проблемам преступности (ЕКПП), который представляет Комитету министров свое заключение относительно предлагаемой поправки.

3. Комитет министров рассматривает предлагаемую поправку и заключение, представленное ЕКПП, и после консультации сторонами настоящей Конвенции, не являющимися государствами-членами, может принять эту поправку.

4. Текст любой поправки, принятой Комитетом министров в соответствии с положениями пункта 3 настоящей статьи, направляется Сторонам Конвенции для утверждения.

5. Любая поправка, принятая в соответствии с положениями пункта 3 настоящей Статьи, вступает в силу на тридцатый день после того, как все Стороны сообщат Генеральному секретарю о своем согласии с этой поправкой.

Статья 45 - Урегулирование споров

1. Европейский комитет по проблемам преступности (ЕКПП) получает информацию о толковании и применении настоящей Конвенции.

2. В случае возникновения спора между Сторонами относительно толкования или применения настоящей Конвенции они стремятся к урегулированию спора путем

переговоров или любыми другими мирными средствами по своему выбору, включая передачу этого спора, с согласия заинтересованных Сторон, в ЕКПП, в арбитражный суд, решения которого имеют для Сторон обязательную силу, или в Международный суд.

Статья 46 - Консультации Сторон

1. Стороны, в соответствующих случаях, периодически проводят консультации с целью содействовать:

(a) эффективному применению и выполнению настоящей Конвенции, включая выявление любых относящихся к ней проблем, а также последствий любого заявления или оговорки, сделанных в соответствии с настоящей Конвенцией;

(b) обмену информацией о важных изменениях в правовой, политической или технической сферах, имеющих отношение к киберпреступности, и сбору доказательств в электронной форме;

(c) рассмотрению возможных дополнений или поправок к настоящей Конвенции.

2. Европейский комитет по проблемам преступности (ЕКПП) периодически получает информацию о результатах консультаций, упомянутых в пункте 1.

3. ЕКПП в соответствующих случаях оказывает содействие в проведший консультаций, упоминаемых в пункте 1, и принимает необходимые меры для оказания помощи Сторонам в их усилиях по внесению дополнений или поправок в Конвенцию. Самое позднее через три года после вступления в силу настоящей Конвенции Европейский комитет по проблемам преступности (ЕКПП) во взаимодействии со Сторонами проводит пересмотр всех положений Конвенции и, в случае необходимости, рекомендует принять любые соответствующие поправки.

4. За исключением случаев, когда расходы, понесенные в процессе выполнения положений пункта 1, берет на себя Совет Европы, их несут сами Стороны на установленных ими условиях.

5. Секретариат Совета Европы оказывает помощь Сторонам в выполнении их обязанностей, вытекающих из положений настоящей Статьи.

Статья 47 - Денонсация

1. Любая Сторона может в любое время денонсировать настоящую Конвенцию путем уведомления на имя Генерального секретаря Совета Европы.

2. Такая денонсация вступает в силу в первый день месяца, наступающего по истечении трехмесячного срока, считая с даты получения уведомления Генеральным секретарем.

Статья 48 - Уведомление

Генеральный секретарь Совета Европы уведомляет государства-члены Совета Европы, не являющиеся его членами государства, которые участвовали в разработке настоящей Конвенции, а также любое государство, присоединившееся или получившее предложение присоединиться к настоящей Конвенции о:

(a) любом подписании;

(b) сдаче на хранение любой ратификационной грамоты или любого документа о принятии, одобрении или присоединении;

(c) любой дате вступления в силу настоящей Конвенции в соответствии с положениями статей 36 и 37;

(d) любом заявлении, сделанным в соответствии с положениями статьи 40 или оговорки, сделанной в соответствии с положениями статьи 42;

(e) любых других актах, уведомления или сообщения, относящихся к настоящей Конвенции.

В удостоверение чего нижеподписавшиеся, должным образом на то уполномоченные представители подписали настоящую Конвенцию.

Совершено в Будапеште 23 ноября.2001 г. в одном экземпляре на английском и французском языках, причем оба текста имеют одинаковую силу. Этот экземпляр передается на хранение в архивы Совета Европы. Генеральный секретарь Совета Европы направляет заверенные копии данного документа каждому государству-члену Совета Европы, не являющимся его членами государствам, участвовавшим в разработке настоящей Конвенции, и любому государству, получившему предложение присоединиться к ней.

Комментарий к Конвенции о киберпреступности

Е. Волчинская

Комментарий к Конвенции о киберпреступности

В этом выпуске журнала публикуется полный текст международной Конвенции о киберпреступности. Прокомментировать этот важный документ мы попросили советника аппарата Комитета Госдумы по безопасности Елену Волчинскую.

Конвенция принята осенью 2001 года и служит своего рода ориентиром для совершенствования уголовного и уголовно процессуального законодательства России в сфере борьбы с киберпреступностью. Следует отметить, что в подготовке этого документа принимали участие и российские эксперты.

Россия пока не присоединилась к Конвенции, т.к. это накладывает на государство определенные обязательства. Кроме, приведения нашего законодательства в соответствие с международными нормами и правилами в данной области, необходимо также создать специальное подразделение в структуре правоохранительных органов РФ для взаимодействия и оказания правовой помощи в режиме реального времени (статья 34) соответствующим подразделениям в странах, присоединившихся к Конвенции.

Уголовный Кодекс РФ предусматривает ответственность за преступления, связанные с использованием компьютерных технологий (глава 28 “Преступления в сфере компьютерной информации”). Составы преступлений по статьям 272-274 этой главы частично (по смыслу, но не по форме) совпадают с составами, содержащимися в Конвенции. Например, в Конвенции (статья 4 "Воздействие на данные") - преднамеренное повреждение, удаление, изменение, блокировка данных без права на это. В УК РФ диспозиция статьи 272 включает уничтожение, модифицирование, блокирование или копирование охраняемой законом информации при неправомерном доступе. Конвенция распространяется и на иные правонарушения, в том числе, связанные с детской порнографией, а также с нарушением авторских и смежных прав (статьи 9 и 10), ответственность на которые предусмотрена соответственно в статьях 242 и 146 УК РФ.

Есть и очевидные пробелы в российском законодательстве, которые предстоит заполнить в случае присоединения к Конвенции, хотя развитие и совершенствование уголовного и уголовно-процессуального законодательства обусловлено, в первую очередь, практикой правоприменени и возникновением новых видов преступлений. Например, Конвенция (ст. 6 п. a) ii), в качестве уголовных преступлений квалифицируется производство, продажа, приобретение для использования или иные формы предоставления в пользование компьютерных паролей, кодов доступа или иных аналогичных данных, с помощью которых может быть полуен доступ к компьютерной сети. Здесь проявляется общая идеология

Конвенции, которая, в отличие от отечественного законодательства, направлена на детализацию и конкретизацию преступных деяний.

Компьютерная преступность не имеет границ. Эта ее особенность осложняет как поиск и идентификацию лиц, совершающих международные преступления с использованием компьютерных технологий, так и определение страны, и соответственно – конкретного национального законодательства, в соответствии с которым киберпреступления должны караться. Конвенция довольно подробно излагает вопросы юрисдикции, разъясняя в каких случаях и на какой территории будут в судебном порядке преследоваться и наказываться люди, совершившие компьютерные преступления на территории Европы, на борту самолет или на водном транспорте.

Значение Конвенции выходит за рамки чисто законодательных вопросов. Этот документ закладывает основу для расширения практического сотрудничества российских и европейских правоохранительных структур в предотвращении и раскрытии киберпреступлений.

Приведение российского законодательства в соответствие с положениями данной Конвенции, равно как и основанные на этом документе практические шаги по координации международных усилий должны повысить эффективность противодействия киберпреступности как в России, так и в странах Европы.

Протест против Конвенции

Обращение общественных организаций с протестом против принятия Конвенции о киберпреступности

18 октября 2000 г.

Уважаемые члены комитета экспертов по киберпреступности, Комитета министров и Парламентской ассамблеи!

Мы обращаемся к вам от имени широкого спектра организаций гражданского общества со всего мира для того, чтобы возразить против предлагаемой к принятию Конвенции по киберпреступности. Мы полагаем, что предложенная конвенция противоречит установившимся нормам защиты личности, неоправданно расширяет полицейские функции правительства, подрывает развитие технологий сетевой безопасности и снижает ответственность государства в области правоохранительной деятельности.

В частности, мы возражаем против положений, требующих от провайдеров Интернета вести записи о деятельности их клиентов (статьи 17, 18, 24, 25). Эти положения создают значительную угрозу прайвеси и другим правам пользователей Интернета. Они противоречат существующим принципам защиты информации, таким, как Директива ЕС о защите данных (Data Protection Directive of the European Union). В прошлом подобная информация использовалась для выявления диссидентов и преследования меньшинств. Мы призываем вас не вводить аналогичные меры применительно к модемной сети. По нашему мнению, вся статья 18 несовместима со статьей 8 Европейской конвенции о защите прав человека и с решениями Европейского суда по правам человека.

Мы возражаем против концепции <незаконных устройств>, описанной в статье 6. Мы полагаем, что этой концепции не хватает четкости формулировок, а значит, она может стать основой для проведения следственных действий против любого человека, вовлеченного в совершенно законную деятельность, имеющую отношение к компьютерам. Как уже сказали технические эксперты, это положение помешает развитию новых методов обеспечения безопасности и придаст государству неподобающие ему функции слежки за

перспективными научными разработками.

Мы также возражаем против серьезного расширения понятия преступлений в области авторского права (ст. 10). Едва ли можно считать доказанным, что за нарушение копирайта должно непременно следовать уголовное наказание. Действующие международные соглашения таких мер не предусматривают. Конвенция не должна вводить новые уголовные наказания в ту область, где имеется столь не устоявшееся национальное законодательство. Мы не можем согласиться с подобными планами, когда ряд стран не признает преступность тех или иных действий. Это наше требование является основным для сохранения суверенного права государств.

Мы полагаем, что по вопросу проведения международных расследований должны быть согласованы четкие процедуры, и что ни один правоохранительный орган не должен действовать от имени другой страны без четких следственных процедур в пределах собственной юрисдикции. Естественно, что в разных странах существуют разные правила, но именно сейчас есть возможность согласовать их, обеспечивая при этом высокий уровень защиты прав человека.

Положения статей 9 и 11 могут оказать негативное влияние на свободный обмен информацией и идеями. Введение ответственности Интернет-провайдера за содержание материалов, принадлежащих третьей стороне - бессмысленная обуза, которая лишь поощряет слежку за частными коммуникациями.

Статья 14, устанавливающая требования к поиску и захвату информации, хранящейся в компьютерах, лишена необходимых процедур, защищающих личность и гарантирующих соблюдение закона. Так, в ней не предпринимается попытка обеспечить независимый юридический надзор (основу уважения базовых прав и свобод) до того, как государственный орган начинает работать с информацией. Подобные действия международные правовые нормы расценивают как <грубое вмешательство>.

Статьи 14 и 15 могут быть истолкованы так, что будет выдвинуто требование обеспечить государственным органам доступ к шифровальным ключам. Это принудит граждан свидетельствовать против самих себя, что несовместимо со статьей 6 Европейской конвенции и с решениями Европейского суда по правам человека. Следует обратить внимание на двусмысленность, возникающую в пределах одной и той же статьи о доступе правительственных органов к шифровальным ключам. Совет Европы должен прояснить это положение с тем, чтобы страны-участники не считали конвенцию мандатом на принятие законодательных актов, приводящих к свидетельствованию против самого себя.

Мы также резко возражаем против самой процедуры разработки данного проекта. Правоохранительные органы и представители влиятельных частных лиц, действуя несовместно с демократическими принципами, приложили усилия, чтобы сделать этот процесс закрытым и установить свои правила игры. Мы полагаем, что этот процесс нарушает требования открытости и противоречит демократическим принципам принятия решений.

Эксперты в области прайвеси недвусмысленно выражают свое несогласие с проектом Конвенции. Согласно одному из высказываний экспертов, попытки разработать международную конвенцию по киберпреступлениям приведут к <фундаментальным ограничениям прайвеси, анонимности и шифрования>.

Люди, имеющие отношение к защите данных, так же ясно выражают свое несогласие с проектом. Международная рабочая группа по защите данных в телекоммуникациях (International Working Group on Data Protection in Telecommunications) критиковала попытки принять требование о хранении информации об обмене данными и рекомендовала принять ряд усовершенствований в системе безопасности в связи с новым уголовным законодательством.

Технические эксперты тоже не согласны с проектом. В письме, подписанном известными пользователями, преподавателями и распространителями систем безопасности, говорится, что <предлагаемый проект может неумышленно привести к объявлению вне закона технологий и программного обеспечения, широко используемых для защиты компьютера от

внешних атак>, и что он <наносит вред по пользователям, преподавателям и разработчикам систем безопасности>.

Свое несогласие с проектом Конвенции выражает и широкий спектр организаций, представляющих гражданское общество.

Мы полагаем, что прежде, чем расширять полномочия следователей и прокуроров, необходимо внимательно проанализировать соответствие предложений статьям 8 и 10 Европейской конвенции по правам человека и соответствующим решениям Европейского суда. Мы считаем, что это не было сделано при разработке данного проекта. Мы полагаем, что руководящие принципы в области криптографии Организации по экономическому и сотрудничеству и развитию (OECD Cryptography Policy Guidelines) и руководящие принципы ОЭСР по безопасности информационных систем (OECD Guidelines for the Security of Information Systems) демонстрируют более сбалансированный и широкий взгляд на необходимость распространения мощных технологий безопасности, направленных на снижение риска компьютерных преступлений, нежели обсуждаемый проект.

Наконец, во Всеобщей Декларации прав человека прямо говорится о том, что государство принимает обязательство защищать прайвеси коммуникаций и сохранять свободу самовыражения в новых средствах связи. В ст. 12 говорится: <Никто не может подвергаться произвольному вмешательству в его личную и семейную жизнь, произвольным посягательствам на неприкосновенность его жилища, тайну его корреспонденции>. Далее, в ст. 19 сказано: <Каждый человек имеет право на свободу убеждений и на свободное выражение их; это право включает свободу беспрепятственно придерживаться своих убеждений и свободу искать, получать и распространять информацию и идеи любыми средствами и независимо от государственных границ>.

Мы призываем вас не одобрять в настоящее время предлагаемый проект. Мы, нижеподписавшиеся, готовы предоставить Совету Европы экспертов в данной области, которые помогли бы подготовить улучшенную версию документа, направленную на то, чтобы не только карать, но и предотвращать компьютерные преступления.

С уважением,

American Civil Liberties Union (США)
http://www.aclu.org/

Associazione per la Liberta nella Comunicazione Elettronica Interattiva
(Италия)
http://www.alcei.it/

Bits of Freedom (Нидерланды)
http://www.bof.nl/

Canadian Journalists for Free Expression (Канада)
http://www.cjfe.org/

Center for Democracy and Technology (США)
http://www.cdt.org/

Computer Professional for Social Responsibility (США)
http://www.cpsr.org/

Cyber-Rights & Cyber-Liberties (Великобритания)
http://www.cyber-rights.org

Derechos Human Rights and Equipo Nizkor (США)
http://www.derechos.org/

Digital Freedom Network (США)
http://www.dfn.org/

Electronic Frontier Foundation (США)
http://www.eff.org/

Electronic Frontiers Australia (Австралия)
http://www.efa.org.au

Electronic Privacy Information Center (США)
http://www.epic.org/

Feminists Against Censorship (Великобритания)
http://fiawol.demon.co.uk/FAC/

Internet Freedom (Великобритания)
http://www.netfreedom.org/

Internet Society - Bulgaria (Болгария)
http://www.isoc.bg/

Internet Society
http://www.isoc.org/

IRIS - Imaginons un reseau Internet solidaire (Франция)
http://www.iris.sgdg.org

Kriptopolis (Испания)
http://www.kristopolis.org/

LINK Centre, Wits University, Johannesburg (Южная Африка)

NetAction (США)
http://www.netaction.org/

Opennet
http://www.opennet.org/

Privacy International (Великобритания)
http://www.privacyinternational.org/

quintessenz (Австрия)
http://www.quintessenz.at/

Verein fur Internet Benutzer (Австрия)
http://www.vibe.at/

XS4ALL (Нидерланды)
http://www.xs4all.nl/

Ссылки:

Конвенция Совета Европы по кибер-преступлениям (проект)
http://conventions.coe.int/treaty/EN/projets/cybercrime.doc

Конвенция Совета Европы о защите прав человека и основных свобод
http://www.coe.fr/eng/legaltxt/5e.htm

Общая информация по конвенциям Совета Европы
http://conventions.coe.int/treaty/EN/cadreintro.htm

Заявление IAB/IESG по Вассенаарскому соглашению

http://www.iab.org/iab/121898.txt

Политика IETF в области прослушивания (RFC 2804)
ftp://ftp.isi.edu/in-notes/rfc2804.txt

Руководящие принципы ОЭСР по политике в области криптографии (1997 г.)
http://www.oecd.org//dsti/sti/it/secur/prod/e-crypto.htm

Руководящие принципы ОЭСР по безопасности информационных систем (1992)
http://www.oecd.org//dsti/sti/it/secur/prod/e_secur.htm

Комментарии Security Focus к конвенции Совета Европы
http://www.securityfocus.com/news/39

Заявление технических профессионалов
http://www.cerias.purdue.edu/homes/spaf/coe/TREATY_LETTER.html

Всеобщая Декларация прав человека
http://www.un.org/Overview/rights.html

Когда говорить НЕТ

Когда говорить “нет”

В последнем, шестом номере журнала Competitve Intelligence Magazine за прошлый год известный специалист КР Джон МакГональ (Helicon group) и его коллега Кирк Тайсон (Tyson Chicago) поместили короткое эссе на тему, когда профессионал конкурентной разведки должен говорить своему заказчику (а им может быть его/ее начальник или внешнему клиент) твердое НЕТ.

Это необходимо, по их мнению, когда клиенты или начальство попросту не понимают суть конкурентной разведки как вполне легального и этически оправданного вида информационной деятельности. Бывает и так, что автор запроса или задания прекрасно это понимает, но настаивает на выполнении задания,

хотя задача имеет отношение скорее не к КР, а корпоративному шпионажу.

Итак, советуют эксперты, необходимо говорить НЕТ, когда:

1. задание сопряжено с нарушением закона;

2. задание противоречит принятому в компании клиента кодексу деловой этики;

3. задание нарушает кодекс этики, принятый Обществом профессионалов конкурентной разведки;

4. когда Ваше собственное представление об этике предостерегает от ошибочного шага;

5. когда клиент настаивает на некорректном получении информации, используя распространенный довод “так поступают все”.

Strategic_and Competitive Analysisi книжная лавка

Strategic and Competitive Analysis: Methods and Techniques for Analyzing Business Competition.

Craig S. Fleisher, Babette Bensoussan

2003, Prentice Hall, 450 pages.

Авторы книги выделяют наиболее распространенные среди профессионалов конкурентной разведки модели бизнес-анализа и дают им подробную характеристику. Для сравнительного описания и оценки каждой модели они используют метод FAROUT©, используя критерии доступности и легкости использования аналитической модели, практичности и полезности.

Наряду с традиционными методами анализа (portfolio, value chain analysis), в кнбиге рассматриваются такие сравнительно новые методы как сценарный анализ, анализ ресурсов, анализ функциональных возможностей.

В поле зрения авторов как техника внешнего анализа (бизнес-среда), так и техника, сфокусированная на внутренних факторах деятельности организации.

Книга предназначена для практиков конкурентной разведки, как опытных экспертов, так и новичков в этом деле, маркетологов, студентов и слушателей бизнес-школ, просто интересующихся методами анализа.

Espinage_And The Craft - review

F,W.Rustmann

CIA, INC: Espionage And The Craft of Business Intelligence.

Jr. Brassey’s. 217 pages

Автор книги Ф. Рустман прослужил 24 года в отделе секретных операций ЦРУ и после выхода в отставку основал компанию деловой разведки CTC International group Limited.

Его профессиональное прошлое, отмечает The Tampa Tribune, имело значение для вывода, который он обосновывает в своей книге: «наибольшая угроза бизнесу очень часто исходит изнутри». Автор детально описывает слабости и уязвимости компаний, наиболее типичные сложные ситуации, в которые они попадают, методы и способы защиты внутренней конфиденциальной информации.

В частности, приводит пример, когда высокое должностное лицо одной автомобильной компании «передал» конкуренту шестерых ведущих служащих и важную информацию. Финал скандальной истории таков: конкурент был вынужден выплатить потерпевшей стороне компенсацию в 100 млн. долларов и закупить запчасти на один миллиард долларов.

В книге также рассматривается киберпреступность, способы проникновения во внутриофисные компьютерные сети, базы данных, личные дела.

Особе внимание автор уделяет методике проверки поступающих на службу в компанию. По его мнению, этот аспект работы с кадрами недооценивается, в то время как очень часто сведения, предоставляемые при приеме на работу об образовании и послужном списке кандидата, далеки от реальности.

Книга завершается разделом о терроризме и рекомендациями по личной защите в зарубежных поездках.