ISSN 1727-1584

форма власності; предмет цього злочину, транспортні засоби, має всі ознаки чужого майна та додатково характеризується специфічними ознаками, закріпленими у примітці до ст.286 КК, яка носить комплексний характер, тобто розповсюджується на ряд статей КК; з огляду на те, що основним безпосереднім об'єктом цього злочину є власність, а не транспортна безпека, доцільно перенести кримінальну-правову заборону на вчинення цього злочину до розділу VI "Злочини проти власності".

ЛІТЕРАТУРА

1. Коржанський М.Й. Визначення окремих понять у Кримінальному кодексі України // Право України. -2002. -№ 10. –С.83-88.

2. http: // www.ipolis. ru/sign/ugon/ugon_carakter.htm - 15.07.2003.

3. Касынюк В.И., Корчева З.Г. Вопросы квалификации транспортных преступлений. -К.: УМК ВО, 1988. –70с.

4. Коржанський М.Й. Кваліфікація злочинів. -К.: Юрінком-Інтер, 1998. –415 с.

5. Бондаренко Н.А., Дзюба В.Т. Квалификация преступлений против общественного порядка и общественной безопасности. -К.: НИИ РИО КВШ, 1990. –70 с.

6. Шупаківський Р. Визначення об'єкта і предмета незаконного заволодіння транспортним засобом // Право України. -2003. -№ 4. –С.101-102.

7. Пасенюк О.М. Кримінальна реформа // Юридичний вісник України. -№ 10. -16.11.2001.

8. Матышевский П.С. Ответственность за преступления против социалистической собственности. -К.: Вища школа, 1983. –175 с.

9. Науково-практичний коментар до Кримінального кодексу України /Під ред. С.С. Яценка. -К.: А.С.К., 2002. – 934 с.

10.Ємельянов В.П. Кваліфікація злочинів проти власності. -Х.: Рубікон, 1996. –112 с.

11. Уголовный кодекс Республики Беларусь. –Минск: Изд-во «Амалофея», 1999. –314 с.

Надійшла до редколегії 11.02.2004

АНДРЮЩЕНКО И.Н. ОБЪЕКТ НЕЗАКОННОГО ЗАВЛАДЕНИЯ ТРАНСПОРТНЫМ СРЕДСТВОМ: ТРАНСПОРТНАЯ БЕЗОПАСНОСТЬ ИЛИ СОБСТВЕННОСТЬ?
Определен основной непосредственный объект незаконного завладения транспортным средством и место состава этого преступления в структуре Особой части Уголовного кодекса Украины.

***

ANDRJUSHCHENKO I.N. OBJECT ILLEGAL CAPTURE THE VEHICLE: TRANSPORT SAFETY OR THE PROPERTY?
The basic direct object illegal capture by a vehicle and a place of structure of this crime in structure Special parts of the criminal Code of Ukraine is determined.

УДК 343.851:004.7

Л.В. БОРИСОВА

Национальный университет внутренних дел

КРИМИНАЛИСТИЧЕСКАЯ ПРОФИЛАКТИКА МЕЖДУНАРОДНЫХ КОМПЬЮТЕРНЫХ ПРЕСТУПЛЕНИЙ

Рассмотрены основные проблемы компьютерных преступлений и их профилактики.

В современном международном праве существует понятие именно обязанности государств сотрудничать друг с другом и с ООН. До 1945 года это сотрудничество зависело от их доброй воли, а с принятием Устава ООН, основными принципами обязанности государств сотрудничать друг с другом и ООН стали: во-первых, то, что необходимость поддерживать мир и обеспечивать безопасность можно только посредством сотрудничества в разных сферах международной жизни; во-вторых, современные проблемы настолько усложнились, что в одиночку их решать уже практически невозможно [1, с.69].

Современное международное право полагает, что мировое сообщество состоит из независимых государств, обязательными атрибутом которых является собственная территория, на которой государство осуществляет полную юрисдикцию.

Соглашение о правах и обязанностях государств, принятое в 1993 г. в Монтевидео утверждает, что государство, будучи «представителем международного права», должно обладать постоянным населением, определенной территорией, правительством, возможностью устанавливать отношения с другими странами. Государство «характеризуется объективно присущим ему особым политико-юридическим свойством – суверенитетом» [2, с.166] и «каждое государство обязано уважать суверенитет других участников системы, то есть их право в пределах собст-

ISSN 1727-1584

венной территории осуществлять законодательную, исполнительную, административную и судебную власть без какого-либо вмешательства со стороны других государств» [3, с.28]. Таким образом, государство имеет право издавать законы, управлять, определять юрисдикцию и компетентность собственных служб и организаций, и, кроме того, законы, принятые в этом государстве, обязательны для всех, проживающих на территории этого государства. Территориальная целостность является также краеугольным камнем для системы ООН, проявляемая в определении того, что государство должно быть высшей властью на собственной территории.

Многие долгое время протестовали против подобного определения суверенитета, объясняя это тем, что никогда еще не существовало «полного» и «безусловного» суверенитета. Как бы то ни было, исходя из традиционных концепций юрисдикции и суверенитета, международное право признает юрисдикцию различных «мнений» на предписание и исполнение. Наименее спорной и наиболее очевидной основой осуществления законодательной деятельности государства является территориальная основа. Территориальный принцип является базовым для осуществления странами своего законодательства. В случаях, когда в основе лежат несколько принципов, доминирующим все равно является территориальный, потому что для осуществления законодательной деятельности необходима возможность представить обе стороны перед судом.

Другим принципом, также практически не вызывающим возражений, является «национальный принцип», т.е. возможность государства осуществлять юрисдикцию над своими гражданами, находящимися в любой точке мира. В соответствии с обычным законодательством, все преступления считаются «локальными», т.е., кроме специально оговоренных, все преступные деяния не подразумевают какой-либо экстратерриториальный эффект. Граждане, находящиеся за пределами своего государства, не обязаны полностью соблюдать законы своего государства. Возникает вопрос муниципального законодательства каждой страны в отдельности и проблема применения соответствующего закона. Государство не может применять юридическое воздействие на своего гражданина, находящегося на территории другого государства, и вынуждено ожидать его (гражданина) возвращения.

«The effects principle» более проблематичен. В его основе лежит возможность государства осуществлять уголовное преследование за деяние, угрожающее интересам государства, совершенное за пределами этого самого государства. Нет необходимости пояснять, что не существует конкретной определенности, насколько то или иное действие влияет на государственные интересы, и в каком случае потерпевшее государство может применять этот принцип; очевидно одно - совершенное деяние обязано различными странами рассматриваться как чрезвычайно преступное, что должно дать потерпевшей стороне основания применять подобное экстратерриториальное регулирование. Но тогда получается, что возможность государства осуществлять юрисдикцию за пределами своей территории противоречит принципам международного права.

«Защитный принцип» может рассматриваться как несколько ограниченный «effects principle». В соответствии с ним, государственная юрисдикция может распространяться на деяния, угрожающие безопасности или другим государственным интересам, совершенные иностранными гражданами. Очевидно, что довольно сложно оценить степень возможных угроз, позволяющий использовать этот принцип.

Еще более противоречивым является принцип «пассивной индивидуальности», т.е. право государства законодательно защищать своих граждан от возможных преследований за пределами собственной территории. Некоторые аналитики считают, что подобная юридическая основа не может иметь всеобщего признания, кроме того, использование подобной юрисдикции противоречит национальным законодательствам некоторых стран и определенным международным соглашениям.

Принципом юрисдикции с обширным доступом и, вероятно, самым узким спектром, является принцип, основанный на т.н. «общей юрисдикции». Он применим для очень узкой категории действий, за совершение которых предусмотрено законодательное преследование странами, разделяющими этот принцип, вне зависимости от места совершения таких преступлений и их влияния на государство, осуществляющее юрисдикцию.

Во-первых: существование различных принципов и факт того, что большинство из них противоречат друг другу, должно привести к мысли о том, что проблемы юрисдикции не новы в современном международном праве. Internet и компьютерные системы только расширяют спектр потенциальных проблем.

Во-вторых: следует отметить очевидное противоречие «глобализации» и «безграничности» Internet изложенным принципам юрисдикции, которое несет определенные изменения в концепциях осуществления юрисдикции.

Юридическое равенство государств не означает их фактического равенства, что учитывается в реальных международных отношениях [3, с.30]. Существование нескольких юридических основ вполне традиционно. В большинстве противоречивых случаев решение, как правило, принимается либо в пользу «территориального» принципа, либо в соответствии с определенными международными соглашениями. Тем не менее, сегодня вполне может возникнуть ситуация, когда попытка одной страны определить правила экстратерриториальной юрисдикции другой страной может восприниматься как посягательство на государственный суверенитет. Такими примерами являются ситуации, когда одно государство пытается осуществить действия, противоречащие местному законодательству; или же государство определяет криминальным деяния, не являющимися таковыми в соответствии с территориальной юрисдикцией.

Отсутствие границ – Internet. Перед тем, как начать дискуссию, каким образом Internet «ликвидирует» границы

ISSN 1727-1584

и «территориальность», важно осознать, что там, где чтят законность, Internet является лишь функцией глобальной телекоммуникационной революции. Пока существуют огромные объемы данных, связанных с помощью Internet, эта сеть, без сомнения, является единственной (и наиболее важной) информационной сетью в мире. Кроме Internet существует еще множество частных специализированных сетей, но, даже не учитывая их, можно утверждать, что изобретение модема (сегодня уже считающееся очень «древним») и международной телефонии означало, что люди, сидящие перед компьютером в одной стране, могут иметь неограниченные возможности по воздействию на компьютеры, находящиеся в других странах.

На техническом уровне – к битам и байтам. Основные Internet протоколы (IP) не рассчитаны на хранение данных о территориальном местонахождении клиента. Пакет информации, отмеченный для перевода из одного места в другое, просто ищет наилучший путь перехода от одного IP-адреса к другому. Представим довольно вероятную ситуацию. Некий пользователь, находящийся в Австралии, легко может, используя «telnet»-протокол, связаться с Unix-компьютером, находящимся в Сингапуре. Далее пользователь получает доступ к компьютеру на достаточно низком уровне. Вместо обычного созерцания web-страницы, австралиец вступает в более «близкие» отношения с «host»-компьютером. TCP/IP протокол, лежащий в основе сети Internet, устроен таким образом, что каждое нажатие клавиши пользователем передается на «host»-компьютер, где бы он (компьютер) не находился. Аналогично и каждый бит «host»-компьютера, адресованный подсоединившемуся пользователю, совершит путешествие через Internet от одного компьютера к другому. Таким образом, как в случае web-страницы, так в случае «telnet» пользователя и любого другого приложения, использующего TCP/IP протокол, происходит игнорирование территориальных границ. Компьютеры, расположенные между пользователем в Австралии и «host»-компьютером в Сингапуре не обязательно «знают» данные, переводимые с их помощью из пункта А в пункт Б через Internet. Их задача заключается лишь в переводе определенных «пакетов» информации от одного IP-адреса к другому.

Более того, связь через Internet вообще не имеет каких-либо географических ограничений. Раньше существовала довольно отчетливая связь между электронным адресом и его географическим размещением, но сегодня этого уже фактически нет. Также принято, чтобы существовала определенная корреляция между именем домена web-страницы и ее «родиной». Но сегодня уже и это ограничение не является реальным, поскольку сеть чрезвычайно распространена, и в ней предлагается множество «открытых» имен доменов, что фактически ликвидирует географическую «принадлежность» web-страницы.

Преступники и компьютеры – катятся вниз по наклонной? Преступники очень быстро осознали масштабы возможностей, предоставляемых Internet и электронными коммуникациями. Потери, понесенные коммерческими и государственными структурами за последние четыре года оцениваются в $ 600 млн. Среди всех киберпреступлений, совершаемых в мире, все больше становится т.н. «международных», т.е. использующих в качестве средств/жертв информационные системы, расположенные в различных странах. Например, в 1994 году на U.S. Air Force Laboratory была осуществлена атака, где в качестве «проводников» участвовало не менее 8 стран. В результате проведенного расследования New Scotland Yard арестовал 16-ти летнего хакера Richard Pryce, использовавшего компьютер с весьма скромными возможностями. Он был осужден, в соответствии с Britain's Computer Misuse Act 1990, к уплате в качестве штрафа всего лишь £ 1200.

В этих случаях требовалось проведение большого, комплексного и тщательного расследования, поскольку были атакованы информационные системы правительственных организаций. Преступный потенциал киберпреступлений, включающий шпионаж и саботаж, представляет большое беспокойство для всех стран. Но следует учесть, что даже простое и бесхитростное использование Internet может применяться для совершения вполне «традиционных» преступлений. Примером является классическое жульничество типа «раздуть и сплавить» (pump and dump), при котором соучастниками преступника распространяются слухи, посредством которых (слухов) цена каких-либо довольно недорогих объектов (как правило, дешевых акций) резко возрастает. Преступники продают эти объекты (акции), приобретенные по первоначальной цене, и, соответственно, остаются в большом выигрыше. В мае 1999 года житель Мельбурна Steven George Hourmouzis осуществил сделку по подобной схеме. И хотя он находился в Австралии, а «раздуваемые» им акции продавались через U.S.NASDAQ, сотрудничество американских и австралийских правоохранительных органов привело к его аресту и наказанию.

Другой распространенной преступной деятельностью в киберпространстве является продажа информации о кредитных картах, мошенничество при продаже товаров через Internet с последующим не предоставлением оных, не выполнение других торговых обязательств и т.д. Различные организации опубликовали списки наиболее распространенных, по их мнению, форм мошеннической деятельности в Internet. Такая деятельность хотя и более безвредна, по сравнению с другими формами преступной деятельности, но потенциально может повредить доверию к Internet как к среде ведения электронной коммерции.

Также следует отметить авторов различных вирусов, произведения которых, могущие принести (и приносящие) огромные убытки, распространены по всей мировой сети; одним из самых известных, по крайней мере, сегодня, является написанный филиппинцем Love Letter вирус.

Используя другие сравнительно «новые» технологии, киберпреступники могут поставить иные серьезные задачи перед правоохранительными органами. The Denial Service атака в феврале 2000 года является примером т.н. «разветвленной» атаки, когда при ее проведении используется

ISSN 1727-1584

большое число компьютеров. Эти компьютеры могут быть «сознательными» участниками, но, как правило, они являются невольными «сообщниками», будучи поражены различными вирусами типа «червяк» или «Троянский конь». Поскольку в нападении может принимать участие множество компьютеров, и они могут быть запрограммированы уничтожить «вирусный» код после проведения атаки, такие атаки чрезвычайно сложно отследить.

Следующим важным аспектом является развитие технологий шифрования, и используя их, преступники смогут хранить информацию, которая, даже будучи обнаруженной, вряд ли с легкостью может быть дешифрована.

Расследование киберпреступлений – бессмысленное занятие? После того, как мы рассмотрели: концепции, обычно принимаемые международным правом за основы соответствующих юрисдикций; каким образом Internet делает некоторые из таких концепций несостоятельными; каким образом преступники используют огромные технические возможности для совершения своих черных дел; предлагается рассмотреть юридические проблемы, возникающие перед следователем непосредственно во время расследования таких преступлений.

Трудности расследования. Осуществление расследования киберпреступлений довольно сложно в любой стране мира. Практически невозможно гарантировать факт того, что свидетельства (улики) могут быть получены, изолированы от вмешательства и вообще допустимы для представления в суде. Когда же к этим проблемам еще добавить элемент «интернациональности», то полученная смесь станет еще более «горькой».

Для того, чтобы обеспечить сотрудничество с соответствующим иностранным агентством надо, как минимум, знать, к кому обратиться. В связи с тем, что в некоторых случаях могут требоваться неотлагательные меры и могут быть задействованы партнеры в различных часовых поясах, было бы предусмотрительно открыть канал связи с соответствующими полномочиями для иностранных государств, что обеспечит обслуживание таких запросов в любое время дня и ночи во всех часовых поясах. Также международному сотрудничеству в немалой степени могут мешать различные юридические разногласия. В качестве примера приведем следующий случай:

В 1999 году вирус ILOVEYOU был запущен в Internet. По примерным оценкам, ущерб составил около U.S.$ 10 млрд., 80 % федеральных правительственных организаций США были заражены этим вирусом, пострадало 80 % шведских и 30 % английских информационных систем. Более того, даже АТМ системы в Бельгии были вынуждены прекратить свою работу. Когда же преступник был обнаружен, выяснилось, что он живет в пригороде Манилы, столицы Филиппин, и тогда же правоохранительные органы столкнулись с серьезной проблемой, - на Филиппинах не существовало специального закона, предусматривающего уголовную ответственность за совершенные преступником деяния. Поскольку для экстрадиции требуется признание действий злоумышленника преступными с двух сторон, а в данном случае на родине его действия не трактовались таковыми, то и экстрадиция была, соответственно, невозможной.

До тех пор пока большинство стран мира не примет законы, предусматривающие уголовную ответственность за преступления, совершенные в киберпространстве, такие юридические «дыры» будут делать международное сотрудничество в данной области невозможным и впредь. Филиппины, получив резкое осуждение со стороны мирового сообщества, быстро приняли полный кодекс законов, криминализирующих подобные преступные деяния. Тем не менее, большая часть мирового сообщества все еще не достаточно готова к борьбе с киберпреступлениями. Последние исследования показали, что только 9 из 52 стран, в которых проводилось изучение законодательной базы, законодательно готовы к борьбе с киберпреступностью.

Более того, даже если каждая страна примет требуемую законодательную базу, при расследовании киберпреступлений будет необходима помощь специальных представителей для исследования особенностей законодательств этих стран. Еще следует отметить, что область киберпреступлений принадлежит к области т.н. «высоких» технологий, и крайне необходимо, чтобы все страны обладали достаточно высоким техническим потенциалом в данной области. Следовательно, мировое сообщество должно сосредоточить свои усилия на помощи менее развитым государствам. Важно понимать, что проблема киберпреступлений – проблема не только «богатых» стран, и только общими усилиями и сотрудничеством можно ее решить. В мировом сообществе возникает все большая убежденность в необходимости эффективной борьбы с киберпреступностью. Но как этого можно добиться? Очевидно, существуют несколько путей – односторонние действия, частичное или всестороннее сотрудничество.

Односторонние действия. Для эффективной борьбы с киберпреступностью, по крайней мере, должна существовать законодательная база, предусматривающая уголовную ответственность за совершения преступлений, классифицируемых как «киберпреступления». Сюда должны включаться несанкционированные: доступ к компьютерам и компьютерным системам; изменение компьютерных данных; перехват данных; попытки отказать в законном доступе к компьютеру или компьютерной системе. Важно отметить, что односторонние действия не могут быть панацеей при борьбе с киберпреступностью. Как показано выше, эффективное решение международных проблем в данной области невозможно без международного сотрудничества. Тем не менее, в качестве основы или предпосылки к международному сотрудничеству, экстрадиции и взаимопомощи, государства должны иметь возможность самостоятельно реагировать на киберпреступления.

Частичное сотрудничество. С момента, когда в государстве возникает законодательная база для борьбы с киберпреступностью, может возникнуть необходимость в установлении партнерских отношений в данной области со странами-соседями. Например, экстрадиция может быть

ISSN 1727-1584

распространена и на осужденных по статьям о киберпреступлениях. Сюда же относятся соглашения о сотрудничестве на рабочем уровне, как формальные, так и неофициальные (соглашения). Например, Генеральный прокурор США Janet Reno способствовала созданию «Lawnet» – информационной сети, корректирующей действия правоохранительных органов в области киберпреступлений на всей территории США. В будущем эта сеть должна стать основой сотрудничества с соответствующими агентствами других стран, а также юридически способствовать быстрой локализации источника передачи данных, свидетельств (улик), помогать расследованию киберпреступлений иными способами. Сейчас трудно сказать, насколько успешным будет использование «Lawnet» на международном уровне сравнительно с ее функционированием в рамках США. Тем не менее, для стран, которые еще серьезно не занимались проблемой борьбы с киберпреступностью, опыт США может стать хорошей базовой точкой для работы в данной области.

Международные соглашения. Двустороннее сотрудничество может быть формой взаимной юридической (и не только) помощи. Но в связи с тем, что проблема киберпреступности затрагивает (или затронет в ближайшем будущем) практически все мировые государства, заключать двусторонние соглашения со всеми заинтересованными странами может быть довольно неэффективной формой сотрудничества. Поэтому необходимо искать более эффективные, многосторонние соглашения, возможно, на базе ООН. Всестороннее соглашение является выгодным по многим соображениям. Во-первых, такое соглашение исключает чрезмерные сложности, могущие возникнуть при большом количестве двусторонних соглашений. Во-вторых, оно способствует разрешению спорных вопросов, обычно возникающих за счет разногласий в законодательствах между странами-партнерами. Более того, оно вообще является базовым для международного правового сотрудничества в области киберпреступности.

На протяжении 4 лет представители Европы и США работали над проектом такого международного соглашения. Будучи принятым множеством стран, оно должно обеспечить «необходимый минимум» в законодательных базах стран-участниц и устанавливает т.н. «черный список» преступлений, ответственность за которые должна быть предусмотрена в национальных законодательствах, а также формирует механизм международного сотрудничества при расследовании и судебном преследовании в области киберпреступлений.

Однако, когда проект этого соглашения стал достоянием гласности, многие промышленные гиганты выступили против его принятия, поскольку оно казалось чрезмерно строгим и навязчивым, ущемляющим человеческие права. Другие выступали за то, что такое соглашение под маской «международности» просто проводит в жизнь политику США в данной области, направленную против конкурентов в Европе и Азии. В результате множества протестов против проекта этого соглашения, Совет Европы пересмотрел некоторые ключевые положения (intruder detection and counter-hacking tools should not be criminalized). В частности, большой спор вызвал вопрос о том, какую информацию о своих клиентах должны предоставлять Internet-провайдеры в случае запроса со стороны правоохранительных органов.

Очевидной остается необходимость в многостороннем международном сотрудничестве, без которого эффективная борьба с киберпреступностью просто невозможна.

Территориальность останется. Хотя Internet исторически был (и остается) географически независимым, существуют признаки возможного изменения такой ситуации. Это следует из того, что географически отследить и локализовать провайдера и web-страницу не является невозможным. Два следующих примера пояснят, почему.

Пример первый. Длительное время Соединенные Штаты применяли меры по контролю экспорта на «сильное» криптографическое программное обеспечение. Как следствие, легальное получение таких продуктов из открытых архивов в США было ограниченно пользователями на территории США. При попытке получения программного обеспечения проверялась принадлежность IP-адреса заказчика к Internet провайдерам США. Хотя такая методика была не совсем совершенной и, как пример, ограничения получения информации путем определения географического местоположения заказчика имел место.

Пример второй. Французский суд, хотя и при противодействии Yahoo, предписал принять возможные меры, чтобы пользователи Internet из Франции не могли получить доступ к сайтам Yahoo, содержащих нацистскую тематику. Это решение было принято после того, как специальная авторитетная экспертная комиссия установила, что не нарушая технологии и архитектуру Internet можно с 90 % процентной уверенностью установить географическую принадлежность пользователя Франции.

Два приведенных примера показывают, что проблемы, ставящиеся перед нами современными технологиями, могут решаться с помощью тех же технологий. Очевидно, что понятие территориальности может оказаться фундаментальным и в формировании концепции «киберправа».

Экстратерриториальное регулирование станет проще. Далее, даже если территориальность останется критическим фактором криминального регулирования или преследования. Поэтому мы полагаем, что различные экстратерриториальные трудности и разногласия, имеющие место сегодня, которые связаны с уже слегка устаревшими концепциями суверенитета и юрисдикции, в ближайшем будущем канут в Лету. Широчайший спектр возможностей для граждан одной страны влиять на жизнь других, не менее достойных граждан в других странах, приводит к неизбежному переосмыслению понятия «суверенитета». Важно также отметить, что концепция территориальности по-прежнему останется базовой.

Взаимное международное сотрудничество будет развиваться. Совместно с ослаблением «традиционных» сомнений в отношении экстратерриториального регулирова-

ISSN 1727-1584

ния, государства начнут самостоятельно способствовать взаимному международному сотрудничеству, что ни в коей мере не будет противоречить понятию «суверенитета», т.к. одним из его атрибутов является способность государства устанавливать отношения с другими государствами, порой даже независимо от понятия территориальности. Для достижения положительных результатов требуется участие максимально возможного количества стран. Этот процесс, безусловно, займет немалое время. Если еще учесть разный уровень технического развития стран, то становится очевидным, что технологии неизбежно будут опережать законодательство. Кроме того, существуют мнения, что Internet и электронная коммерция станут настолько популярными и распространенными, что любые международные и юридические проблемы будут представлять собой существенные проблемы при расследовании киберпреступлений. В такой ситуации государства найдут возможности пойти на необходимые, возможно и немного неприятные меры, а иного пути успешно бороться с киберпреступностью не существует.

ЛИТЕРАТУРА

1. Тимченко Л.Д. Международное право: Учебник. - Харьков: Консум; Ун-т внутр. дел, 1999. -528 с.

2. Курс международного права: В 7 т. -Т.1. Понятие, предмет и система международного права /Ю.А. Баскин, Н.Б. Крылов, Д.Б. Левин и др. -М.: Юриздат, 1989. --360 с.

3. Международное право: Учебник /Отв. ред. Ю.М. Колосов, В.И. Кузнецов. –М.: Международные отношения, 1996. –608 с.

Поступила в редколлегию 20.04.2004

БОРИСОВА Л.В. КРИМІНАЛІСТИЧНА ПРОФІЛАКТИКА МІЖНАРОДНИХ КОМП'ЮТЕРНИХ ЗЛОЧИНІВ
Розглянуто основні проблеми комп'ютерних злочинів і їхньої профілактики.

***

BORISOVA L.V. CRIMINALISTIC PREVENTIVE MAINTENANCE OF THE INTERNATIONAL COMPUTER CRIMES
The basic problems of computer crimes and their preventive maintenance are considered.

В.С. ВЕНЕДИКТОВ
докт. юрид. наук, проф.
Національний університет внутрішніх справ

УДК 364.442.6-057.36

СТАН СОЦІАЛЬНО-ПРАВОВОГО ЗАХИСТУ ПРАЦІВНИКІВ ОРГАНІВ ВНУТРІШНІХ СПРАВ В СУЧАСНИХ УМОВАХ РОЗВИТКУ ДЕРЖАВИ ТА СУСПІЛЬСТВА

Розглянуті сучасні проблеми соціально-правового захисту працівників органів внутрішніх справ та надані пропозиції з його вдосконалення.

В сучасних умовах розвитку процесів гуманізації соціально-правових інститутів суспільства, розширення правових гарантій захисту прав, свобод і законних інтересів громадян, перед органами внутрішніх справ стоять складні і відповідальні завдання, які вимагають принципово нових підходів до їх вирішення, суттєвого внеску кожного працівника ОВС у справу охорони прав, свобод і законних інтересів людини і громадянина, громадського порядку; зміцнення економічного потенціалу держави, її конституційного устрою. Ефективність функціонування органів та підрозділів внутрішніх справ безпосередньо залежить від якості персоналу та його соціально-правової активності, що, в свою чергу, обумовлено ступенем захищеності прав, свобод та законних інтересів кожного працівника з боку держави.

Слід зазначити, що для служби працівників органів внутрішніх справ характерні значні фізичні, психологічні й емоційні перевантаження. Це і стресові ситуації, і реаль-