

личная и семейная тайна в советский период либо вообще не упоминались в законе (в том числе и в уголовном), либо в законе провозглашались и защищались отдельные ее аспекты (например, такие, как тайна связи), либо данное право декларировалось, но защита его оставалась только фрагментарной.

Изменения в сфере юридической охраны частной жизни человека произошли в 1993 г. 12 декабря 1993 г. на всенародном референдуме была принята ныне действующая Конституция Российской Федерации. Статьями 23 и 24 Конституции впервые введены такие понятия как «частная жизнь», «личная тайна», «семейная тайна». Конституция не только закрепила само право, но и установила запрет на совершение действий с информацией о частной жизни человека без его согласия. В ней, как известно, говорится: «Сбор, хранение, использование и распространение информации о частной жизни лица без его согласия не допускаются» (ст. 24 Конституции РФ). Такие изменения были связаны с тем, что Российская Федерация была провозглашена демократическим государством, в котором чело-

век, его права и свободы признаются высшей ценностью.

В уголовном законодательстве неприкосновенность частной жизни и запрет на совершение действий со сведениями, составляющими личную или семейную тайну, нашли свое отражение в УК РФ 1996 г. В этом кодексе в гл. 19 законодатель, как известно, предусмотрел ответственность за нарушение неприкосновенности частной жизни лица. Ст. 137 УК РФ предусматривает ответственность за незаконное соби́рание или распространение сведений о частной жизни лица, составляющих личную или семейную тайну.

В целом, следует отметить, что развитие уголовно-правовых норм, предусматривающих ответственность за нарушение неприкосновенности частной жизни, отражает стремление законодателя к закреплению в нормативно-правовых актах приоритета прав и свобод человека и гражданина. В соответствии с этим наблюдается тенденция к такому изменению норм, при котором можно говорить о реальной, а не декларативной защите частной жизни лица.

Литература

1. Уложение о наказаниях уголовных и исправительных 1866 г. с дополнениями по 01 декабря 1881 г. СПб., 1882.
2. Российское законодательство X–XX веков. Т. 8. М., 1991.
3. Резон А. Уголовное уложение. Краткое изложение глав положений его в сопоставлении с действующим законодательством. СПб., 1903.
4. Борзенков Г. Если задета честь // Человек и закон. 1998. № 1.
5. Ной И.С. Охрана чести и достоинства личности в советском уголовном праве. М., 1959.

Е.В. Громов

РАЗВИТИЕ УГОЛОВНОГО ЗАКОНОДАТЕЛЬСТВА О ПРЕСТУПЛЕНИЯХ В СФЕРЕ КОМПЬЮТЕРНОЙ ИНФОРМАЦИИ В ЗАРУБЕЖНЫХ СТРАНАХ (США, ВЕЛИКОБРИТАНИИ, ФРГ, НИДЕРЛАНДАХ, ПОЛЬШЕ)

Юридический институт Томского государственного университета

Законодательство об уголовной ответственности за компьютерные преступления в различных странах мира существенно отличается.

Одной из первых стран мира, принявшей меры по установлению уголовной ответственности за совершение преступлений рассматриваемого вида, явились Соединенные Штаты Америки, где компьютерная преступность появилась несколько раньше, чем в других государствах.

В 1977 г. в США был разработан законопроект о защите федеральных компьютерных систем. Он предусматривал уголовную ответственность за:

- введение заведомо ложных данных в компьютерную систему;
- незаконное использование компьютерных устройств;
- внесение изменений в процессы обработки информации или нарушение этих процессов;
- хищение денежных средств, ценных бумаг, имущества, услуг, ценной информации, совершенные с использованием возможностей компьютерных технологий или с использованием компьютерной информации.

На основе данного законопроекта в октябре 1984 г. был принят Закон о мошенничестве и зло-

употреблении с использованием компьютеров – основной нормативно-правовой акт, устанавливающий уголовную ответственность за преступления в сфере компьютерной информации. В последующем он неоднократно (в 1986, 1988, 1989, 1990, 1994 и 1996 гг.) дополнялся.

Нынче он включен в виде §1030 Титула 18 Свода законов США [1, р. 632–634; 2, с. 111–114].

Данный закон установил ответственность за деяния, предметом посягательств которых является «защищенный компьютер» (находящаяся в нем компьютерная информация). Под ним понимается:

1) компьютер, находящийся в исключительном пользовании правительства или финансовой организации, либо компьютер, функционирование которого было нарушено при работе в интересах правительства или финансовой организации;

2) компьютер, являющийся частью системы или сети, элементы которой расположены более чем в одном штате США.

Одновременно уголовный закон устанавливает, что уголовная ответственность наступает в случаях:

1) несанкционированного доступа – когда посторонний, по отношению к компьютеру или компьютерной системе, человек вторгается в них извне и пользуется ими;

2) превышение санкционированного доступа – когда законный пользователь компьютера или системы осуществляет доступ к компьютерным данным, на которые его полномочия не распространяются.

Данный закон устанавливает ответственность за семь основных составов преступлений, которыми признаются:

– компьютерный шпионаж, состоящий в несанкционированном доступе или превышении санкционированного доступа к информации, а также получение информации, имеющее отношение к государственной безопасности, международным отношениям и вопросам атомной энергетики (§1030 (a)(1));

– несанкционированный доступ или превышение санкционированного доступа к информации из правительственного ведомства США, из какого бы то ни было защищенного компьютера, имеющего отношение к межштатной или международной торговле, а также получение информации из финансовых записей финансового учреждения, эмитента карт или информации о потребителях, содержащейся в файле управления учета потребителей (§1030 (a)(2));

– воздействие на компьютер, находящийся в исключительном пользовании правительственного ведомства США, или нарушении функционирования компьютера, используемого полностью или частично Правительством США (§1030 (a)(3));

– мошенничество с использованием компьютера – доступ, осуществляемый с мошенническими намерениями, и использование компьютера с целью получения чего бы то ни было ценного посредством мошенничества, включая незаконное использование машинного времени стоимостью более 5 тысяч долларов в течении года, т.е. без оплаты использования компьютерных сетей и серверов (§1030 (a)(4));

– умышленное или по неосторожности повреждение защищенных компьютеров (§1030 (a)(5));

– мошенничество путем торговли компьютерными паролями или аналогичной информацией, позволяющей получить несанкционированный доступ к информации, если такая торговля влияет на торговые отношения между штатами и с другими государствами, или на компьютер, используемый правительством США (§1030 (a)(6));

– угрозы, вымогательство, шантаж и другие противоправные деяния, совершаемые с использованием компьютерных технологий (§1030 (a)(7)).

Также можно выделить §1029 Титула 18 Свода законов США [3, р. 631–632; 4, с. 109–111], которым предусмотрена ответственность за торговлю похищенными или поддельными устройствами доступа, которые могут быть использованы для получения денег, товаров или услуг.

Несмотря на столь детальную регламентацию вопросов уголовной ответственности за компьютерные преступления, правоохранительные органы США испытывают значительные затруднения в случаях, когда речь ведется о привлечении к ответственности лиц, которые совершают компьютерные преступления, осуществляя доступ к компьютерам США из-за рубежа. По мнению экспертов этого можно было бы избежать при условии включения в статьи уголовного закона квалифицирующих признаков – совершения преступлений с использованием возможностей глобальных компьютерных сетей и осуществления несанкционированного доступа с компьютеров, находящихся за пределами США, или через них [5].

Была вынуждена отреагировать на компьютерные преступления и Великобритания, известная консерватизмом правовой системы. Длительное время Великобритания пыталась справиться с данным явлением, используя свой многовековой опыт судопроизводства, но под «напором» компьютерной преступности «сдалась». С августа 1990 г. вступил в силу Закон о злоупотреблениях компьютерами.

В соответствии с ним к уголовно наказуемым отнесены:

– умышленный противозаконный доступ к компьютеру или содержащимся в нем компьютерной информации или программам (ст. 1);

– умышленный противозаконный доступ к компьютеру или содержащимся в нем компьютерной информации или программам для их последующего использования в противозаконных целях (ст. 2);

– неправомерный доступ к компьютерной информации на машинном носителе, в компьютере, компьютерной системе или сети, с целью, или если это повлекло уничтожение, блокирование, модификацию либо копирование информации, нарушения работы компьютера, компьютерной системы или сети (ст. 3).

Одним из последних подтверждений серьезности проблемы компьютерных преступлений и решительности государств в борьбе с этой проблемой может служить вступление в действие в Великобритании «Закона о терроризме 2000 года». Данный закон призван усилить борьбу в связи с использованием территории Великобритании как базы различными подрывными группировками. При этом отмечается, что в данном законе определение терроризма впервые расширяется и затрагивает область киберпространства. Английские правоохранительные органы вправе считать террористическими действия, которые «серьезно вмешиваются или серьезно нарушают работу какой-либо электронной системы» и принимать к компьютерным преступникам, избавленным в таких действиях, столь же решительные меры как к боевикам Ирландской рабочей армии [6, с. 1–2].

В Германии встал вопрос о закреплении уголовной ответственности за преступления в сфере компьютерной информации в УК уже в 1986 г. (по данным статистики в 1987 г. было зарегистрировано 3355 таких преступлений, а в 2002 г. – уже 57488). Эти составы преступлений были введены «Вторым законом о борьбе с экономической преступностью» (2. Gesetz zur Bekämpfung der Wirtschaftskriminalität) в УК ФРГ 1 августа 1987 г. В Уголовном кодексе Германии [7] не существует специального раздела, посвященного компьютерным преступлениям (преступлениям в сфере компьютерной информации); нормы, содержащие ответственность за преступления в сфере компьютерной информации рассредоточены по разделам Особенной части кодекса:

– § 202a шпионаж данных (Ausspähen von Daten);

– § 263a компьютерное мошенничество (Computerbetrug);

– § 269 фальсификация данных, имеющих доказательственное значение (Fälschung beweiserheblicher Daten);

– § 270 обман при помощи ЭВМ при обработке данных (Täuschung in Rechtsverkehr bei Datenverarbeitung);

– § 303a изменение данных (Datenveränderung);

– § 303b компьютерный саботаж (Computersabotage).

Необходимо отметить, что немецкий уголовный закон использует специальный термин – Daten, определение которого дает в абз. 2 § 202a – это данные, которые сохранены или передаются электронным, магнитным или иным, непосредственно визуально не воспринимаемым способом [8, с. 347–348].

В § 202a – шпионаж данных, входящем в раздел 15 Уголовного кодекса ФРГ «Нарушение неприкосновенности и тайны частной жизни», предусмотрена ответственность тех лиц, «кто незаконно получает данные, то есть, которые ему не предназначаются и особо охраняются от незаконного к ним доступа, или кто передает их другому лицу». За совершение данного преступления, согласно УК ФРГ, предусмотрена уголовная ответственность в виде лишения свободы на срок до трех лет или денежно-го штрафа.

§ 263a – компьютерное мошенничество [9, с. 2105–2115], – выделено в самостоятельный вид мошенничества, за которое предусматривается ответственность до 5 лет лишения свободы или денежный штраф (т.е. как за неквалифицированный вид мошенничества). Данная норма сконструирована следующим образом: «Кто, действуя с намерением получить для себя или третьего лица имущественную выгоду, причиняет вред имуществу другого лица, воздействует на результат обработки данных путем неправильного создания программ, использования неправильных или неполных данных или иного неправомерного воздействия на результат обработки данных». В системе особенной части УК ФРГ, данный состав находится в 22 разделе – «Мошенничество и преступное злоупотребление доверием», содержащем десять параграфов, описывающих помимо простого и квалифицированного мошенничества различные его виды (в основу разделения мошенничества на виды положен способ совершения преступления).

§ 269 – фальсификация данных, имеющих доказательственное значение [10, с. 662–665], – находится в 23 разделе – «Фальсификация документов», в котором предусмотрена ответственность за различные способы фальсификации документов. Данный вид состава предусматривает уголовную ответственность за сохранение или изменение при помощи ЭВМ, путем обмана, данных, имеющих доказательственное значение, приводящее к восприятию документов как сфальсифицированных или поддельных, либо использование такого рода сохраненных или измененных данных.

В этом же разделе находится еще одна норма – обман при помощи ЭВМ при переработке данных [там же, с. 665–666] (§ 270 УК ФРГ). Причем, под переработкой понимается получение из введенных

данных посредством компьютерных программ новых данных.

В разделе 27 – «Повреждение имущества» наряду с различными способами и видами повреждения имущества находятся и два состава преступления, относимых учеными-юристами к компьютерным преступлениям – изменение данных (§ 303a) [11, с. 2344–2347] и компьютерный саботаж (§ 303b) [там же, с. 2347–2349].

Ответственность за первый состав преступления в виде лишения свободы до двух лет или денежного штрафа наступает, если лицо «противоправно стирает, делает непригодным для использования или изменяет данные». За второй – в виде лишения свободы на срок до 5 лет или денежного штрафа за нарушение обработки данных, имеющих существенное значение для чужого предприятия, организации или органа, если лицо совершило преступление, предусмотренное § 303a или испортило, повредило, сделало непригодным для дальнейшего использования по назначению или изменило устройство для переработки данных или носитель информации.

Таким образом, составы компьютерных преступлений сконструированы как квалифицирующие виды простых составов преступлений, имеющих различные объекты посягательств.

Среди европейских государств, которые повели решительную борьбу с компьютерными преступлениями с момента их появления в жизни общества одно из ведущих мест занимают Нидерланды (Голландия). В Нидерландах был создан Консультативный комитет по компьютерным преступлениям, который предложил конкретные рекомендации по внесению изменений в Уголовный кодекс и Уголовно-процессуальный кодекс Нидерландов [12].

Консультативный комитет не дал определения компьютерных преступлений, но разработал их классификацию.

В то же время полицейское разведывательное управление, занимающейся регистрацией всех случаев компьютерных преступлений, использует следующее определение компьютерного преступления: это поведение, которое (потенциально) вредно и имеет отношение к устройствам, связанным с компьютерами с точки зрения хранения, передачи и обработки данных. Полицейское разведывательное управление делает различие между компьютерными преступлениями, в которых компьютер является объектом преступления, и теми, в которых он – орудие преступления.

Начиная с 1987 г. полицейское разведывательное управление использует для анализа пять видов компьютерных преступлений:

– совершаемые обычным способом, но с использованием технической поддержки в компьютерной среде;

– компьютерное мошенничество;

– компьютерный террор (совершение преступлений с целью повреждения компьютерных систем);

1) использование несанкционированного доступа;

2) использование вредоносных программ, типа компьютерных вирусов;

3) совершение других действий, включая физическое повреждение компьютера;

– кража компьютерного обеспечения (пиратство);

– остаточная категория, включающая все другие типы преступлений, которые не подпадают под вышеперечисленные категории.

Данный перечень видов преступлений в целом соответствует приведенной выше Рекомендации № R (89) 9 Совета Европы, но отличается более простым их описанием.

Причина отсутствия общепризнанного определения компьютерного преступления заключается в том, что, по мнению нидерландских ученых, существует множество трудностей при формулировании определения, которое, с одной стороны, было бы достаточно емким, а с другой – достаточно специальным. Применяется два понятия компьютерного преступления – в узком и широком смысле. В узком смысле – это совершение преступления, которое невозможно выполнить без использования компьютера или другого автоматического устройства как объекта или инструмента преступления.

В 1993 г. в Нидерландах был принят Закон о компьютерных преступлениях, дополняющий УК Голландии новыми составами:

– несанкционированный доступ в компьютерные сети (ст. 138a (1));

– несанкционированное копирование данных (ст. 138a (2));

– компьютерный саботаж (ст. 350a (1), 350b (1));

– распространение вирусов (ст. 350a (3), 350b);

– компьютерный шпионаж (ст. 273 (2)).

В ряд статей УК Голландии, предусматривающих ответственность за совершение традиционных преступлений (вымогательство (ст. 317, 318), запись (прослушивание, копирование) информационных коммуникаций, кража путем обмана служб (ст. 362с), были внесены дополнения, в редакции других статей (саботаж (ст. 161, 351), подлог банковских карточек (ст. 232) – даны специальные разъяснения. Были значительно изменены такие составы, как шпионаж (ст.ст. 98, 98a), вмешательство в коммуникации (ст. 139a, 139b), порнография (ст. 240b), что позволяет в настоящее время использовать данные составы преступлений, в соответствующих случаях, и для борьбы с компьютерными преступлениями [там же, с. 110–111, 125–128, 165–166, 168, 179, 191–192, 203–205].

Таким образом, уголовное законодательство Нидерландов предоставляет достаточно широкие возможности для борьбы с различными видами компьютерных преступлений, устанавливая помимо специальных норм дополнительные квалифицирующие обстоятельства в уже существующие уголовно-правовые нормы.

В модельном Уголовном кодексе Союза Независимых Государств компьютерные преступления помещены в XII раздел «Преступления против информационной безопасности», состоящей из одной главы с таким же названием и семи статей – ст. 286–292 УК СНГ [13, с. 195–197].

В целом можно вести речь о схожести УК СНГ и УК РФ, однако имеется ряд существенных отличий. Больше по сравнению с УК РФ количество статей объясняется выделением в УК СНГ самостоятельных статей в зависимости от субъективной стороны (при наличии умысла). Так, помимо несанкционированного доступа к компьютерной информации, повлекшие неосторожные последствия (ст. 286 УК СНГ, аналог ст. 272 УК РФ), отдельно предусмотрена уголовная ответственность, например, за модификацию компьютерной информации, компьютерный саботаж. УК СНГ выгодно отличается от УК РФ, носящего бланкетный в части компьютерных преступлений. В УК СНГ даются определения ряда понятий, например модификация компьютерной информации, компьютерный саботаж, неправомерное завладение компьютерной информацией. Однако санкции, предусмотренные в нормах УК СНГ, несомненно, нуждаются в более детальной проработке, так как имеются несоответствия между общественной опасностью деяний и наказанием за них. Отдельно в УК СНГ (ст. 290) предусмотрена уголовная ответственность за изготовление и сбыт специальных средств для получения неправомерного доступа к компьютерной информации, к компьютерной системе или их сети, что также является положительным моментом [там же, с. 197].

В ст. 287 УК СНГ заложены основы для правильного разграничения компьютерных и иных смежных составов преступлений, это также заслуживает положительной оценки [там же, с. 195].

Внимания заслуживает и системное изложение квалифицирующих признаков компьютерных преступлений. Для УК РФ в целом характерно именно системное изложение квалифицирующих признаков, однако в главе 28 законодатель ограничился простым перечислением квалифицирующих признаков.

Наказания, предусмотренные в УК СНГ за компьютерные преступления, не превышают наказания за преступления средней тяжести. Однако, неправомерное завладение информацией, совершенное при квалифицирующих обстоятельствах (со-

пряженное с насилием, совершенное с целью получения особо ценной информации), наказывается как тяжкое преступление (ч. 3 ст. 289 УК СНГ). За особо квалифицированный вид такого преступления (совершение преступления организованной группой, сопряженное с причинением тяжкого вреда здоровью или по неосторожности смерти либо иных тяжких последствий) – наказание назначается как за особо тяжкое преступление (ч. 4 ст. 289 УК СНГ). Такой подход представляется вполне обоснованным, так как помимо общественных отношений в сфере компьютерной информации причиняется вред другому объекту – жизни и здоровью граждан (нарушается нормальное развитие иных общественных отношений). При совершении преступления группой лиц по предварительному сговору или организованной группой, несомненно, повышает степень и характер общественной опасности преступления. Введение дополнительно квалифицирующего признака – совершение преступления с целью получения особо ценной информации, представляется спорным. Несомненно, существует более или менее ценная информация, однако данная категория является оценочной и зависит от субъективного восприятия значимости информации тем или иным лицом. При введении такого квалифицирующего признака необходимо в законодательном порядке дать некоторые ориентиры, позволяющие правоприменителю объективно определять ценность информации [там же, с. 196].

В Уголовном кодексе Республики Польша [14] содержится глава XXXIII «Преступления против охраны информации», состоящая из 6 статей, объектом которых являются общественные отношения в сфере информации как таковой. Общественные отношения в сфере компьютерной информации являются собой лишь часть объекта. Из этой главы можно упомянуть только о двух статьях – ст. 267 и 268 УК Польши. В ст. 267 УК устанавливается уголовная ответственность за неправомерный доступ к информации, в том числе путем повреждения электронного, магнитного или иного особого средства обеспечения ее безопасности. В ст. 268 УК Польши предусматривается уголовная ответственность лиц, не имеющих на то полномочия уничтожения, повреждения удаления или изменение записи на компьютерном носителе информации, имеющей особое значение обороноспособности страны, безопасности связи, функционирования правительственных или государственных органов. Данное преступление, согласно УК Польши, карается как раскрытие информации, составляющей государственную тайну.

Статьи 278, 287 УК Польши [там же, с. 95–96, 98], находящиеся в главе XXXV «Преступления против имущества», также можно отнести к «ком-

пьютерным» составам преступлений. Эти нормы предусматривают ответственность за:

– получение без согласия управомоченного лица чужой компьютерной программы с целью извлечения имущественной выгоды (ст. 278);

– влиянием неуправомоченным на то лицом на автоматизированное преобразование, собирание или передачу информации, или изменение, удаление, введение новой записи на компьютерный носитель информации с целью получения имущественной выгоды или причинения вреда другому лицу (ст. 287).

Достаточно интересным представляется то, что в данном случае если вред причинен самому близкому лицу, преследование возбуждается по заявлению потерпевшего.

Таким образом, в УК Польши проведено разделение компьютерных преступлений на две самостоятельные группы (соответственно их размещению в УК Польши) в зависимости от того, на что было направлено деяние субъекта – на собственно получение информации, либо на получение материальной выгоды. Такое разграничение представляется достаточно спорным, так как и в первом и во втором случаях субъект завладевает определенным объемом информации; и в первом, и во втором случаях лицо может быть заинтересовано именно получением материальной выгоды (например, передача вознаграждения за уничтожение информации

на компьютерном носителе, имеющей значение для обороноспособности страны.).

Исходя из вышеизложенного, можно сделать вывод, что зарубежное законодательство пошло по пути разграничения компьютерных преступлений в зависимости от той сферы общественных отношений, на которую посягает преступник. Данные сферы соответствуют криминологическим группам компьютерных преступлений. Можно выделить следующие три группы:

1) экономические компьютерные преступления (наиболее распространенные и опасные преступления), например, компьютерное мошенничество § 263a УК ФРГ;

2) компьютерные преступления против прав и свобод индивидуальных субъектов и организаций, нарушающие неприкосновенность частной сферы, например, незаконные злоупотребления информацией, находящейся на компьютерных носителях, разглашение сведений, имеющих частную, коммерческую тайну (сведения помимо конфиденциального характера, должны находиться на компьютерных носителях);

3) компьютерные преступления против интересов государства и общества в целом, например дезорганизация работы различных систем (оборонных, энергетических, газоснабжения), изменения данных при подсчете голосов на выборах и др.

Литература

1. Federal Criminal Code and Rules / Title 18 – Crime and Criminal Procedure – § 1030 Fraud and related activity in connection with computers – (amendment received to February 15, 1999), West Group, St. Paul. Minn, 1999.
2. Айков Д., Сейгер К., Фонсторх У. Компьютерные преступления. Руководство по борьбе с компьютерными преступлениями. М., 1999.
3. Federal Criminal Code and Rules / Title 18 – Crime and Criminal Procedure – § 1029 Fraud and related activity in connection with computers – (amendment received to February 15, 1999), West Group, St. Paul. Minn, 1999.
4. Айков Д., Сейгер К., Фонсторх У. Компьютерные преступления. Руководство по борьбе с компьютерными преступлениями. М., 1999.
5. Robert J. Sciglimpaglia. Computer Hacking: A Global Offense, 3 Pace Y.B. Int'l L. 199, 231 (1991); Keith Nicholson. International computer crime: a global village under siege / New England International & Comparative Law Annual. № 2. 1997. New England School of Law, Boston, Massachusetts. <http://www.nesl.edu/annual/vol2/computer.htm>
6. Хакеров впервые официально приравняли к террористам // Компьютерра. 2001. № 7.
7. Strafgesetzbuch mit Einführungsgesetz, Völkerstrafgesetzbuch, Wehrstrafgesetz, Wirtschaftsstrafgesetz, Betäubungsmittelgesetz, Versammlungsgesetz, Auszügen aus dem Jugendgerichtsgesetz und dem Ordnungswidrigkeitengesetz sowie anderen Vorschriften des Nebenstrafrechts. München, 2002.
8. Joeks Wolfgang. Strafgesetzbuch.. Studienkommentar. München, 2003.
9. Schönke/Schröder. Strafgesetzbuch. Kommentar. München, 2001.
10. Joeks Wolfgang. Strafgesetzbuch.. Studienkommentar. München, 2003.
11. Schönke/Schröder. Strafgesetzbuch. Kommentar. München, 2001.
12. Уголовный кодекс Голландии / Науч. ред. д.ю.н., проф. Б.В. Волженкин, пер. с англ. И.В. Мироновой. СПб, 2000.
13. Модельный уголовный кодекс для государств СНГ // Панфилов Е.И. Попов А.С. Компьютерные преступления. СПб., 1998.
14. Уголовный кодекс Республики Польша / Отв. ред. Э.А. Саркисова, А.И. Лукашов. Пер. с польск. Д.А. Бариловича. Минск, 1998.