Міністерство освіти і науки України
ДВНЗ «Прикарпатський національний
університет імені Василя Стефаника»

Навчально-науковий юридичний інститут

Міжнародний журнал

Право і суспільство

International Journal

Law & Society

Журнал засновано
у 2014 році

Видається
двічі на рік

Випуск 7

Івано-Франківськ - 2018

ISSN 2410-4787

Свідоцтво
про державну реєстрацію КВ 20893-10623 Р
від 21 липня 2014 року

М68 Міжнародний журнал «Право і суспільство» *[текст]*: за ред. д-ра юрид. наук, проф. Васильєвої В.А. - Випуск 7. – Івано-Франківськ: Фоліант, 2018. - 119 с.

Випуск підготовлено за матеріалами Міжнародної науково-практичної конференції, організованої Навчально-науковою лабораторією дослідження проблем політики в сфері боротьби зі злочинністю Науково-дослідного інституту вивчення проблем злочинності імені академіка В.В.Сташиса спільно з навчально-науковим юридичним інститутом ДВНЗ «Прикарпатський національний університет імені В.Стефаника» (м.Івано-Франківськ, 26-28 квітня 2018 року) за підтримки Координатора проектів ОБСЄ в Україні. Висвітлюються результати наукових досліджень стосовно політики в сфері боротьби зі злочинністю. Для студентів, слухачів, курсантів юридичних факультетів, науковців, практичних працівників та всіх зацікавлених осіб

Адреса редакційної колегії:
76018, м. Івано-Франківськ, вул. Шевченка, 44а
Тел.: (0342) 59-61-33
E-mail: lawdept@pu.if.ua

РЕДАКЦІЙНА КОЛЕГІЯ

Mariusz Załucki, Prof, nadzw, Dr hab, Голова інституту приватного права Академії А.Ф.Моджевського, завідувач кафедри цивільного права (Польща, Краків)

Алиев Амир - проф., д.ю.н., завідувач кафедри ЮНЕСКО по правам людини і інформаційному праву юридичного факультету Бакінського Державного Університету (Азербайджан, Баку)

Зорин Георгий Алексеевич, проф., д.ю.н., професор кафедри кримінального процесу і криміналістики Гродненського державного університету ім. Янки Купали (Білорусь, Гродно)

Чебуранова Светлана Егоровна, доц., к.ю.н., Декан юридичного факультету Гродненського державного університету ім. Янки Купали (Білорусь, Гродно)

Адамович Сергій Васильович, проф., д.і.н., Професор кафедри теорії та історії держави і права Юридичного інституту ПНУ ім. В. Стефаника (Україна, Івано-Франківськ)

Борисов Вячеслав Іванович, проф., д.ю.н., Професор кафедри кримінального права Національного юридичного університету ім.Ярослава Мудрого, акад. НАПрН України, академік-секретар відділу кримінально-правових наук НАПрНУ, член Міжнародної асоціації кримінального права (Україна, Харків)

Васильєва Валентина Антонівна, проф., д.ю.н., Заслужений юрист України, Директор навчально наукового юридичного інституту, Завідувач кафедри цивільного права ПНУ ім. В. Стефаника (Україна, Івано-Франківськ)

Кобецька Надія Романівна, проф., д.ю.н., Завідувач кафедри трудового, екологічного та аграрного права ПНУ ім. В. Стефаника (Україна, Івано-Франківськ)

Крупчан Олександр Дмитрович, проф., д.ю.н., Заслужений юрист України, академік НАПрН України, Директор НДІ ПП ім. Ф.Г.Бурчака (Україна, Київ)

Луць Володимир Васильович, проф., д.ю.н., академік НАПрН України, Голова спеціалізованої Ради НДІ ПП ім. Ф.Г.Бурчака (Україна, Київ)

Фріс Павло Львович, проф., д.ю.н., Заслужений діяч науки і техніки України, Завідувач кафедри кримінального права ПНУ ім. В. Стефаника, член Міжнародної асоціації кримінального права (Україна, Івано-Франківськ)

Алиев А.И.

Доктор юридических наук, профессор, Бакинский Государственный Университет, Юридический факультет, Заведующий кафедрой ЮНЕСКО по правам человека и информационному праву

Ибрагимова А.Н.

Доктор философии по праву, Бакинский Государственный Университет, Юридический факультет, Преподаватель кафедры "Конституционное право"

Рзаева Г.А.

Доктор философии по праву, Бакинский Государственный Университет. Юридический факультет, Преподаватель кафедры ЮНЕСКО по правам человека и информационному праву

Aliyev A.I.

Prof. Baku State University, head of department:Human rights and information law of UNESCO

Ibrahimova A.N.

PhD Lecturer at the Department of Constitutional law at Baku State University

Rzayeva G.A.

PhD Lecturer at the UNESCO department of Human rights and information law at Baku State University

ИНФОРМАЦИОННАЯ БЕЗОПАСНОСТЬ: ПРОБЛЕМА НЕПРИКОСНОВЕННОСТИ ЛИЧНОСТНЫХ ПРАВ

Понятие личностных прав

В наших законах отсутствует понятие «личностных прав». Личностные ценности, входящие в понятие личностных прав не определены путем перечисления, также в законах не дано открытое и четкое определение понятия личностных прав. Однако как общепринято в доктрине,

права на такие личностные ценности, как жизнь, физическую полноценность, здоровье, честь и достоинство, имя, изображение, частную жизнь, персональные данные, свободы, признаваемые по причине существования лиц, выражают личностные права.

Защита личности как целого позволит ценностям, формирующим личность воспользоваться данной защитой.

Особенности личностных прав

1.Абсолютность особенности быть правом.

Личностные права абсолютны, т.е. могут быть адресованы каждому лицу, а правообладатель, в свою очередь, может желать не нарушения данного права для каждого лица (14, с.127)

2.Особенность быть личностью.

Понятие личности оценивается не богатством, т.е. наличием денег, а охраняет нравственные ценности, не носящие экономическую ценность. Однако в некоторых ситуациях вследствие нападения на ценности существования данной личности материальный ущерб может стать основным предметом обсуждения. Например, распространение врачом скрытой съемки, проведенной в ходе обследования какого-либо лица может подорвать доверие пациента к нему, вследствие чего врач теряет пациента и т.д.

3.Особенность привязанности к личности.

Личностное право является одним из прав, предоставленных личности по причине того, что он является личностью и не может быть предоставлено другому, не вызывает потерю времени, от него нельзя отказаться, не может обанкротиться, может быть использовано лишь правообладателем.

4. Отсутствие особенности сэкономить.

Личностные права являются принадлежащим только своему обладателю правом лица, которым он не экономит и от которого не откажется (10, с.93)

Классификация личностных прав

Законодателем границы личностных прав не ограничены. Меняющиеся человеческие взаимоотношения, развивающаяся технология, непрерывное изменение и развитие личностных ценностей в связи с повседневными требованиями, как основной вопрос повестки дня обусловили важность отсутствия границ в данном вопросе. Однако если учесть, что данная ситуация создаст трудности в определении личностных ценностей, то примерная классификация личностных ценностей в краткие сроки способна содействовать устранению проблем, которые могут воз-

никнуть в будущем. В число личностных прав, в наибольшей степени подвергающихся этой дискриминации входят материальные личностные права, нравственные личностные права и социальные личностные ценности. (4, с.231) Поэтому целостность лица формируется на базе права на здоровье, нравственной целостности и физических личностных ценностей. Например, право лица на требование уважения к его отношениям с индивидами, вместе с которыми он живет в обществе, к целостности семьи относится к нравственным личностным ценностям. А честь и достоинство, частная жизнь и свобода лица, развиваемые и охраняемые им внутри общества во взаимоотношениях с другими членами общества формируют социальные ценности лица (6, с.23)

Некоторые авторы классифицируют личностные ценности как физические, нравственные личностные ценности и профессиональные, коммерческие ценности. Такие ценности, как физическая целостность, нравственное развитие, обеспечивающие наделенность человека здоровым и безупречным физическим качеством и способность его продолжения, являются его физическими ценностями. А нравственные личностные ценности включают такие ценности, как честь и достоинство, частная жизнь, свободы. Как отмечает турецкий автор Тандоган, составить полный список личностных ценностей и подразделить их на категории по ограниченному перечню невозможно.

Нам представляется, что нельзя выделять личностные ценности в полной мере, так как личностные ценности в одном направлении входят в одну личностную ценность, а в другом направлении - в совершенно иную. Эти ценности, являются проявлением личностного права, вследствие чего лишь одно вмешательство способно нарушить несколько личностных ценностей. Следует также отметить, что личностные права ввиду наличия общих особенностей образуют тесную целостность (8, с.153)

Основные личностные ценности

Жизнь

Наиболее важной физической ценностью лица является его жизнь. Лицо не может отказаться от своего права на жизнь, так же требование уважения этого права со стороны других является его естественным правом. Убийство лица расценивается как нарушение его важнейшей ценности, вследствие чего право на жизнь находится под защитой понятия личностные права(6, с.123). Право на жизнь во многих законодательных актах защищается различными нормами (в уголовном законодательстве - наказаниями, в медицинском законодательстве – обязанностями врача и т.д.), А ст. 27 Конституции Азербайджанской Республики провозглашено

право каждого на жизнь.В нашем государстве и во многих государствах законом не разрешается распоряжение лицом своей жизнью – эвтаназия. Отношение к вопросу эвтаназии выражено в Законе Азербайджанской Республики «Об охране здоровья населения» от 26 июня 1997 г. Ст. 38 данного закона дано понятие эвтаназии и подобная медицинская операция в Азербайджане запрещена (5, с.142.).Однако известно, что в ряде государств право на жизнь, как одно из личностных прав, устанавливается в зависимости от воли лица. Например, в Нидерландах эвтаназия разрешена.

Физическая неприкосновенность

Лицо имеет права над каждым органом своего тела. Материальный и моральный ущерб, возникающий в тех случаях, когда они подвергаются нападению находятся под защитой личностных прав. Лицо, в отличие от права на жизнь, обладает правом экономии над своей физической целостностью. Для охраны здоровья лица его физическая неприкосновенность может быть ограничена(17, с.171).Например, в случае гангрены в ноге физическая неприкосновенность ограничивается и нога ампутируется, однако в итоге удается спасти жизнь. Но не следует забывать, что проведение научных исследований над умершим человеком, трансплантация органов также должна осуществляться на основе согласия, данного лицом при жизни в рамках закона.

Здоровье

Хотя и право на здоровье может исследоваться в рамках права на жизнь, здоровье лица выражает регулярное функционирование его физического органа и его врожденную естественную целостность, вследствие чего некоторые авторы, в отличие от целостности тела, расценивают здоровье как отдельная личностная ценность.И физическое, и душевное здоровье находятся под охраной личностных прав(13, с.63)

Имя и фамилия

Имя (фамилия) являсь одним из средств, позволяющих различать лицо от других, одновременно выражает принадлежность лица к семье и предоставляет ему возможность использования социальной позиции семьи, к которой он принадлежит.Нельзя забывать, что сокращенные имена, символические имена и адреса электронной почты также пользуются охраной имени.

Честь и достоинство

Честь и достоинство являются выражением суммы ценностей, которые даются лицу обществом.Это одновременно является объективной ценностью, выражающей доверие и уважение к лицу внутри общества.

По причине рождения лица человеком он пользуется доверием и уважением (достоинством) с рождения, одновременно он завоевывает доверие и уважение (честь) в связи со своим поведением внутри общества, умением и социальной позицией. Честь и достоинство для физических лиц так же важны, как и для юридических лиц.

Честь и достоинство, отражающие выделенный лицу обществом роль, могут меняться по месту и времени. По этой причине при оценивании наличия оскорбления чести и достоинства лица необходимо рассмотреть ситуацию, исходя из объективной ценностной оценки по месту и времени нападения и перспектив нормального лица.

Наиболее распространенной формой нападения на лицо является оскорбление его чести и достоинства, которые должны защищаться и уголовным законодательством, и частным правом. Поведение с целью унижения, ошибочного представления лица в смешном или неприглядном образе, осуществление против него враждебных действий относятся к случаям унижения чести и достоинства и наносят ущерб нравственным ценностям(18, с.237)

Изображение и голос

Под изображением понимается не только изображение, получаемое посредством фотоаппарата, а также изображение в фильме посредством видеозаписи или телевидении, изображение посредством кисти или карандашей, или отображение карикатуры. Получение изображения человека и его дальнейшее использование вопреки собственному желанию, использование изображения с приведением его в непригодное состояние и вопреки интересам лица противоречат личностным правам. Личностное право на изображение не означает, что никогда не может быть произведено изображение человека вопреки его желанию. В ходе мероприятия, или конкурса у политика, или спортсмена не получается разрешение на запись его изображения. И наоборот запись изображений другого лица в его доме, или на улице будет носить особенность вмешательства в частную жизнь. В ситуациях, основывающихся на согласии не может быть речи о противоправности.

Голос тоже считается одним из личностных прав. Запись голоса лица, распространение, изменение, уничтожение данной записи без его согласия противоречит личностным правам(16).

Частная жизнь

Понятие частная жизнь выражает сферу, охраняемую в связи с частной и семейной жизнью личности, уважением к его жилищу и телефонным разговорам, формированием личности, его действиями и решения-

ми, осуществляемыми втайне и независимо от других. Частная жизнь личности связана с его личностными качествами. Каждый день все более растет нарушение личной неприкосновенности с использованием против него наряду с традиционными способами (тайное проникновение в жилище, прослушивание, копирование и кража информации и т.д.), современных способов (мини-микрофоны, датчики, камеры с дистанционным управлением волновые передатчики и т.д.).

Общая жизненная среда

Каждый, живущий внутри общества имеет жизненную среду, складывающуюся из не скрываемого, разделяемого им по требованию общества с другими членами социума и проводимого перед ними поведения, за которым другие лица могут беспрепятственно следить. Данная жизненная среда, разделяемая лицом с иными лицами и реализуемая перед обществом не является скрытой. Если лицо говорит среди всех, то не может ставиться требование об охране тайны этого разговора. Возможность слежения всеми и явность события, даже в случае отсутствия видения со стороны других, достаточны для включения события в общую жизненную среду(21, с. 652).

Общая жизненная среда, как правило, не может воспользоваться правом на личную неприкосновенность. События, возникающие в данной среде и без того легко выслеживаются, разделяются другими лицами и само лицо не имеет никаких интересов для их скрытия. Выслеживание и обнаружение события в общей жизненной среде возможно при условии непротивоправности. А изложение событий в в общей жизненной среде с целью распространения сплетен и оскорбления, в унижающей честь и достоинство форме, употреблением неэтичных выражений признается противоправным. Данные о личной жизни людей, работающих в данной сфере входят в сферу личной неприкосновенности и вследствие этого вмешательство в указанные данные также признается противоправным. Однако лучше было бы дать событиям правовую оценку в соответствии с ходом событий. Можно разъяснить таким образом, что если распространение изображений манекенщицы, которая делает фотосъемки в пляжной одежде у моря не должно расцениваться как нарушение права на личную неприкосновенность, то скрытая съемка фотографий учителя или лица иной профессии в пляжной одежде у моря и их распространение должно расцениваться как нарушение права на личную неприкосновенность. Сведения о событиях в общей жизненной среде, особенно о деятельности людей политики, спорта и культуры не может расцениваться как вмешательство в частную жизнь. Если какое-либо лицо не жела-

ет, чтобы кто-либо кроме близких лиц, с которыми он говорит о своей частной жизни не знал этих данных, то указанные данные признаются принадлежащими этому лицу (12, s. 78)

Частная жизненная среда в узком смысле

Здесь речь идет о данных, не реализуемых в общей жизненной среде, разделяемых лишь с близкими к лицу людьми и открытых им, которыми никто кроме них не может воспользоваться. Близкие к лицу члены семьи, родственники, товарищи по работе составляют одну группу. События, реализующиеся в ее рамках не являются событиями, о которых знают, или должны знать все, а жизненными событиями, о которых может знать группа людей известного количества. Не входящие в скрытую жизненную среду лица семейные и профессиональные события также отражаются в данной среде. Приобретение, распространение и изучение указанных сведений третьими лицами считается вмешательством в частную жизнь. Часто возникают трудности при разграничении данной жизненной среды от иных жизненных сред. Распространение событий в частной жизненной среде в узком смысле лицами, с которыми данная жизненная среда разделяется, не признается противоправным. Однако выслеживание и изложение этих событий со стороны масс-медиа без согласия самого лица признается противоправным (11, s.63). К способам приобретения этих сведений вопреки воле лица можно отнести приобретение такими техническими средствами, как устройства звукозаписи, видеозаписи, прослушивание телефонов. Приобретение сведений подобным образом противоправно и является вмешательством в частную жизнь.

Скрытая жизненная среда

Закрытая жизненная среда, о которой лицо не желает наличия знаний у других людей, кроме его самого и доверенных лиц является скрытой жизненной средой. Лицо может поделиться событиями или тайнами своей скрытой жизненной среды только по своему желанию, в желаемых им формах, объемах и с желаемыми лицами. По этой причине вне разрешения и желания лица вмешательство в эту среду, ее исследование, изложение полученных сведений недопустимо. К скрытой жизненной среде относят: сведения со значением личной тайны, интимность семейной жизни, половой жизни и чувств, письма, переписка (электронная или бумажная), право на одиночество, необходимое для формирования творчества и личности лица частными данными (right to be let alone).

Разница событий в скрытой жизненной среде от событий в частной жизненной среде заключается в том, что пределы разделения с близкой средой лица и сообщения другим события в частной жизненной среде

в узком смысле известны и учитываются, а использование событий в скрытой жизненной среде доверяемыми лицом людьми в качестве подобной информации запрещается (15, с.150).Однако эти два предела часто невозможно отделить, так же невозможно отрицать, что они превращаются в отношения, меняющиеся от лица к лицу.

Дальнейшее технологическое развитие еще более усложняет эти отношения и их защита становится более уязвимой. Для вхождения события в состав понятия частной жизни и пользования защитой данного права каждое событие должно расцениваться в отдельности; результат должен достигаться с учетом жизни, профессии и социального положения лица, пределов вмешательства и особенностей события. Выражаясь в более простой форме, разделение лицом сведений о своей жизни, профессии, деятельности со своими близкими вовсе не должно расцениваться как открытость данных и согласие на их передачу иным лицам, их использование. Или хотя и лицо является публичным политиком, деятелем культуры, спортсменом, открытым для всех должна быть только его профессиональная деятельность, а частная жизнь всегда должна оставаться неприкосновенной. В противном случае это должно расцениваться как противоправная деятельность(8, 153)

В соседней Турции в судебном процессе, рассмотревшем выплату моральной компенсации за распространение разговора женатого артиста со своей возлюбленной в результате скрытой записи его телефонных разговоров суд вынес следующее решение: «Ввиду наличия тайны разговоров двух лиц, связанных с их частной жизнью, прослушивание телефонов лица и распространение записей прослушенных телефонных разговоров противоречит охране частной жизни и является нарушением целостности частной жизни лица, сохранение тайны которой необходимо. Если даже человек является известным в обществе лицом, тайна частной жизни не может быть раскрыта ни в какой форме. Телефонные разговоры никакого лица не могут прослушиваться без вступившего в законную силу постановления суда» (8, с.160).Подобные вмешательства в скрытую жизненную среду часто могут носить характер вмешательства в разговоры о семейной и частной жизни, честь и достоинство.

Запись, фиксация и распространение изображения и разговоров лица путем тайного, несанкционированного проникновения в его частную семейную среду может привести к вмешательству в частную жизнь. Переписка и разговоры являясь выражением лицом своих чувств и мыслей путем использования различных слов и отражением этих чувств посредством голоса может вылиться в произведение (например, признание в

любви стихами), отсутствие защиты со стороны авторских прав входит в составную часть подобной личной неприкосновенности и пользуется ее защитой.

Технические данные о регистрации, документах, счетах, деятельности и управлении предприятием в связи с внутренними делами предпринимателя, коммерсанта, профессионала, такие особенности, как производственное положение и взаимоотношения с клиентами составляют его профессиональную и коммерческую тайну.

Изучение коммерческих и профессиональных данных не является противоправным.Например:получение банками или кредитными организациями информации о деятельности предпринимателей, желающих получить кредит, приобретение сведений об их финансовом положении, платежоспособности, уровне доходов для выдачи им кредита соответствует требованиям права (19, с. 227)

Изучение и фиксация деятельности, связанной с семейной жизнью третьими лицами является противоправным. Распространение тайны семейной жизни в словесной, письменной форме и посредством прессы противозаконно, так же использование сведений, раскрывающих семейные тайны в доказательствах, представляемых правозащитником создает юридическую ответственность.

Неприкосновенность жилища, проникновение в жилище вопреки желанию лица, осуществление обыска, изъятие имеющихся там предметов связаны с неприкосновенностью по выслеживанию и фотографированию лица без его разрешения. Лицо, являющееся владельцем жилища обладает свободой регулирования своей жизни в желаемой форме и защиты от вмешательства иных лиц в нежелательной форме. В этом смысле проникновение других лиц в жилище в целях получения сведений о свободной деятельности лица внутри жилища и ее прослушивание, запись голоса и изображения, тайное выслеживание, осуществление обыска и изъятие предметов жилища являются поведением, нарушающим личную неприкосновенность.Статья 33 Конституции АР называется «Право на неприкосновенность жилища». В ст. 33.2 указано, что «Никто не вправе проникать в жилище против воли проживающих в нем лиц, иначе как в случаях, установленных законом, или на основании судебного решения» (1,с.24).

Одним из наиболее важных и нуждающихся в защите средств частной жизни является получение сведений и обеспечение конфиденциальности. Противоправное раскрытие данных, изложенных лицом в письме, их перехват с целью изучения написанного, уничтожение, рапростране-

ние без его ведома и желания признаются противоправным деянием. К сведениям, передаваемым через письмо наряду с традиционными письмами, отправляемыми почтой, также относятся сведения, передаваемые посредством таких средств, как электронное сообщение, факс, телеграф. Прослушивание телефонных разговоров лица без вступившего в законную силу постановления суда, сбор данных в целях приобретения доказательств и иных целях являясь абсолютно противоправным и признается вмешательством в частную жизнь. Глава 23 Уголовно-Процессуального Кодекса АР называется «Охрана конфиденциальности во время уголовного судопроизводства», эта глава в целом затрагивает вопросы охраны конфиденциальности сведений, составляющих личную и семейную тайну, государственной и коммерческой тайны в ходе уголовного судопроизводства в целом. Статья 199 УПК называется «Охрана личной и семейной тайны». В п. 3 данной статьи указано, что если органом, осуществляющим уголовный процесс, по соответствующему постановлению суда какому-либо лицу предложено сообщить или предоставить сведения, относящиеся к его личной жизни, это лицо имеет право быть уверенным в необходимости собирания таких сведений по возбужденному уголовному делу, а в противном случае отказаться от их дачи. Требуя от лица сообщения или предоставления сведений, относящихся к жизни самого этого лица или другого лица, со ссылкой на необходимость этого, орган, осуществляющий уголовный процесс, должен внести в протокол допроса или иного следственного действия подтверждающие записи о необходимости получения таких сведений. Доказательства, раскрывающие личные или семейные тайны, должны исследоваться в закрытом судебном заседании. Ущерб, причиненный какому-либо лицу нарушением неприкосновенности личной жизни, разглашением личной или семейной тайны, подлежит возмещению в порядке, предусмотренном законодательством Азербайджанской Республики. Как видно из содержания статьи, конфиденциальность сведений, относящихся к частной и семейной жизни в полной мере защищается правоохранительными органами государства (3,с.235)

Информационная технология и личностные права.

1. Понятие и сфера охвата информационной технологии.

Слово телекоммуникация возникло посредством добавления к слову “communication” (связь) префикса «теле» и означает «электронная связь». Под электронным понимается передача, отправление и получение любых знаков, символов, голосов, изображений и данных без проводов, через оптическую, электрическую, электрохимическую или иную систему.

Мы не ошибемся, если исходя из законодательного понятия будем утверждать, что независимо от места и формы возникновения, разработки или хранения темы телекоммуникационной деятельности, речь идет о достижении передачи, отправления и получения входящих, способных превратиться в любой вид голоса, знака, символа, изображения иных электронных сигналов. По мнению турецкого автора Экиджи, для расценивания функционирования какого-либо данного в качестве телекоммуникации важны характер данного и особенность системы передачи. Данные должны быть данными, передача которых возможна посредством знаков, голосов, символов, изображений, электронных, электромагнитных сигналов. Кроме того, подобные данные должны передаваться через провода, беспроводную, оптическую, электронную, электромагнитную, электрохимическую, электромеханическую или иную систему передачи. Исходя из понятия телекоммуникации и указанных особенностей услуг следует принимать, что телефон, телеграф, факс, кабельное телевизионное вещание, радиовещание и интернет входят в сферу охвата понятия телекоммуникации(9, s.117).

Сфера телекоммуникации и проблема неприкосновенности личностных прав

Сегодня в Азербайджане стремительно внедряются информационные технологии и предоставляемые ими возможности. Стремительное распространение пользования интернетом наглядно доказывает, что Азербайджан следит за пульсом современной эпохи. Многие люди пользуются интернетом для исследований, налаживания отношений, участия в социальных проектах, участия в экономической деятельности или просто для развлечения. Редко можно найти студента, у которого бы не была страница в фейсбуке. Для лица наличие мобильного телефона является важным условием, а его отсутствие расценивается окружением с удивлением. Электронная почта став более предпочтительной по сравнению с традиционной почтой, оставила ее далеко позади. Радиоволны стали неотъемлемой частью нашей жизни.

В Азербайджане следят за развитием технологий, новые технологические средства в скором времени становятся достоянием людей, однако это развитие также несет с собой большие проблемы. Наиболее серьезной проблемой является вопрос безопасности данных, распространяемых через социальные сети. Мы часто не задумываеися, что делимся глубоко личностными данными. Например, личные сведения, вводимые нами в социальную сеть фейсбук могут приравниваться к сведениям, приобретаемым правоохранительными органами в результате тщатель-

ного поиска. В фейсбуке и твиттере люди делятся практически каждой своей минутой, местами своего нахождения и людьми, с которыми они встречаются. А это больше всего облегчает работу правоохранительных органов. При этом фиксируются предложения, адресованные нам «для лучшего обслуживания», обеспечения безопасности в государственной и частной сфере, сведения в целях предотвращения преступности, сведения о состоянии нашего здоровья для установления точного диагноза, выбранные нами товары посредством карт купли-продажи, данные слежения за часами нашего посещения места работы, спортивных клубов, или прогулок и наши биометрические данные для установления наличия разрешения на вход. Наиболее задаваемым вопросом в связи с этим является: где, кем, хранятся, в каких целях на какие сроки используются, какие стадии проходят и кому выдаются эти данные, собираемые государством и частным сектором различными, все более развивающимися, рапространяющимися средствами. Ответ на этот вопрос заключается не только в степени обеспечения тайны частной жизни, являющейся конституционным правом, а в уровне защиты «личной свободы», являющейся неотъемлемой частью человеческого достоинства. Постоянное выслеживание считается первейшим препятствием на пути развития человека. Именнно в демократических государствах защита персональных данных на правовой плоскости также является шагом, предпринятым государством для решения указанной проблемы.

Осуществление первого правового регламентирования по данной теме в 1970-е гг. в Западной Европе не является случайностью ни по времени, ни по месту реализации. 1970-е гг. являются временем роста использования компьютеров и баз данных особенно со стороны государств для обработки сведений о гражданах. Существует горький опыт опасностей, к которым могут привести безграничная фиксация и координация персональных данных в недавнем прошлом государств Западной Европы во главе с Германией. Ни тогда, ни сейчас замедление технологического развития, предотвращение распространения полезных сведений не были признаны путем выхода. Эти цели должны обеспечиваться уполномоченными лицами, ответственными структурами (20, с.65, 17, с.447). Важно признание сохранения свзи лица с принадлежащими ему сведениями, выражаясь цитатой из известного постановления Конституционного Суда Германии, принятого в 1983 году, признание «права на определение будущего информации» (İnformationelle Selbstbestimmung).

Следя за правовыми текстами, развиваемыми в этих целях с 1970-х гг. до сегодняшнего дня необходимо отметить, что новые технологические

средства обуславливает внесение изменений и в указанные юридические тексты. Оспаривание пересмотра указанных норм в рамках ЕС в последнее время демонстрирует, что этот период еще не закончился (21, с.647)

Европейская Конвенция о защите прав человека и основных свобод как средство обеспечения права на неприкосновенность персоналных прав

Одну из основных ролей, пожалуй главную роль в правовом регулировании неприкосновенности персональных прав играет Европейская Конвенция о защите прав человека и основных свобод и являющийся средством обеспечения реализации указанной конвенции Европейский Суд по Правам Человека. Европейский Суд по Правам Человека расценил большую часть фундаментальных принципов защиты персональных данных в сфере охвата ст. 8 Конвенции. ЕСПЧ особенно с середины 1980-х гг. защиту персональных данных в растущей пропорции обеспечивает положениями Конвенции. Согласно Суду, право на определение будущего персональных данных входит в сферу охвата ст. 8./Тирер против Великобритании, 5856/72, 1978 31 his/. Суд также дал оценку учету социальных изменений при выполнении своих обязанностей /Джосси против Великобритании, 10843/84, 1990, 35 his/

Как видно из различных постановлений ЕСПЧ, основная цель заключается в действенной и выгодной защите прав, а не в их мифическом или теоретическом отстаивании. Это должно стать правилом, подлежащим соблюдению не толко со стороны ЕСПЧ, а со стороны всех государств.

Следует также отметить, что очень трудно дать понятие особенно «частной жизни».Эта трудность связана с неопределенностью границ частной сферы и государства. А это в конечном итоге требует индивидуального подхода к каждому случаю. При рассмотрении различных органов суда выясняется, что частная жизнь не должна ограничиваться интимной сферой лица, а также включать его отношения с другими. Данный подход дал значительные последствия с точки зрения защиты персональных данных: лицо и в случае прослушивания его рабочего или домашнего телефона, и в случае записи его деятельности в частной и государственном секторе без своего ведома для защиты может обратиться для защиты по ст. 8 Европейской Конвенции о защите прав человека и основных свобод. Суд придерживается одинакового подхода к нарушению индивидуальных прав путем использовании и традиционных средств, и новых технологий. В этом смысле слежение за электронной почтой лица, получение, передача и использование ее данных также формируют состав ст.8 (24, с.117).

ЕСПЧ свое первое важное постановление по данной проблеме вынесло в деле Класс и другие против Германии.Так, суд перечислил важные элементы, подпадающие в сферу охвата «частной жизни»: сбор и архивирование персональных данных индивидов со стороны официальных структур (Аманн против Швейцарии, b.n 27798/95, 2000;Ротару против Румынии, 28341\95, 2001), прослушивание телефонных разговоров (Малоне против Великобритании 8691\79, 1984; П.Г. и Ж.Х.Б. против Великобритании 44787\98, 2001), использование собранных данных для других целей (Линдер против Швейцарии, 9248\81, 1987), тайна данных о состоянии здоровья (З. против Финландии 22009\93, 1997; М.С. против Швеции1 20837\92, 1997), запись отпечатков пальцев и фотографий со стороны ПОО (Мюррей против Великобритании 14310\88, 1994) приобретение персональных данных (Гаскин против Великобритании 10454\83, 1989), хранение персональных данных больше положенного срока (С. и Марпер против Великобритании 30562\04, 30566\04, 2008)

Пределы права на уважение частной и семейной жизни, регулируемой ст. 8 Европейской Конвенции о защите прав человека и основных свобод закреплены во втором пункте данной статьи. Этот пункт устанавливает пределы судебного вмешательства в случаях нарушения требований положения об уважении частной жизни.Согласно указанному пункту, вмешательство в частную жизнь допускается в определенной степени лишь в случаях, когда такое вмешательство предусмотрено законом и необходимо в демократическом обществе. (25, s.372)

Конвенция СЕ «О защите физических лиц при автоматизированной обработке персональных данных», подписанная 28 января 1981 г. в городе Страсбурге была ратифицирована Азербайджанской Республикой 30 сентября 2009 г. с соответствующими оговорками, что в конечном итоге обусловило принятие 11 мая 2010 г. Закона АР «О персональных данных» (27).

Телекоммуникационный сектор и нарушение личностных прав

С приумножением к росту средств связи и их использования таких факторов, как технологическое развитие и рапространение использования компьютеров прогресс в телекоммуникационной сфере приобретает еще большее значение.Поэтому при использовании информационных и коммуникационных технологий в более действенной и распространенной форме в базе сектора и страны наряду с экономическими и глобальными доходами личностные права нуждаются в усиленной защите.

Связь наряду с обеспечением социальной, культурной и интеллектуальной коммуникации, тесно связана с персональными данными лица,

его частной жизнью и свободой обмена информацией. По этой причине везде, где существует связь, неизбежно речь идет о личностных правах. Случаи нарушения личностных прав в телекоммуникационной сфере могут совершаться и в открытой, и в скрытой форме третьими лицами.В статье случаи нарушения частной жизни исследованы с этих двух аспектов (7, с. 256).

1. Телекоммуникационный сектор и персональные данные.

Персональные данные являясь частью услуг в телекоммуникационном секторе, приобретают еще большее значение. Тема защиты персональных данных впервые была рассмотрена в 1980 году, в итоге были приняты следующие руководящие принципы:

- Ограниченность и обусловленность принципами сбора и использования персональных данных
- Принцип качества в персональных данных
- Принцип определенности цели при сборе и использовании персональных данных
- Принцип целесообразного использования
- Принцип принятия необходимых мер для защиты персональных данных
- Принцип открытости
- Принцип персонального участия в персональных данных
- Принцип обязательственности

Без правового регулирования смысла персональных данных, оснований их защиты, принципов, обеспечивающих такую защиту и исключений из нее, обязательств лиц, хранящих данные, прав индивидов, вера в безопаность указанных прав уменьшается. К сожалению, в правовой сфере сталкиваемся со следующей реальностью: многие наши персональные данные за пределами частной сферы не защищены. Вторая важная сфера проблемы проявляется в том, что ответственность перед угрозами, которые могут исходить от подобной беззащитности уменьшилась. Этот недостаток особенно связан с тем, что сами лица делятся персональными данными в социальных сетях независимо от существования такой необходимости. Можно привести такой пример: зачем для пользования скидками в магазине необходимо быть обладателем карты, в которой отражаются персональные данные?

Персональные данные раньше расценивались в рамках понятия частной жизни и Лиссабонским договором приобрели статус основного права(22). Ст. 32 Конституции АР называется «Право на личную неприкосновенность», как видно из статьи персональные данные могут

быть использованы лишь в случаях, допускаемых законом или с согласия лица. После изменений, внесенных на референдуме 2016 г. в ст. 32 Конституции были включены пп. 6, 7 и 8. Кроме того, следует отметить, что и на референдуме 2009 г. пп. 2 и 3 данной статьи были дополнены, а п. 5 был вынесен на референдум в качестве нового положения и включен в Конституцию.Согласно изменению, внесенному в Конституцию референдумом 2009 г., за исключением случаев, установленных законом, каждый может ознакомиться с собранными о нем сведениями. Каждый обладает правом потребовать исправления или изъятия (ликвидации) собранных о нем сведений, не соответствующих действительности, неполных, а также полученных с нарушением требований закона (1, с.23). Вместе с этим регулированием, были усовершенствованы нормативные правовые акты, приняты новые законы, направленные на защиту личностных прав. Основные правила защиты персональных данных регулируются законом.Нам представляется, что исходя из этого регулирования, следует принять, что персональные данные являются отдельной категорией права и отдельной ценностью в смысле личностного права.

Понятие персональных данных в «Директиве защиты данных» ЕС за номером 95/46 разъясняется как «любая информация, связанная с идентифицированным или идентифицируемым физическим лицом». Согласно ст. 2.1.1. Закона АР «О персональных данных» от 11 мая 2010 г. персональные данные - это любая информация, позволяющая прямо или косвенно определить лицо(26).

Имя, фамилия, возраст, пол, номер удостоверения личности, семейное положение, адрес, электронный адрес, голос, изображение, работы, доходы, виртуальные данные, задолженность, медицинские данные, генетический профиль, этническое и расовое происхождение, частная жизнь, данные о судимости, финансовые и налоговые данные, личные предпочтения и иные подобные данные могут рассматриваться в рамках понятия персональных данных(23).

Право на защиту персональных данных являясь конституционным правом, одновременно стало объектом УК АР. Так, ст. 155 УК АР закреплена под заглавием «Нарушение тайны переписки, телефонных переговоров, почтовых, телеграфных или иных сообщений», а ст. 156 – под заглавием «Нарушение неприкосновенности частной жизни». В 2017 г. санкции, предусмотренные за нарушение положений данной статьи еще более ужесточены (2, s.145)

2. Телекоммуникационный сектор и принцип скрытости.

В п. 6 ст. 5 - «Правовой режим и защита персональных данных» - Закона АР «О персональных данных» закреплено, что «В целях осуще-

ствления информационного обеспечения общества в сфере телекоммуникаций, почтовой связи, адресной и других сферах в информационные системы общего пользования могут вноситься с письменного согласия субъекта предоставленные им данные о себе (фамилия, имя, отчество, дата и место рождения, пол, гражданство, номер телефона и электронный адрес, место жительства и пребывания, специальность и место работы, вид осуществляемой деятельности, семейное положение, фотография и другие данные)». Ст. 1 Закона называется «Цель закона», в данной статье в качестве одной из основных целей указана «защита права на сохранение тайны личной и семейной жизни». Согласно этому принципу, за исключением случаев, допускаемых законами и правосудием, прослушивание, запись, хранение, изменение телекоммуникации противоречит закону(26).

В заключение следует отметить, что сегодня в период практического стирания понятия частная жизнь для защиты своей личности и персональных особенностей одним из самых эффективных средств является правовое регулирование, направленное на защиту персональных данных. А это правовое регулирование, направленное на защиту индивидуальных прав хотя и не способно обеспечить полноценную защиту перед стремительно развивающимся потоком технологии и ростом информации, но в определенной степени выступает единственным средством воздействия для предотвращения проблем. По этой причине в соответствии с требованиями времени существует серьезная потребность в дальнейшем усовершенствовании нормативных правовых актов в данной сфере.

1. *Конституция Азербайджанской Республики, издательство Закон, Баку 2018, 100 с.*
2. *Уголовный кодекс Азербайджанской Республики, Юридический дом издательство , Баку 2017, 755 с.*
3. *Уголовно-процессуальный кодекс Азербайджанской Республики, Юридический дом издательство, Баку, 2018, 789 с.*
4. *Алиев А.И. Международная защита прав человека: учебник. Баку, 2009, 490 с.*
5. *Аскеров З. Конституционное право. Учебник , Баку, 2011, 757 с.*
6. *Арпаджи Абдулкадир: личные права (реальные личности), (Стамбул, 2000 год), 167 с.*
7. *Экиджи Шерафетдин, Законодательство о турецком телекомуникации в частном секторе (Электронная связь), Издательство Ведат, Стамбул, 2006, 350 с.*

8. *Имре, Захит, «Вопросы, касающиеся защиты частной личности и неприкосновенности личных прав», том 39, S.1-4, 1974 с.147-168*
9. *Каплан Явуз, Закон, применимый к защите прав интеллектуальной собственности в Интернете. Анкара, 2004, 246 с.*
10. *Мустафа Дураль, Туфан Эгуз, Турецкое частное право Том II Личные права, издательский дом Филиз, Стамбул, 2017, 377 с.*
11. *Огуз Шимшек, Защита личных данных в конституционном праве, издательство Бета, Стамбул, 2008, 225 с.*
12. *Оздамир Хайрунниса, Защита персональных данных в области электронной связи в соответствии с условиями частного права. Анкара, 2009, 292 с.*
13. *Озтан, Билгя: Индивидуальные право, реальные личности, 9-е издание, Анкара, 2000. 188 с.*
14. *Сердар Илькнур, нарушение и правовая защита прав личности посредством радио и телевидения, Анкара, 1999 год. 428 с.*
15. *Сойсал Тамер, «Юридическая ответственность за вмешательство в права личности по электронной почте» Ассоциация адвокатов Анкары, выпуск 1, Анкара, 1965. с.144-167*
16. *Шен, Эрсан, Защита государством и обществом тайных, конфиденциальных личных прав. Юридический дом Казанджи, No: 48, Стамбул, 1996, http://sen.av.tr/en/index.html*
17. *Волкан Сырабащи, Нарушение интернетом и радиотелевизионным вещанием личных прав человека, Анкара, 2007, Печать 2, стр. 552 с.*
18. *Блинов А.М. Информационная безопасность: Учебное пособие. Ростов на Дону: Феникс, 2010. 324 с.*
19. *Петренко С.А., Курбатов В.А. Политики безопасности компании при работе в интернет, ДМК Пресс 2011, 396. С.*
20. *Banisar David, Freedomofinfo.Global Survey: Freedom of Information and Access to Government Record Laws Around the World.publisher freedominfo.org, 2004, 90 p.*
21. *Baxter, R.S. "Freedom of Information: Dispute Resolution Procedures", European Public Law, Volume: 2, Issue: 4, 1996, p.635-661.*
22. *European İntegration Working Group, "Civil Rights, Security and Consumer Protection in EU", http//library.Fes.de/pdf-files-id/ipa/06449. 7 p.*
23. *"Global Trends on The Right to Information: A Survey of South Asia", https://www.article19.org/data/files/pdfs/publications/south-asia-foi-survey.pdf 16.04.2018*

24. HINS, Wouter; Voorhoof, Dirk , Access to State-Held Information as a Fundamental Right under the European Convention on Human Rights. European Constitutional Law Review, 3 (1), T M C ASSER PRESS, 2007, p. 114–126.

25. Jack Beatson, QC and Yvonne Cripps, Freedom of expression and freedom of information : essays in honour of Sir David Williams. Oxford University Press, 2000, 421 p.

26. http://e-qanun.az/framework/19675

27. http://e-qanun.az/framework/18625

Алиев А.И., Ибрагимова А.Н., Ржаева Г.А. Информационная безопасность: проблема неприкосновенности личностных прав

Безопасность людей - это либо комфортная жизнь общества, либо способность защищаться от внутренних и внешних угроз. Каждому нужен закон, который обеспечит внутреннюю безопасность общества и общество, которое последует за ними. Однако, хотя безопасность является обязанностью государств, каждый член общества должен, в свою очередь, обязан выполнить свои обязательства. Сегодня правительства осуществляют управление с помощью информационных технологий, что ускоряет переход от традиционного к электронному правительству и формирует электронное правительство. Это изменение в управлении, наряду с повышением важности информации и информационных технологий, также подняло важный вопрос, такой как информационная безопасность. Информационная безопасность - это механизм защиты от несанкционированного доступа к информации, раскрытия, уничтожения, изменения или повреждения личной, профессиональной, коммерческой и государственной тайны. Нарушение информационной безопасности приведет к искажению, искоренению информации, ее целостности, целостности и конфиденциальности и, таким образом, к ослаблению управления. Информация должна быть полностью защищена, независимо от ее формы, целостности и конфиденциальности. , информационная безопасность является важным критерием защиты как частной, так и общественной безопасности и защиты любых угроз, с которыми они могут столкнуться. Самым чувствительным моментом в обеспечении информационной безопасности является человек. Таким образом, человеческий фактор играет решающую роль в обеспечении информационной безопасности. Люди должны быть проинформированы о безопасности, чтобы обеспечить государство, организацию, в которой оно работает, и безопасность личной информации. В этой связи в статье рассматривается проблема информационной безопасности, неприкосновенность личных прав, личных прав, личных данных и их неприкосновенность.

Ключевые слова: информационная безопасность, личные права, права личности, классификация личных прав, узкое понятие личной жизни, более широкое понятие личной жизни, проблема информационных технологий в отношении личных прав

A.I.Aliyev, A.N.Ibrahimova, G.A.Rzayeva. Information security: the problem of inviolability personal rights

For people, the security of individuals is either a comfortable life of the society, an ability to defend against internal and external threats. Everyone needs a law that will ensure the inner security of the society, and the society that will follow them. However, although security is the duty of the states, each member of society should, in turn, be required to do so and to fulfill their commitments. Today, governments are implementing management with the help of information technology, which accelerates transition from traditional to e-government and forms e-government. This change in management, along with increasing the importance of information and information technology, has also raised an important issue, such as information security. Information security is a protection mechanism against unauthorized access to information, the disclosure, destruction, alteration, or damage of personal, professional, commercial, and state secrets. Infringement of information security will cause distortion, eradication of information, its integrity, integrity and privacy, and thus weakening of management. Information should be protected in its entirety regardless of its form, integrity and confidentiality. Information security is an important criterion for the protection of both private and public security, and the protection of any threats they may face. The most sensitive point in ensuring information security is human. Thus, the human factor plays a crucial role in providing information security. People should be informed about this subject in order to ensure the state, the organization operates personal information security. In this regard, the article examines the problem of information security, the inviolability of personal rights, personal data, and their inviolability.

Key words: information security, personal rights, individual rights, classification of personal rights, narrow concept of personal life, broader concept of private life, the problem of information technology in relation to personal rights, information technology problem of personal rights

Бабенко А.М.

доктор юридичних наук, доцент, завідувач кафедри теорії та історії держави і права Одеського державного університету внутрішніх справ

Babenko A.M.

Doctor of Law, Associate Professor, Head of the Department of Theory and History of State and Law of Odessa State University of Internal Affairs

КРИМІНОЛОГІЧНА ОЦІНКА РИЗИКІВ І ЗАГРОЗ У КОНТЕКСТІ ЗАХИСТУ КРИТИЧНОЇ ІНФРАСТРУКТУРИ В УКРАЇНІ (РЕГІОНАЛЬНИЙ АСПЕКТ)

Об'єктами критичної інфраструктури традиційно вважаються підприємства та установи таких галузей народного господарства, як енергетика, хімічна, продовольча промисловість, транспорт, банки та фінанси, енергетика, у тому числі й атомна, газо-, нефтепроводи, інформаційні технології та телекомунікації (електронні комунікації), охорона здоров'я, комунальне господарство та ін. Перелічені галузі народного господарства є стратегічно важливими для функціонування як економіки, так і безпеки держави, суспільства та населення в цілому, оскільки виведення з ладу або руйнування об'єктів цих галузей можуть мати вельми негативні наслідки для національної безпеки та обороноздатності держави, природного середовища, призводячи до значних матеріальних та фінансових збитків, людських жертв, погіршення іміджу Української держави на міжнародній арені тощо.

Під «ризиком» слід розуміти наявність небезпек та загроз, ймовірність настання будь-якої шкоди для населення держави в цілому та окремих її регіонів. Оцінка ризиків захисту критичної інфраструктури нами розглядається як дієвий механізм аналізу стану убезпечення території України від кримінологічних загроз. У кримінології, як у математиці та в економіці під час аналізу тих чи інших видів загроз увага завжди привертається до визначення статистичних ризиків, що засноване на статистичних даних, наукових, технічних та експертних оцінках. Саме такого підходу ми будемо дотримуватися під час побудови схеми та викладення основних результатів нашого дослідження.

У представленому дослідженні спростуємо або підтвердимо гіпотезу щодо наявності чи відсутності для України ризиків ядерної або техногенної катастрофи, пов'язаної з існуванням об'єктів атомної енергетики,

газотранспортної системи, та наявними у тих чи інших регіонах країни окремими видами злочинності, включаючи й тероризм.

Нагадаємо, що перший в світі атомний реактор був побудований у 1942 р. у США. Роботи щодо його створення проводилися під керівництвом італійського фізика Е. Фермі. В Європі першим ядерним реактором стала установка Ф-1. Її запуск відбувся 25 грудня 1946 р. у Москві під керівництвом академіка В. Курчатова. Українську атомну енергетику започатковано у 1977 р., коли у промислову експлуатацію було введено перший енергоблок Чорнобильської АЕС із реактором РБМК-1 000 (1 000 МВт). Зараз атомна енергетика функціонує у 30 країнах світу. Всього працює 440 ядерних реакторів, з яких: 104 знаходяться у США, 59 – у Франції, 54 – в Японії, 31 – у РФ, 19 – у ФРН. Україна має 15 діючих ядерних реакторів і посідає 10-те місце у світі за їх кількістю.

В основному перелічена атомна енергетика має мирний характер, але світу відомі випадки застосування атому у військових цілях, що призвело до масштабних катастроф із чисельними жертвами та руйнуваннями. Так, наприкінці Другої світової війни 9 серпня 1945 р. збройні сили США здійснили ядерні атаки на японські міста Хіросіму і Нагасакі. Від вибухів миттєво загинуло понад 70 тис. мешканців Хіросіми та 60 тис. мешканців Нагасакі. Із серпня по грудень 1945 р. загальна кількість тих, які померли від ран і хвороб, спричинених радіацією, склала близько півмільйона осіб в обох містах. Соціально-економічні наслідки й досі не підраховані.

Ще одним прикладом виявилася сумно звісна Чорнобильська катастрофа. Уніч на 26 квітня 1986 р. відбулася найвідоміша у світі техногенна катастрофа внаслідок вибухів і руйнування четвертого енергоблоку Чорнобильської атомної електростанції. Відбувся радіоактивний викид потужністю 300 умовних Хіросім. Загальна сума прямих збитків унаслідок зазначеної аварії у 1986-1989 рр. становила 12,6 млрд доларів США, із них: утрати матеріально-технічних комплексів – на суму 1,4 млрд доларів США; непрямі збитки від невикористання сільськогосподарських угідь, водних і лісових ресурсів, об'єктів промисловості та введення нових потужностей – на суму 160 млрд доларів США.

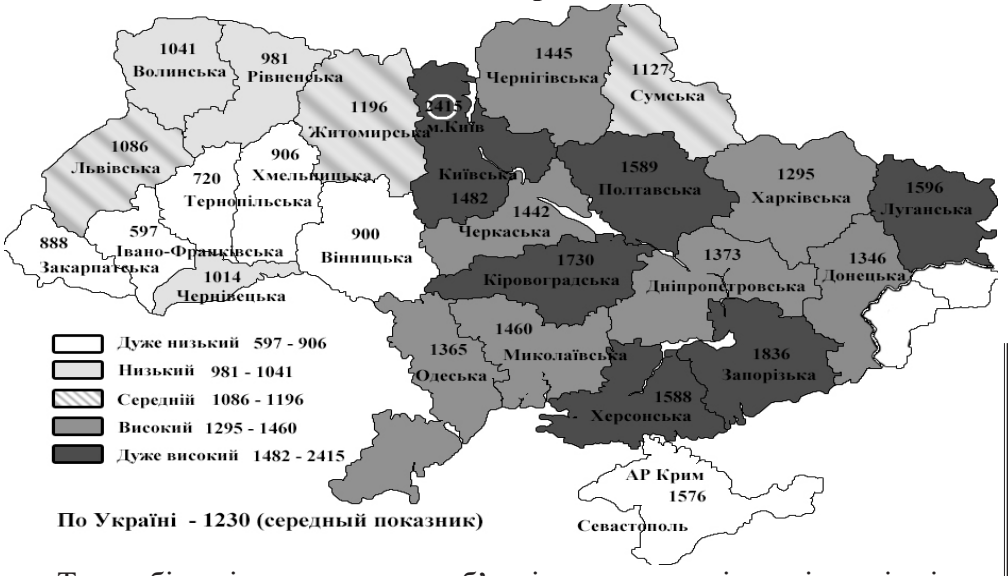
На сьогодні енергетичні потреби України забезпечує розвинута структура об'єктів відповідної сфери. Серед найвідоміших із них: 1) розгалужена система газотранспортної системи, що простирається від східних до західних та від північних до південних кордонів України; 2) чотири діючі атомні електростанції. Газотранспортна система України включає 36 тис. км магістральних газопроводів різного призначення і продуктивності, 71 компресорну станцію (122 компресорних цехи), понад 1 600 газорозподільних станцій, 12 підземних сховищ газу з найбільшим в Європі, після РФ, активним обсягом газу – понад 32 млрд м3, або 21,3 % від загальноєвропейської активної ємності. На «вході» ГТС спроможна

прийняти до 290 млрд м3, а на «виході» передати 175 млрд м3. Потужність атомних електростанцій України є такою: Південноукраїнська АЕС – 3 000 МВт; Хмельницька АЕС – 2 000 МВт; Рівненська АЕС – 2 880 МВт; Запорізької АЕС – 6 000 МВт; Чорнобильської АЕС до катастрофи складала 3 200 МВт.

Аналіз географії розташування об'єктів критичної інфраструктури підвищеної небезпечності (атомних електростанцій та об'єктів і потужностей газотранспортної системи) свідчить про їх розташування у зонах підвищеної кримінологічної загрози (Карта 1).

Карта 1

Географія інтенсивності злочинності в Україні на 100 тис. населення за 2017 рік



Також більшість зазначених об'єктів розташовані у регіонах із підвищеним рівнем терористичної загрози, соціальної напруженості, високим рівнем убивств та самогубств (Карта 2, 3,4).

Що стосується злочинів, пов'язаних із терористичними актами, то якщо у 2013 р. було обліковано всього 4 факти, то починаючи з 2014 р. їх стабільно вчиняється понад 1 тис. (Табл.1). Найбільш небезпечними у цьому сенсі виявилися території Донецької, Луганської, Одеської, Київської та Запорізької області. Нагадаємо, що саме на цих територіях розташовані атомні електростанції і більшість об'єктів газотранспортної системи та її мереж. Враховуючи потужність атомних електростанцій та географію розміщення об'єктів газотранспортної мережі, навіть одного випадку тероризму, вчиненого у Рівненській або Хмельницькій області, може вистачити для масштабної катастрофи (Карта 2)

Карта 2. Географія терористичних актів та створення терористичних груп чи організацій за 2016-2017 роки

Табл.1. Динаміка терористичних актів (ст.258 КК України), вчинених в Україні за 2009-2017 роки

Роки	2009	2010	2011	2012	2013	2014	2015	2016	2017
К-сть	-	-	-	-	4	1 499	1 295	1 865	1 385

Реальність кримінологічних загроз для об'єктів критичної інфраструктури в нашій країні може підсилюватися катастрофічним знеціненням як власного життя, так й життя стосовно іншої людини. На це яскраво вказує висока інтенсивність убивств та самогубств у регіонах України (Карта 3, 4).

Карта 3.Географія інтенсивності вбивств в Україні на 100 тис. населення за 2017 рік

Із представлених даних випливає, що найбільш небезпечними для життя територіями України є місто Київ (31) та Київська область (18,8), а також Луганська (30,7), Донецька (29,5), Миколаївська (17,2), Одеська (12,9), Запорізька (12,9) та низка інших областей України (Карта 3,4). Інтенсивність вбивств і самогубств на 100 тис. населення у кілька разів перевищують епідеміологічний поріг, що дорівнюється 10 випадків на 100 тис. населення.

Карта 4. Географія інтенсивності самогубств в Україні на 100 тис. населення за 2017 рік

Представлені результати свідчать про надзвичайно високу насиченість територій розміщення об'єктів критичної інфраструктури не лише загальною злочинністю, а й злочинами терористичної спрямованості, вбивствами та самогубствами (Карта 1, 2, 3, 4; Табл. 2). На карті 3 та 4 представлені дані, на яких видно, що більша частина нашої країни знаходиться у небезпечній для проживання зоні. Буде дуже прикро, якщо колись мирна і квітуча країна перетвориться на отруєну територію, на якій є неможливим подальше проживання; отримає статусу території, де панують вбивці та самогубці.

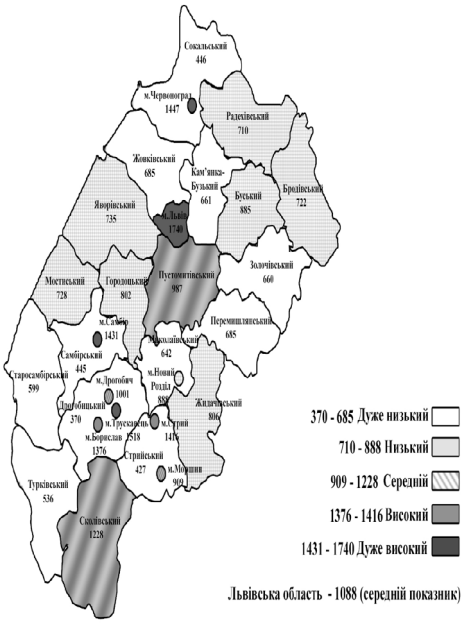
У розрізі населених пунктів окремих регіонів нами встановлено більш детальну картину криміногенної напруженості та насиченості злочинністю.

У таблиці 2 наведені узагальнені дані, які свідчать про окремі негативні параметри певних регіонів, що можуть виявитися факторами підвищення рівня кримінологічних загроз. Невтішною з точки зору загроз для критичної інфраструктури України виявилася й статистика окремих видів злочинності. Так, в Україні щорічно вчиняється близько 30

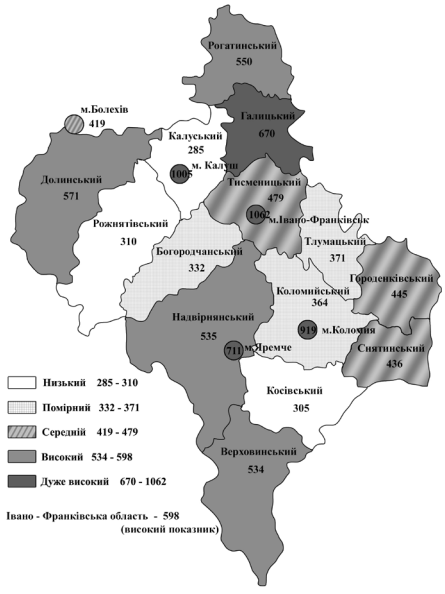
злочинів, пов'язаних із порушенням вимог режиму радіаційної безпеки (ст. 2671 КК України). Стабільно високим виявився рівень пошкоджень об'єктів магістральних або промислових нафто-, газо-, конденсатопроводів та нафтопродуктопроводів (ст. 292 КК України) – близько 200 злочинів на рік. Реальність кримінологічних загроз зазначеним об'єктам може бути пов'язана з високою мілітаризацією українських регіонів. Щороку тут фіксується близько 8 тис. злочинів, пов'язаних із незаконним поводженням зі зброєю, бойовими припасами або вибуховими речовинами (ст. 263 КК України) (Табл. 3), що не виключає її застосування у випадках підвищення рівня соціальної напруженості в Україні.

Карта 5. Географія кримінологічних загроз у розрізі окремих регіонів України

Інтенсивність злочинності у Львівській обл.

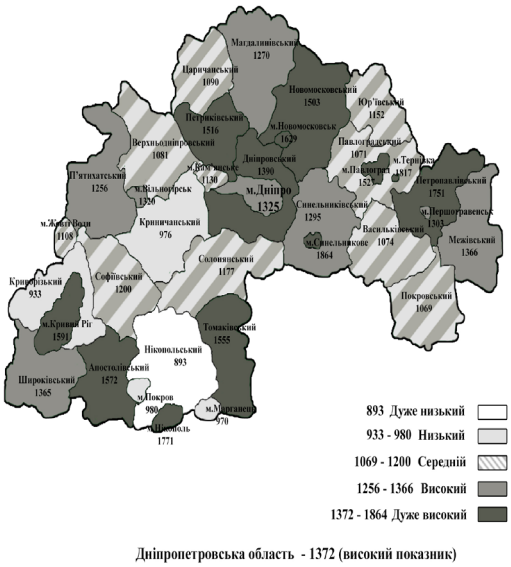


Інтенсивність злочинності у Івано-Франківській обл.



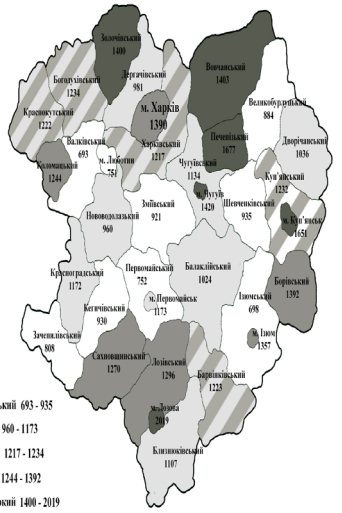
Карта 6. Географія кримінологічних загроз у розрізі окремих регіонів України

Інтенсивність злочинності у Дніпропетровській обл.



Дніпропетровська область - 1372 (високий показник)

Інтенсивність злочинності у Харківській обл.



Харківська область - 1298 (високий показник)

Низький 960 - 1173
Середній 1217 - 1234
Високий 1244 - 1392
Дуже високий 1400 - 2019

Табл.2. Регіональні особливості кримінологічної небезпеки в Україні

Україна	Київ	Дніпро	Одеса	Харків	Львів
Населення	2 933 537	993 212	1 010 986	1 450 334	757 955
К-сть злочинів	70 662	13 290	16 243	20 166	13 190
Рівень злочинності	2 408	1 338	1 606	1 390	1 086
Вбивства	925 (327)	182 (367)	124 (304)	96 (335)	33 (196)
Самовбивства	167	668	445	215	126

Табл. 3. Динаміка окремих злочинів, які можуть являти реальну загрозу для об'єктів критичної інфраструктури України

Рік/Параметри	2014	2015	2016	2017
ст. 267-1 КК	45	38	22	30
ст. 292 КК	331	245	264	164
ст. 263 КК	7 228	7 409	6 307	8 002

Підсумовуючи вищевикладене, зазначимо, що атомні електростанції та газотранспортна система є двома найважливішими видами об'єктів критичної інфраструктури України, оскільки вони: по-перше, є джерелами енергії для внутрішнього споживання; по-друге, забезпечують експорт електроенергії та відповідно прибутки країни; по-третє, є гарантами соціально-економічної та політичної стабільності у регіоні. До тих пір, доки вони функціонуватимуть у повному обсязі та в штатному режимі, в Україні не можливе проведення крупномасштабних операцій військового характеру. Припинення роботи зазначених об'єктів може призвести не лише до економічного та соціального, а й до політичного дисбалансу, що здатне викликати негативні геополітичні наслідки. Стабільному функціонуванню АЕС та ГТС України, а, отже, й геополітичній стабільності в Україні з високим ступенем можуть перешкоджати такі кримінологічні загрози, як-от:1) висока інтенсивність злочинності в окремих регіонах; 2) злочини терористичного характеру; 3) великий обсяг незаконного обігу зброї у місцевого населення; 4) високий рівень схильності окремих категорій населення до насильства; 5) негативний стан соціальної та соціально-психологічної обстановки (високий рівень самогубств, безробіття, соціальної напруженість тощо); 6) чинники геополітичного характеру.

Саме на ці обставини необхідно звертати увагу правоохоронним органам під час визначення ризиків та профілактики кримінологічних загроз для стабільного функціонування об'єктів критичної інфраструктури.

Бабенко А.М. Кримінологічна оцінка ризиків і загроз у контексті захисту критичної інфраструктури в Україні (регіональний аспект)

У статті визначено, що об'єктами критичної інфраструктури традиційно вважаються підприємства та установи таких галузей народного господарства, як енергетика, хімічна, продовольча промисловість, транспорт, банки та фінанси, енергетика, у тому числі й атомна, газо-, нафтопроводи, інформаційні технології та телекомунікації (електронні комунікації), охорона здоров'я, комунальне господарство та ін.

Геополітичній стабільності в Україні з високим ступенем можуть перешкоджати такі кримінологічні загрози, як-от:1) висока інтенсивність злочинності в окремих регіонах; 2) злочини терористичного характеру; 3) великий обсяг незаконного обігу зброї у місцевого населення; 4) високий рівень схильності окремих категорій населення до насильства; 5) негативний стан соціальної та соціально-психологічної обстановки (високий рівень самогубств, безробіття, соціальної напруженість тощо); 6) чинники геополітичного характеру.

Ключові слова: кримінологічні ризики і загрози, кримінологічна оцінка, критична інфраструктура, захист критичної інфраструктури

Babenko A.M. Criminological Assessment Of Risks And Threats In The Context Of Protection Of Critical Infrastructure In Ukraine (Regional Aspects)

The article states that objects of critical infrastructure are traditionally considered enterprises and institutions of such sectors of the national economy as energy, chemical, food industry, transport, banks and finance, power engineering, including nuclear, gas, oil pipelines, information technologies and telecommunications (electronic communications), health care, utilities, etc.

Geopolitical stability in Ukraine with a high degree can hinder such criminological threats, such as: 1) high crime intensity in selected regions; 2) crimes of a terrorist nature; 3) the large volume of illicit trafficking of weapons from the local population; 4) high level of inclination of certain categories of population to violence; 5) negative state of social and socio-psychological situation (high suicide rate, unemployment, social tension, etc.); 6) factors of geopolitical character.

Keywords: criminological risks and threats, criminological assessment, critical infrastructure, protection of critical infrastructure

Батиргареєва В.С.
доктор юридичних наук, старший науковий співробітник, заступник директора з наукової роботи Науково-дослідного інституту вивчення проблем злочинності імені академіка В.В. Сташиса НАПрН України

Batyrgareeva V.S.
Doctor of Law, Senior Researcher, Deputy Director for Scientific Work of the Research Institute for the Study of Crime Problems named after Academician V.V.Stashys NALS of Ukraine

НОВИЙ ВИД ЗЛОЧИННОСТІ У СФЕРІ МОРАЛЬНОСТІ, ПОВ'ЯЗАНИЙ ІЗ ВИКОРИСТАННЯМ ІНФОРМАЦІЙНО-ТЕЛЕКОМУНІКАЦІЙНИХ СИСТЕМ ЯК ОБ'ЄКТІВ КРИТИЧНОЇ ІНФОРМАЦІЙНОЇ ІНФРАСТРУКТУРИ

У постанові Кабінету Міністрів України «Про затвердження Порядку формування переліку інформаційно-телекомунікаційних систем об'єктів критичної інфраструктури держави» від 23 серпня 2016 р. № 563 зазначається, що Перелік інформаційно-телекомунікаційних систем об'єктів критичної інфраструктури держави затверджується Кабінетом Міністрів України. Затвердження такого Переліку, безумовно, виявлятиметься вагомим кроком у напрямі підвищення рівня захисту інформації, що обробляється в інформаційно-телекомунікаційних системах об'єктів критичної інфраструктури, покликаних забезпечити стабільне функціонування найважливіших для економіки держави, суспільства та безпеки населення підприємств і установ. Метою включення певних інформаційно-телекомунікаційних систем об'єктів критичної інфраструктури держави до побідного Переліку є їх захист від кібератак. До речі, кібератака, промислові аварії, пандемії, стихійні лиха визначаються як загрози критичній інфраструктурі соціуму як такій. Разом із тим до загроз відносять й терористичну та злочинну діяльності [1].

На сьогоднішній день Переліку інформаційно-телекомунікаційних систем об'єктів критичної інфраструктури не затверджено, хоча не можна не відмітити, що кіберпростір є середовищем здійснення потенційно

небезпечних дій проти держави, суспільства чи особи, в тому числі й злочинних. Слід вказати, що у плані de lege ferenda законодавцю при визначенні такого переліку акцент окремо треба робити на визнанні об'єктом критичної інфраструктури суспільства й самого кіберпростору як специфічного, окремого (як водний, повітряний, космічний тощо) виду простору, що охоплює не лише суто інформаційну інфраструктуру, а й певну частину самого інформаційного простору (інформації, що циркулює в ньому) [2, с.11]. Наприклад, у сучасному офіційному безпековому дискурсі США (Air Force Cyber Command Strategic Vision (2008); National Security Strategy USA (2010)) кіберпростір розглядається саме як «фізичний» простір [3, с.69].

Моральний стан суспільства, і, як з'ясувалося, не лише українського, сьогодні потерпає від протиправних дій, що вчиняються з використанням кіберпростору як уявного середовища, в якому за допомогою комп'ютерних мереж циркулює цифрова інформація [4, с.121]. Сьогодні в Україні в повному обсязі присутні всі ключові «класичні» кіберзлочини (шахрайство, здирництво, несанкціонований доступ до персональної інформації користувачів та автоматизованих баз даних, поширення порнографії, продаж зброї чи наркотиків тощо), і щороку їх кількість лише зростає [3, с.210].

Якщо виходити із розуміння кіберзагрози як намірів, дій або явищ, що створюють небезпеку інтересам людини, суспільства та держави шляхом інформаційного впливу на соціальні об'єкти, інформаційну інфраструктуру та інформаційні ресурси в кібернетичному просторі [4, с.191], то попутно мішенню подібних загроз може виявлятися й виявляється свідомість людини як соціальний об'єкт. Тому недаремно до основних загроз життєво важливим інтересам людини, суспільства, держави, які реалізуються за допомогою інформаційних, телекомунікаційних та інформаційно-телекомунікаційних систем, сьогодні відносять зростаючі масштаби поширення кіберзлочинності як такої та негативні інформаційно-психологічні впливи на суспільну свідомість і маніпулювання нею з кіберпростору [5, с.351].

Майже одразу з появою комп'ютерних технологій з'явилися особи, які почали використовувати ЕОМ із протиправною метою; і якщо раніше це були люди, що мали досить великий обсяг знань та досвід у сфері високих технологій, то зараз є непоодинокими випадки, коли комп'ютерну техніку з протиправною метою використовують пересічні громадяни, що мають лише базові навички роботи з нею [6, с.215].

Останніми роками на території України набирає обертів так званий вебкам-моделінг. Це така сфера Інтернет-бізнесу, що побудована на спіл-

куванні веб-моделі і чоловіка-спостерігача в онлайн відео-чаті, на оплатній основі, за яке чоловіки автоматично сплачують гроші.

Подібне явище виникло у 1999 р., коли деякі моделі засвоїли можливості інтернет-простору і стали показувати приватні шоу через вебкамеру. У ті роки тільки починалося знайомство с порталами всесвітньої павутини, тому можливість поспілкуватися з привабливою моделлю вічна-віч зацікавила багатьох. У приватному чат-руме (від англ. chartroom – болтати, бесідувати в чаті) спілкування відбувалося лише з одним користувачем, який сплачував щохвилинний тариф [7]. Чим довше у такий спосіб чоловіки спілкуються з вебкам-моделями, тим більше останні отримують грошей, оскільки заробіток вебкам-моделі залежить від часу проведеного з чоловіком в Інтернеті. Є дані, що сьогодні вебкам-моделінгом займаються у світі 5,7 млн. жінок, у РФ ця цифра складає майже 533 тис. жінок [8]. Стосовно України таких відомостей отримати не вдалося, але відомо, що «ініціатива» подібного способу заробітка перехоплена з російського інтернет-простору. За «спілкування» деякі сайти пропонують від 2 до 5 тис. доларів щомісячно.

Насправді вебкам-бізнес – це інтернет-проституція, одна з галузей підпільної порноіндустрії. На сайті «modelwebcam.ru», що займаються вербовкою таких моделей, можемо прочитати (мовою оригіналу): «Основная суть работы веб-модели видео-чат с мужчинами, желающими общаться с привлекательными девушками через интернет в режиме реального времени. Такое занятие не имеет никаких сложностей – вы флиртуете с посетителем из вашей персональной комнаты посредством вебкамеры и получаете за это серьезные деньги. Личную комнату можно зарегистрировать на специализированном вебкам-ресурсе. Время для интернет-общения каждая веб-модель выбирает самостоятельно в зависимости от своего желания и настроения. Необходимо рационально составить график работы, подходящий именно вам, и следовать ему неукоснительно. Чем больше времени вы посвящаете вебкам-бизнесу – тем выше ваш доход». Здавалося б, нічого в принципі протиправного у такому спілкуванні немає, але до тих пір, поки таке спілкування не матиме характеру інтимного. Так, у гонитві за легкою прибутком веб-моделі часто погоджуються на демонстрацію в процесі такого спілкування інтимних частин свого тіла; при цьому у чоловіків зараз є технічна можливість записувати результати такого спілкування, роблячи відеозапис, про який жінки навіть не підозрюють [9].

Сьогодні галузь вебкам-бізнесу дуже розвинена: є свої схеми, правила, сленг і навіть наукові посібники про те, як поводити себе з «мемами»

(так вебкам-моделі називають своїх клієнтів), як просуватися вперед і збільшувати свої доходи [10]. Ресурси Інтернету просто перевантажені інформацією про набір моделей до вебкам-судій. Соцмережі спрощують пошук такої роботи і жінок, готових займатися подібної діяльністю. Наведу одну об'яву (мовою оригіналу): «Вакансия: Модель. Компания: Like Studio. Город Харьков. Зарплата 25 тыс. грн. Описание вакансии: В студию премиум сегмента срочно требуется модель. Высокая своевременная зарплата, гибкий график, работа на европейский рынок. Подробности Viber, WhatsApp, Telegram +38073427XXXX».

На теперішній час механізм організації такого бізнесу відпрацьований до дрібниць. Щоб почати працювати вебкам-моделлю, потрібно зареєструватися на спеціальному сайті (сервісі), який саме на цьому спеціалізується. Кожен сайт має свою територіальну аудиторію. Так, Україна «спеціалізується» на країнах Західної Європи та країнах Північноамериканського континенту. Доступ на відповідні сайти з України закрито, щоб виключити можливість упізнати вемкаб-моделі своїми знайомими, друзями, родичами.

Працювати вебкам-моделлю можна двома шляхами. Перший шлях – це працювати на веб-студію. У такому разі питання реєстрації на відповідному сайті, заповнення всієї необхідної інформації, просування моделі в цьому бізнесі, необхідне технічне оснащення, геофільтрації та захисту від запису відеоролика вирішують організатори студії. Це більш простий спосіб, адже і заробітки тут будуть менше, оскільки веб-студії отримують великі відсотки від зароблених вебкам-моделями грошей. Другий шлях – самостійна реєстрація на сайті, придбання відповідного обладнання для інтернет-трансляції, вирішення питань переведення грошей за «сеанси» спілкування з іноземцями на банківські рахунки – є складнішим, але закономірно потенційні заробітки тут більше. До того ж, щоб бути «успішною» вебкам-моделлю, потрібно до цього ще хоча б трохи володіти іноземною мовою, а ще краще кількома (хоча моделям і кажуть, що це не обов'язково), основами психології та деталями успішного самомаркетингу [11].

До речі, щоб пройти реєстрацію на подібному сайті, потрібно вказати не лише достовірні особисті дані, а й надати якісний скан паспорта з фотознімком. Тільки після цього можна отримати власний аккаунт на сайті.

Гроші, що перераховуються на сайт-платформу за спілкування з вебкам-моделями, переводяться через платіжну систему безпосередньо моделі або організаторам веб-студії. Частина із цих грошей в останньому випадку виплачується моделям, а гроші, що залишаються після цього,

витрачаються на підтримку функціонування студії, оплату послуг Інтернет-провайдера, орендної плати за приміщення тощо.

Вебкам-студії розраховані на залучення до відеочатів якомога більшої кількості клієнтів. Тому їх діяльність не обмежується лише налагодженням спілкування вебкам-моделей зі спостерігачами, «легкою» еротикою і так званим стріпом. Нерідко такі студії сприяють виготовленню продукції порнографічного характеру. Тут можна, здавалося б, заперечити, що відеозапис подібних дій на матеріальні носії нібито не здійснюється, щоб йшлося про виготовлення, поширення і т. ін. порнографічної продукції, але ж за Законом України «Про захист суспільної моралі» виробництво та обіг у будь-якій формі продукції порнографічного характеру в Україні забороняються. А згідно зі ст. 1 цього ж самого Закону до продукції такого характеру належить й продукція електронних засобів масової інформації, змістом яких є детальне зображення анатомічних чи фізіологічних деталей сексуальних дій чи які містять інформацію порнографічного характеру [12]. Таким чином, у даному разі відеопродукція порнографічного характеру виготовляється в Україні в режимі реального часу і поширюється в мережі Інтернету. Саме такого підходу дотримується принаймні в Україні слідчо-судова практика. За українським кримінальним законодавством особи, які вербують жінок до вебкам-студій, укладають відповідні угоди із сайтами, орендують приміщення, набувають необхідну для відеотрансляції апаратуру тощо, притягуються до відповідальності за статтями 301 («Ввезення, виготовлення, збут і поширення порнографічних предметів») та 302 («Створення або утримання місць розпусти і звідництво») КК України, хоча щодо ставлення у провину ще й створення місць розпусти практика не є одноманітною. За ст. 301 КК притягуються до відповідальності й вібкам-моделі, якщо буде доведено, що при виконанні побажань клієнтів за грошову винагороду вони поширювали через Інтернет порнографію. Із цього випливає, що зайняття вебкам-моделінгом не таке вже безневинне зайняття, яке за певних обставин може викликати для жінок серйозні правові наслідки. Тому недаремно зараз з'явилася армія адвокатів, які спеціалізуються на доведенні того, що під час такої діяльності має місце лише еротика, а не поширення порнографії. Але ж, по-перше, дати оцінку, чи є будь-які матеріали порнографічними або ні, можуть лише експерти комісії з питань суспільної моралі. А по-друге, за законом будь-яке детальне зображення статевого органу – все вважається порнографією, навіть й тоді, коли статевого акту не відбувається.

У свою чергу, інтернет-платформи, на яких зареєстровані вебкам-студії, що потім залучають жінок до подібної діяльності, або на яких за-

реєстровані моделі, якщо вони реєструються самостійно, розміщені на серверних платформах іноземних держав, таких, як, наприклад, США, Нідерланди, Данія, Португалія, в яких немає кримінальної відповідальності за поширення порнопродукції. Проте зустрічаються й сервісні платформи, дислокацією яких є країни СНД.

За останній рік, за словами начальника відділу Управління по боротьбі зі злочинами, пов'язаними із торгівлею людьми МВС України, у Харківській області О. Золотухіна, у Харкові викрили 8 онлайн-порностудій. У 2017 р. підрозділом відкрито 22 кримінальні провадження і повідомлено про підозру 28 особам. За виготовлення та поширення порнографії у веб-студіях спрямовано до суду 35 кримінальних проваджень по 40 особам [13].

Залишаючи осторонь питання кримінально-правової кваліфікації та методи доведення вини осіб, які організують вебкам-бізнес або які залучені до цього бізнесу, лише зауважимо, що засади моральності суспільства як базового соціального феномена мають визнаватися самостійним об'єктом критичної інфраструктури суспільства як у подібних випадках, так й у випадках вчинення інших протиправних діянь, кримінальна відповідльаність за які передбачена розділом XII КК України. І сьогодні ми є свідками зародження та розвитку нового виду злочинності у сфері моральності, пов'язаного з використанням можливостей інформаційно-телекомунікаційних систем. І ще про одно слід зазначити: правоохоронним органам приходиться боротися вже з наслідками такої проблеми, але ж й до цього часу немає чіткого механізму протидії агітаторам і власникам вебкам-бізнесу в Україні.

1. *Critical Infrastructure Resilience Strategy / Australian Government. URL: http://www.tisn.gov.au. (дата звернення: 13.04.2018).*
2. *Кібербезпека: світові тенденції та виклики для України. К.: НІСД, 2011. С. 11.*
3. *Дубов Д. В. Кіберпростір як новий вимір геополітичного суперництва: монографія. К.: НІСД, 2014. С. 69.*
4. *Попова Т.В., Ліпкан В.А. Стратегічні комунікації: словник / за ред. В.А. Ліпкана. К.: ФОП О.С. Ліпкан, 2016. С. 191.*
5. *Шеломенцев В.П. Основні напрями і суб'єкти забезпечення кібернетичної безпеки України. Боротьба з організ. злочинністю і корупцією (теорія і практика). 2013. № 1 (29). С. 351.*
6. *Манжай О.В. Використання кіберпростору в оперативно-розшуковій діяльності. Право і безпека. 2009. № 4. С. 215. (С. 215-219)*

7. *Вебкам-бизнес. URL: https://ru.wikipedia.org/wiki. (дата звернення: 14.04.2018).*
8. *Modelwebcam.ru Traffic Statistics. URL: https://www.alexa.com/siteinfo/modelwebcam.ru. (дата звернення: 14.04.2018).*
9. *Законна ли работа веб-модели? URL: http://мой-адвокат.укр/news/zakonna_li_rabota_veb_modeli/2016-06-21-243. (дата звернення: 14.04.2018).*
10. *Web-модели или новый вид проституции URL: https://korupciya.com/web-modeli-ili-novyiy-vid-prostitutsii. (дата звернення: 18.04.2018).*
11. *Шокуючий і простий спосіб за допомогою якого українок заманюють займатися проституцією // https://korupciya.com/web-modeli-abo-noviy-vid-prostitutsiyi. (дата звернення: 17.04.2018).*
12. *Про захист суспільної моралі: Закон України № 1296-IV від 20 листопада 2003 р. Відом. Верхов. Ради України. 2004. № 14. Ст. 192.*
13. *Голая правда: за что харьковским веб-моделям обещают по $2000 в месяц URL: https://kh.vgorode.ua/news/sobytyia/353898-kak-v-kharkove-verbuuit-devushek-v-onlain-studyy (дата звернення: 18.04.2018).*

Батиргареєва В.С. Новий вид злочинності у сфері моральності, пов'язаний із використанням інформаційно-телекомунікаційних систем як об'єктів критичної інформаційної інфраструктури

Автор зазначає, що моральний стан суспільства, і, як з'ясувалося, не лише українського, сьогодні потерпає від протиправних дій, що вчиняються з використанням кіберпростору як уявного середовища, в якому за допомогою комп'ютерних мереж циркулює цифрова інформація [4, с.121]. Сьогодні в Україні в повному обсязі присутні всі ключові «класичні» кіберзлочини (шахрайство, здирництво, несанкціонований доступ до персональної інформації користувачів та автоматизованих баз даних, поширення порнографії, продаж зброї чи наркотиків тощо), і щороку їх кількість лише зростає. засади моральності суспільства як базового соціального феномена мають визнаватися самостійним об'єктом критичної інфраструктури суспільства як у подібних випадках, так й у випадках вчинення інших протиправних діянь, кримінальна відповідльаність за які передбачена розділом XII КК України. І сьогодні ми є свідками зародження та розвитку нового виду злочинності у сфері моральності, пов'язаного з використанням можливостей інформаційно-телекомунікаційних систем.

Ключові слова: злочинність у сфері моральності, інформаційно-телекомунікаційні системи, критична інфраструктура

Batyrgareeva V.S. A new type of crime in the field of morality, related to the use of information and telecommunication systems as objects of critical information infrastructure

The author notes that the moral state of society and, as it turned out, not only Ukrainian, today suffers from unlawful acts committed with the use of cyberspace as

an imaginary environment in which digital information circulates through computer networks [4, p. 121]. Today in Ukraine there are all the key «classical» cybercrime (fraud, extortion, unauthorized access to personal information of users and automated databases, the spread of pornography, the sale of weapons or drugs, etc.), and each year they are only increasing. the principles of the morality of society as a basic social phenomenon must be recognized as an independent object of the critical infrastructure of society, in such cases, and in cases of committing other unlawful acts, criminal correspondence for which is provided for in section XII of the Criminal Code of Ukraine. And today we are witnessing the emergence and development of a new type of crime in the field of morality associated with the use of the capabilities of information and telecommunication systems.

Keywords: crime in the field of morality, information and telecommunication systems, critical infrastructure

Голіна В.В.

Національний юридичний університет імені Ярослава Мудрого, професор кафедри кримінології і кримінально-виконавчого права, д.ю.н., юридичних наук, професор, член-кореспондент НАПрН України

Golina V.V.

National Law University named after Yaroslav Mydryy, professor of the department of Criminology and Criminal Execution Law, Doctor of Law, Professor, Corresponding Member of the NALS of Ukraine

Шрамко С.С.

Науково-дослідний інститут вивчення проблем злочинності імені академіка В.В. Сташиса НАПрН України, науковий співробітник відділу кримінологічних досліджень

Shramko S.S.

Scientific research institute of studying crime problems named after academician V.V. Stashis of NALS of Ukraine, researcher of Department of Criminological Researches

СТРАТЕГІЯ ЗМЕНШЕННЯ МОЖЛИВОСТЕЙ ВЧИНЕННЯ ЗЛОЧИНІВ У СИСТЕМІ ЗАХИСТУ КРИТИЧНОЇ ІНФРАСТРУКТУРИ

1. Безпека – головна умова суспільного життя. Втілення й гарантія цієї базової соціальної цінності є вагомим показником спроможності держави убезпечити національні інтереси від зовнішніх і внутрішніх загроз в усіх сферах життєдіяльності. Проблема захисту критичної інфраструктури завжди була актуальною, звернення до неї у теперішній час вкрай важливе, зважаючи на те, що рівень загрози національній безпеці нашої країни залишається високим.

Інфраструктура являє собою сукупність галузей, різноманітних споруд та комунікацій, що забезпечують загальні умови виробництва, необхідні для ефективного розвитку економіки в цілому і повсякденного проживання людей на будь-якій території. Під критичною інфраструктурою вважають сукупність об'єктів інфраструктури держави, які є найбільш важливими для економіки та промисловості, функціонування суспіль-

ства та безпеки населення і виведення з ладу або руйнування яких може мати вплив на національну безпеку і оборону, природне середовище, а також призвести до значних фінансових збитків та людських жертв [1]. Перелік об'єктів критичної інфраструктури визначений у ст. 6 Закону України «Про основні засади забезпечення кібербезпеки України» від 5 жовтня 2017 р. № 2163-VIII. Так, до об'єктів критичної інфраструктури можуть бути віднесені підприємства, установи та організації незалежно від форми власності, які: 1) провадять діяльність та надають послуги в галузях енергетики, хімічної промисловості, транспорту, інформаційно-комунікаційних технологій, електронних комунікацій, у банківському та фінансовому секторах; 2) надають послуги у сферах життєзабезпечення населення, зокрема у сферах централізованого водопостачання, водовідведення, постачання електричної енергії і газу, виробництва продуктів харчування, сільського господарства, охорони здоров'я; 3) є комунальними, аварійними та рятувальними службами, службами екстреної допомоги населенню; 4) включені до переліку підприємств, що мають стратегічне значення для економіки і безпеки держави; 5) є об'єктами потенційно небезпечних технологій і виробництв [2].

2. В Україні захист об'єктів критичної інфраструктури розпорошений в численних нормативно-правових актах, що носять переважно відомчий характер. Це обумовлено тим, що відповідні органи державної влади уповноважені реагувати лише на певні види загроз відносно підпорядкованих об'єктів, тим самим маючи у своєму розпорядженні обмежений набір інструментів та ресурсів. У підготовленій Національним інститутом стратегічних досліджень Аналітичній записці «Щодо створення державної системи захисту критичної інфраструктури» перелічена низка окремих національних систем, що мають відношення до захисту критичної інфраструктури у сучасному розумінні цього терміну, серед яких, зокрема: єдина державна система цивільного захисту; єдина система запобігання, реагування і припинення терористичних актів та мінімізації їх наслідків; державна система фізичного захисту; національна система кібербезпеки. При цьому зазначається, що гострота проблеми захисту критичної інфраструктури полягає у тому, що жодна з існуючих систем не призначена для реагування на усі види загроз, що обумовлює відсутність системного підходу на національному рівні до захисту критичної інфраструктури, який мав би враховувати численні взаємозв'язки її елементів. Разом із тим жоден орган державної влади не опікується проблемами захисту критичної інфраструктури у комплексі [3].

3. Згідно зі ст. 5 Закону України «Про основи національної безпеки України» від 19 червня 2003 р. № 964-IV національна безпека України забезпечується шляхом проведення виваженої державної політики відповідно до прийнятих в установленому порядку доктрин, концепцій, стратегій і програм у політичній, економічній, соціальній, воєнній, екологічній, науково-технологічній, інформаційній та інших сферах [4]. Однією з головних складових державної політики є державна політика боротьби зі злочинністю, яка, у свою чергу, складається із загальносоціальної політики запобігання злочинності (соціальна превенція), кримінологічної політики (стратегія поступового зменшення кількісних показників злочинності, допомога потерпілим), кримінально-правової політики (індивідуалізація кримінальної репресії), кримінальної процесуальної політики (більш широке застосування альтернативних тюремному ув'язненню покарань), кримінально-виконавчої політики (соціальна реінтеграція злочинців) [5, с. 59]. І хоча криміногенним загрозам у контексті захисту критичної інфраструктури увага окремо не приділяється, вони набувають наскрізного характеру, оскільки уразливість її об'єктів пов'язана не тільки з надзвичайними ситуаціями еколого-техногенного характеру, а й з присутністю зловмисних дій людського характеру.

4. Кримінологічна політика за умови її реального впровадження, здатна, спираючись на наукові дослідження, інтегрувати знання та прикладні їх аспекти і на цій основі формулювати запобіжні стратегії. Отже, кримінологічна політика виступає як «генератор» розробки і втілення у життя галузевої конкретизації запобіжних заходів. Останні мають відмінності у спрямованості на криміногенні явища, які в теорії кримінології мають назву «об'єкти».

Поняттям об'єкт запобігання злочинності охоплюються матеріальні і духовні носії детермінант злочинності та її проявів. Об'єкт запобігання злочинності завжди має таку головну властивість як криміногенність, що обумовлює кримінальну практику людей, і завдяки чому такий об'єкт (об'єкти) вивчається у причинно-наслідковому зв'язку. Сутність запобігання злочинності полягає в обмеженні або усуненні криміногенної дії об'єкта. Тому максимальна конкретизація об'єкта, визначення його характерологічних властивостей і уразливих місць слугує для розробки відповідних стратегій і руйнуючих об'єкт заходів, а також концентрації зусиль суб'єктів запобіжного впливу на головних напрямах запобігання та протидії злочинності [6, с. 157].

5. Складовим компонентом системи запобігання злочинності є стратегія зменшення можливостей вчинення злочинів. Зазначена стратегія

представляє собою нормативно врегульовану діяльність державних та недержавних суб'єктів, спрямовану на створення «захисного простору і фізичних бар'єрів для злочинності» (випередження, обмеження, а за можливості й усунення умов, що провокують кримінальну мотивацію або сприяють вчиненню злочину).

У Стратегії національної безпеки України, затвердженої Указом Президента України від 26 травня 2015 р. № 287/2015, визначені такі загрози безпеці критичної інфраструктури: критична зношеність основних фондів об'єктів інфраструктури України та недостатній рівень їх фізичного захисту; недостатній рівень захищеності критичної інфраструктури від терористичних посягань і диверсій; неефективне управління безпекою критичної інфраструктури і систем життєзабезпечення [7]. З огляду на зазначене, убезпечити об'єкти критичної інфраструктури можна лише шляхом усунення наявних виявлених загроз, або умов, що полегшують або навіть сприяють учиненню злочинних посягань, тим самим створивши такі обставини, що утруднюють завершення злочинної мотивації зацікавлених осіб.

6. У межах використання заходів стратегії зменшення можливостей вчинення злочинів розглянемо напрями убезпечення об'єктів критичної інфраструктури від терористичних посягань. Так, на нашу думку, необхідно:

- нейтралізувати політичні чинники, що посилюють загрозу тероризму. Мається на увазі врегулювання соціальних конфліктів, виникаючих внаслідок незадоволення економіко-політичним курсом держави, а також релігійних, національних та територіальних суперечностей;

- обмежити або усунути технічні та організаційні умови, що сприяють терористичній діяльності;

- посилити заходи безпеки стратегічно важливих об'єктів національної інфраструктури (об'єкти газо-, електро- та водопостачання, місця скупчення широкого загалу людей під час проведення політичних та культурно-масових заходів);

- посилити протидію терористичній діяльності на прикордонних територіях та в зоні проведення антитерористичної операції;

- посилити боротьбу з нелегальною міграцією, встановити дієвий контроль за іноземцями, які перетинають кордони України;

- припинити фінансування тероризму;

- посилити контроль за обігом зброї, вибухових речовин та боєприпасів;

- розробити та впровадити на державному рівні систему протидії технологіям впливу на свідомість і поведінку людей для маніпулювання їхніми потребами та цінностями;

- цілеспрямовано формувати громадську думку у напрямку несприйняття ідеології тероризму та осуду будь-яким його проявам [8, с. 66].

7. Протягом останніх років на об'єкти критичної інфраструктури України здійснено низку кібератак, від яких зазнали шкоди мільйони користувачів, а великі компанії понесли фінансові збитки. Відмічається зростання інтенсивності кібератак, спрямованих на інформаційно-телекомунікаційну інфраструктуру, сервери державних та фінансових установ, шкідливе програмне забезпечення використовується під час атак на енергетичну систему України. Зважаючи на загрозливі тенденції поширення цього виду загроз та масштаби шкідливості їх наслідків, слід посилити інформаційну безпеку шляхом: здійснення оцінки ризиків та загроз інформаційній безпеці; ресурсного забезпечення розробки нових технологій захисту від кібератак; поширення та обміну інформацією щодо виявлених кібератак; інформування користувачів мережі про заходи безпеки (наприклад, не відкривати вкладення у підозрілих повідомленнях від сумнівних адресатів, використовувати ліцензійне програмне забезпечення та систему захисту).

1. *Про затвердження Порядку формування переліку інформаційно-телекомунікаційних систем об'єктів критичної інфраструктури держави: постанова Кабінету Міністрів України від 23 серпня 2016 р. № 563. URL: http://zakon3.rada.gov.ua/laws/show/563-2016-%D0%BF (дата звернення: 20.04.2018).*
2. *Про основні засади забезпечення кібербезпеки України: Закон України від 5 жовтня 2017 р. № 2163-VIII. URL: http://zakon5.rada.gov.ua/laws/show/2163-19 (дата звернення: 20.04.2018).*
3. *Аналітична записка «Щодо створення державної системи захисту критичної інфраструктури». URL: http://www.niss.gov.ua/articles/2490/ (дата звернення: 15.04.2018).*
4. *Про основи національної безпеки України: Закон України від 19 червня 2003 р. № 964-IV. URL: http://zakon5.rada.gov.ua/laws/show/964-15 (дата звернення: 15.04.2018).*
5. *Голіна В.В., Колодяжний М.Г., Шрамко С.С. та ін. Громадськість у запобіганні і протидії злочинності: вітчизняний та міжнародний досвід: монографія. Харків: Право, 2017. 284 с.*

6. *Голіна В.В. Об'єкт запобігання злочинності як фундаментальна кримінологічна проблема. Проблеми законності. 2017. Вип. 138. С. 150-161. doi: 10.21564/2414-990x.138.103952.*
7. *Про рішення Ради національної безпеки і оборони України від 6 травня 2015 року «Про Стратегію національної безпеки України»: Указ Президента України від 26 травня 2015 року № 287/2015. URL: http://zakon5.rada.gov.ua/laws/show/287/2015. (дата звернення: 20.04.2018).*
8. *Шрамко С.С. Окремі питання щодо заходів протидії терористичній діяльності Окремі питання щодо заходів протидії терористичній діяльності. Актуальні проблеми кримінально-правової охорони основ національної безпеки України: матеріали кругл. столу (Харків, 26 трав. 2017 р.). Харків: Юрайт, 2017. С. 64-66.*

Голіна В.В., Шрамко С.С. Стратегія зменшення можливостей вчинення злочинів у системі захисту критичної інфраструктури

Безпека – головна умова суспільного життя. Втілення й гарантія цієї базової соціальної цінності є вагомим показником спроможності держави убезпечити національні інтереси від зовнішніх і внутрішніх загроз в усіх сферах життєдіяльності. Проблема захисту критичної інфраструктури завжди була актуальною, звернення до неї у теперішній час вкрай важливе, зважаючи на те, що рівень загрози національній безпеці нашої країни залишається високим.

Інфраструктура являє собою сукупність галузей, різноманітних споруд та комунікацій, що забезпечують загальні умови виробництва, необхідні для ефективного розвитку економіки в цілому і повсякденного проживання людей на будь-якій території. Під критичною інфраструктурою вважають сукупність об'єктів інфраструктури держави, які є найбільш важливими для економіки та промисловості, функціонування суспільства та безпеки населення і виведення з ладу або руйнування яких може мати вплив на національну безпеку і оборону, природне середовище, а також призвести до значних фінансових збитків та людських жертв

Ключові слова: критична інфраструктура, захист критичної інфраструктури

Golina V.V., Shramko S.S. A strategy to reduce the possibility of committing crimes in the system of critical infrastructure protection

Security is the main condition of social life. The embodiment and guarantee of this basic social value is a significant indicator of the state's ability to safeguard national interests from external and internal threats in all spheres of life. The problem of protecting critical infrastructure has always been relevant, the appeal to it at present is extremely important, given that the level of threat to the national security of our country remains high.

Infrastructure is a collection of industries, various buildings and communications that provide the general conditions of production necessary for the effective

development of the economy as a whole and the daily living of people in any territory. The critical infrastructure is considered to be the totality of state-owned infrastructure that is most important for the economy and industry, the functioning of the society and the security of the population, and the decommissioning or destruction of which may have an impact on national security and defense, the natural environment, and lead to significant financial losses and human casualties

Keywords: critical infrastructure, protection of critical infrastructure

Грищук В.К.

доктор юридичних наук, професор,член-кореспондент НАПрН України, декан юридичного факультету Львівського державного університету внутрішніх справ

Grishchuk V.K.

Doctor of Law, Professor, Corresponding Member of the National Academy of Sciences of Ukraine, Dean of the Faculty of Law of Lviv State University of internal affairs

ЯКІСТЬ КРИМІНАЛЬНО-ПРАВОВОГО ЗАБЕЗПЕЧЕННЯ ПРОТИДІЇ ЗЛОЧИННОСТІ У СФЕРІ КРИТИЧНОЇ ІНФРАСТРУКТУРИ В УКРАЇНІ

З широких філософських позицій під якістю слід розуміти сукупність найбільш істотних властивостей, які характеризують даний предмет чи явище і відрізняють його від інших предметів чи явищ оточуючої дійсності.

Механізм кримінально-правового забезпечення якості протидії злочинності у будь-якій сфері суспільного буття складний і багатоплановий. Він включає, зокрема, систему державних і недержавних органів та організацій, законодавчу базу їх діяльності, міжнародну співпрацю. Кожен з названих елементів має бути наділений необхідними якісними інструментальними властивостями.

Стосовно законодавства можна говорити про якість його форми та змісту, пам'ятаючи філософську аксіому, що форма завжди сутнісна, а сутність завжди формована.

Найважливішою передумовою високої якості протидії злочинності у сфері критичної інфраструктури є належний рівень наукового забезпечення розроблення, прийняття та застосування кримінального законодавства: матеріального, процесуального та виконавчого.

На жаль, доводиться констатувати, що наша потужна наука загалом та кримінально-правова, кримінально-процесуальна, кримінально-виконавча і кримінологічна наука, зокрема, не є повноправним суб'єктом правотворчої діяльності. Наукова кримінологічна експертиза законопроектів, якими вносяться зміни до чинного законодавства, не проводиться.

Традиційно, з часів родоначальника науки кодифікації Ієремії Бентама, в доктрині права найвищою формою удосконалення якостей форми і змісту законодавства вважаються кодекси .Саме вони визнані такими в континентальній системі права , оскільки найбільш повно забезпечують(мають забезпечувати), зокрема, такі якості законодавства як його оглядовість, ясність та доступність, відсутність прогалин та суперечностей. Треба зазначити, що, на жаль, українська законотворча практика йде переважно шляхом творення багатоманітних, нерідко суперечливих, окремих законів, якими вносяться багаточисельні зміни до чинного законодавства. Так, станом на сьогоднішній день, в Україні є чинними більше: 6340 законів України, 14130 постанов Верховної Ради, 27240 указів Президента, 12060 розпоряджень Президента, 36920 постанов Кабінету міністрів, 26980 розпоряджень Кабінету міністрів, 30440 нормативних актів міністерств та відомств, які зареєстровані в міністерстві юстиції та понад 200000 цих актів, які не зареєстровані в міністерстві юстиції. До цього можна додати законодавство часів СРСР-біля 43000 та більше 1410 міжнародно-правових актів. В такому правовому полі важко зорієнтуватися навіть висококваліфікованим правникам, не кажучи вже про громадян до яких ці акти адресовані.

Найбільш якісним , як відомо, є той нормативний акт, який не потребує конкретизації в підзаконних нормативних актах або потреба конкретизації норм якого є мінімальною, вимушеною. Світовою правотворчою практикою, ще з сивої давнини, визнано, що таким нормативним актом є кодекс законів.

Якість закону прямо залежить від якості законодавчого органу, сприйняття депутатами принципів права, розуміння ними правил законодавчої техніки, значення кодифікації законодавства. Це проблема значного рівня, бо нинішні законодавці, як правило, не мають юридичної професійної правосвідомості загалом і достатньої правової свідомості зокрема за браком належної юридичної освіти та правозастосувальної практики. Оскільки є такі проблеми, то логічною є проблема неналежної якості законодавства. Особливо це видно у тих випадках, коли прийнятий закон не чітко сформульований, неясний, містить неоднозначні поняття, суперечності. Ситуація ускладнюється відсутністю обов'язкової наукової експертизи законопроектів. Все це разом, як думається, не дозволяє належним чином забезпечити дотримання наукових засад законодавчої техніки, реалізацію в законодавстві кожного з принципів права на науковому рівні, забезпечивши при цьому неодмінно їх гармонійне поєднання. За цих умов виникає питання: як уникнути цих негативних факторів?

Перше. Є потреба розглянути питання про професійність як найбільш притаманну рису законотворця - народного депутата. Очевидним став факт, що професійність полягає не в тому щоб на постійній основі бути присутнім у Верховній Раді, а в здатності розробляти та приймати високоякісні закони, що не є можливим без належної юридичної освіти. Поправити ситуацію можна. При максимальному варіанті вирішення проблеми, в Конституції України і в законодавстві про вибори доцільно встановити ценз, вимогу про наявність у кандидата у народні депутати юридичної освіти. Можливий і інший варіант. За умови запровадження двопалатної Верховної Ради, передбачити гармонійне поєднання принципів професійності та представництва від суб'єктів адміністративно-територіального устрою. Для кандидатів у депутати до верхньої палати – обов'язкова вимога наявності юридичної освіти, а до нижньої палати –ні.

Друге. Дуже давно в доктрині права дискутується питання про нагальну необхідність розроблення та прийняття спеціального закону, який би регулював питання законодавчої діяльності. Зокрема, пропонувалося назвати його "Законом про правотворчість", " Законом про нормативні акти". Та головне не в назві такого закону, а в тому щоб передбачити в ньому обов'язковість наукової правової та кримінологічної експертизи проектів законів, яку, на моє переконання, повинна здійснювати Національна академія правових наук України, яка має достатні підстави стати повноправним суб'єктом законотворчої діяльності. Це може дати відчутний результат і за нині чинних правових засад організації Верховної Ради України.

Третє:про відсутність компетентного державного законопроектного органу, здатного забезпечити розробку проектів законів на наукових засадах.

На сьогоднішній день склалася парадоксальна ситуація при якій в державі відсутній єдиний орган який би системно готував науково обґрунтовані проекти законів, відповідав за їх якість. Ці проекти готують всі – «кому не лінь», переважно люди які не мають глибокої уяви про принципи організації та функціонування держави, про право загалом та принципи правового регулювання зокрема. Найчастіше ця «ноша» падає на Кабінет Міністрів, чи підпорядковані йому Міністерства, що не є їх функціональним завданням. Та й фахівців з юридичною освітою найвищого наукового рівня там практично немає. Крім того, наслідком такої ситуації є, так званий, «відомчий» підхід, коли відомство намагається нав'язати країні, народові своє, нерідко спонтанне, необґрунтоване, суб'єктивне, суперечливе бачення правового врегулювання суспільних

відносин і нерідко не на користь громадян, а що найгірше – корупційне лобіювання інтересів олігархічно-політичних кланів.

Часто, окрилені «голим ентузіазмом», функцію підготовки законопроектів виконують народні депутати, котрі, як правило, або взагалі не мають юридичної чи взагалі будь-якої вищої освіти, або, якщо окремі з них і мають цю освіту, то не найвищого наукового рівня. В народі вірно кажуть, що на «голому ентузіазмі», без належного інтелекту не поїдеш, а якщо й поїдеш, то не далеко. Звідси – якість законів прямо залежить від якості Верховної Ради, її народних депутатів. Тому й не випадково «маємо те, що маємо» – часто низької якості, суперечливе, неефективне, заполітизоване, нерідко прийняте в інтересах вражених корупцією економіко-політичних кланів законодавство, яке не сприяє ефективній протидії корупції, а іноді викликає відомі соціальні конфлікти, гальмує соціальний розвиток.

Закономірно виникає питання про те, що слід зробити аби вийти на якісно вищий рівень правотворчої діяльності. Одним із можливих варіантів його вирішення може бути створення спеціального законопроектного органу, наприклад, Державної кодифікаційної Комісії. Історичний досвід дуже успішної діяльності таких комісій у цілому світі відомий.

Вважаю за доцільне запропонувати для дискусії найважливіші концептуальні підходи до розуміння інструментальної ролі Державної кодифікаційної Комісії України.

1. Державна кодифікаційна Комісія України – єдиний державний орган, який має бути наділений повноваженнями щодо розроблення законопроектів для їх розгляду на Всеукраїнському референдумі чи у Верховній Раді України.

2. Кодифікаційна Комісія України утворюється Президентом України за поданням Національної академії правових наук України.

3. Кодифікаційна Комісія України утворюється у складі 40-50 Державних кодифікаторів (за рахунок, наприклад, скорочення чисельності Верховної Ради через внесення відповідних змін до Конституції України Верховною Радою або вирішення цього питання через Всеукраїнський референдум).

4. Державним кодифікатором може бути особа не молодша 40 років, яка є: громадянином України не менше 20 років, вільно володіє державною мовою, не притягалася до кримінальної відповідальності за вчинення умисного злочину, має позитивну моральну поведінку, має науковий ступінь доктора юридичних наук та вчене звання професора.

Державний кодифікатор не наділяється правовим статусом державного службовця. Він є службовою особою.

5. Соціально-побутове забезпечення державних кодифікаторів та гарантії їх діяльності мають бути на достатньо високому рівні.

6. Державна кодифікаційна Комісія України діє на підставі Закону України «Про кодифікаційну Комісію України», який приймається на Всеукраїнському референдумі. Це надійно убезпечить її від можливого деструктивного впливу з боку Верховної Ради України, дозволить розробляти проекти законів, необхідних для держави, а не в інтересах корумпованих економіко-політичних кланів, чи інших «зацікавлених» суб'єктів.

7. Державна кодифікаційна Комісія України повинна здійснювати свою роботу відповідно до перспективного «Плану кодифікації законодавства України», який складається на 5-10 років і затверджується Президентом України за поданням Національної академії правових наук України.

Правом ініціювання перед Державною кодифікаційною Комісією України питання про розроблення відповідних змін до чинного законодавства повинні мати: Президент України, Верховна Рада України, Кабінет Міністрів України, Уповноважений Верховною Ради України з прав людини, Конституційний Суд України, Верховний Суд України, Антикорупційне Бюро України, Національна академія правових наук України.

8. Розроблений Державною кодифікаційною Комісією України проект Закону, разом з висновком Національної академії правових наук України, має подаватися Президентові України, який вирішує питання про його винесення на Всеукраїнський референдум чи внесення на розгляд Верховної Ради України.

Президент України має право повернути проект Закону на доопрацювання зі своїми зауваженнями до Державної кодифікаційної Комісії України.

9. Депутати Верховної Ради України, розглядаючи внесений Президентом України Закон, голосують постатейно, а у випадку незгоди з окремими положеннями, пропонують свої зміни до нього. Такі пропозиції змін у концентрованому детальному вигляді направляються Головою Верховної Ради до Державної кодифікаційної Комісії України для їх розгляду по суті.

У випадку відмови Кодифікаційною Комісією України щодо врахування відповідної пропозиції щодо зміни законопроекту, вона не може бути внесена повторно на її розгляд.

10. Рішення Державної кодифікаційної Комісії України не можуть бути оскаржені в судовому порядку.

11. Державна кодифікаційна Комісія України не проводить офіційного розгляду скарг, звернень та подань тощо.

Викладені вище судження не позбавлені певних ознак дискусійності як і інші судження щодо аналізу доволі складної української політико-правової дійсності. Запропоновані підходи не розглядаються автором як «істина в найвищій інстанції». Вони, образно висловлюючись, є наболілим закликом до наукової дискусії і наукового пошуку оптимального вирішення дуже важливої практичної проблеми протидії злочинності.

Наступне-це якість мови закону. Закон, як відомо, є своєрідним посередником у діалозі між демократичним законодавцем і правозастосовними органами та людиною. Ефект прямої індукції волі як продукту діяльності свідомості законодавця у свідомість і волю людини, якій вона адресується, неможливий. Воля мусить мати для своєї реалізації передусім чіткий словесний вираз, а коли йдеться про використання для норм закону – якісний словесний письмовий вираз. Законодавець, який розраховує на максимально можливу реалізацію своєї волі, мусить «розмовляти» з тими, кому вона адресується, зрозумілою, максимально однозначною, а отже якісно необхідною мовою.. Цьому може сприяти, зокрема, запровадження на законодавчому рівні лінгвістичної експертизи нормативних актів

Змістовна частина нормативного акту не повинна бути перенасичена оцінними поняттями, термінами. Ця метрологічна засада є неодмінною для встановлення зворотного, діалогічного зв'язку між адресатами (громадяни, службові особи правоохоронних органів) і законодавцем, вироблення дієвої нормативної системи суспільної комунікації, а отже і для забезпечення ефективності правового регулювання. В принципі, недодержання цих правил законодавчої техніки не впливає на юридичну силу закону, однак позначається на рівні зрозумілості волі законодавця в матерії його норм, а отже і на його якості.

Однак чи можна засобами понять, термінів повністю адекватно відтворити оточуючу дійсність? Не впадаючи в ідеалізм, слід відповісти однозначно, що ні, оскільки об'єкти, явища суспільної дійсності надзвичайно багатоманітні, багатогранні й перебувають у постійному русі, розвитку. Адекватне переведення оточуючої дійсності в абсолютно визначені понятійні структури означало б завершення процесу пізнання, що за умови недосконалості самої мови та безмежності матеріального світу неможливе. Таке бажання завжди відображає статус перспективної мети.

Зазначимо, що людська мова розвивається разом з оточуючою дійсністю, але мова як знаряддя, метод пізнання цієї дійсності відстає від її розвитку. Отже, оцінні поняття є «необхідним соціальним злом» і тому немає достатніх підстав погоджуватися з думкою деяких авторів про можливість їх повної заміни формально визначеними поняттями. Разом з цим, багатозначність оцінних понять дозволяє у багатьох випадках одночасно оцінювати конкретне діяння, залежно від суб'єкта оцінки, як законне або незаконне, що розмиває межі законності і справедливості. Думається, коли людина не усвідомлювала через неясність закону, що вчиняє правопорушення, а суд кваліфікує такі дії як протиправні, то це чистої води застосування принципу об'єктивного ставлення у вину. Разом з цим, при цьому знову ж таки зберігається можливість різної (суб'єктивної) оцінки однотипних діянь різними судами, а отже, і можливість зловживань. За таких умов говорити про якість рівності осіб перед законом неможливо, це рівність перед суддівським свавіллям.

Неясність закону, його неоднозначність, як свідчення його низької якості, сприяє розширенню меж судової дискреції (угляду), що здавна оцінюється як небезпечний фактор для правопорядку та демократії. Нагальною є необхідність розумного обмеження в чинному законодавстві можливості судової дискреції (угляду).

У державі демократичного спрямування, коли вольовий припис норми будь-якого нормативного акту не зрозумілий чітко або є двозначним, повинен без винятків, у всіх випадках, діяти принцип: «Будь-який сумнів, неясність щодо змісту вольового припису норми чинного законодавства має тлумачитися правозастосувальним органом на користь людини, щодо якої ця норма застосовується». Цей принцип має застосовуватися не лише судом, а й усіма правозастосувачами. Друге, він повинен діяти не лише при застосуванні законів, але й усіх інших підзаконних нормативних актів, які визначають механізми реалізації прав і свобод людини. Третє, не менш важливе, – цей принцип слід закріпити на Конституційному рівні, що позитивно вплине на якість правового регулювання. При такому підході у державних чиновників буде менше можливостей для зловживання неясністю норм чинних нормативних актів.

Наступне. Окремої уваги заслуговує проблема якості гуманізації законодавства. Гуманістичний потенціал є органічною властивістю, якістю цивілізованого, демократичного суспільства і, з огляду на це, не може бути «дарований» суспільству за чиєюсь доброю волею «зверху» або «з-за кордону», а мусить бути вистражданий самим суспільством, його працею. Таке формування гуманістичного потенціалу відбувається в усіх

сферах суспільного життя впродовж багатьох років під впливом комплексу об'єктивних і суб'єктивних факторів. Отже, розвиток гуманістичних основ демократичного суспільства проходить не довільно, а на ґрунті відповідної зрілості в ньому економічних, соціально-політичних та інших відносин. Недодержання такого підходу обумовлює низьку якість законодавства, свідчить про перехід на позиції волюнтаризму, зловживань в правовій політиці, що неодмінно тягне за собою соціальні диспропорції, підриває фундаментальні основи демократії. Тому жодні благородні, але не виважені, однобокі наміри гуманізації законодавства, що не ґрунтуються на реальних економічних, політичних і соціальних передумовах єдності соціального і морального прогресу суспільства, не можуть принести суспільству користі бути стимулом його розвитку, забезпечити нормальне функціонування правоохоронної системи. В цьому контексті, як приклад " забігання вперед ", можна назвати окремі положення нового кримінального процесуального кодексу України, які піддаються справедливій критиці з боку науковців.

Є необхідність наголосити, що повага до закону повинна мати двосторонній вияв. З боку законодавця - беззастережно поважати людину як розумну, правову істоту, поважати її гідність, права і свободи, сприяти їх утвердженню і розвитку, дбати про створення умов для реалізації її потреб через призму гармонійного поєднання всіх суспільних інтересів. Саме в тому, наскільки закон наділений такими характерними рисами, проявляється його змістовна якість. Лише за таких умов можливий надійний зворотній зв'язок між людиною і державою, між державою та іншими суб'єктами суспільних відносин, а, отже, і висока ефективність державного управління засобами законодавства. З боку громадян-повага до таких розумних, справедливих, гуманних та демократичних законів.

Розглянуті вище теоретико-прикладні проблеми, як загального так і часткового характеру, є лише незначною частиною проблем удосконалення механізму протидії злочинам у сфері критичної інфраструктури.

Грищук В.К. Якість кримінально-правового забезпечення протидії злочинності у сфері критичної інфраструктури в Україні

Механізм кримінально-правового забезпечення якості протидії злочинності у будь-якій сфері суспільного буття складний і багатоплановий. Він включає, зокрема, систему державних і недержавних органів та організацій, законодавчу базу їх діяльності, міжнародну співпрацю. Кожен з названих елементів має бути наділений необхідними якісними інструментальними властивостями.

Якість закону прямо залежить від якості законодавчого органу, сприйняття депутатами принципів права, розуміння ними правил законодавчої техніки, значення кодифікації законодавства. Це проблема значного рівня, бо нинішні

законодавці, як правило, не мають юридичної професійної правосвідомості загалом і достатньої правової свідомості зокрема за браком належної юридичної освіти та правозастосувальної практики. Оскільки є такі проблеми, то логічною є проблема неналежної якості законодавства. Особливо це видно у тих випадках, коли прийнятий закон не чітко сформульований, неясний, містить неоднозначні поняття, суперечності. Ситуація ускладнюється відсутністю обов'язкової наукової експертизи законопроектів. Все це разом, як думається, не дозволяє належним чином забезпечити дотримання наукових засад законодавчої техніки, реалізацію в законодавстві кожного з принципів права на науковому рівні, забезпечивши при цьому неодмінно їх гармонійне поєднання.

Ключові слова: законодавча техніка, закон про кримінальну відповідальність, якість законодавства

Grishchuk V.K. The quality of criminal law enforcement of crime prevention in the field of critical infrastructure in Ukraine

The mechanism of criminal-law support for the quality of combating crime in any sphere of social existence is complex and multifaceted. It includes, in particular, the system of state and non-state bodies and organizations, the legislative basis for their activities, and international cooperation. Each of these elements must be endowed with the necessary qualitative tool properties.

The quality of the law directly depends on the quality of the legislative body, the deputies perceive the principles of law, their understanding of the rules of legislative technique, the importance of codification of legislation. This is a significant issue, since current legislators generally do not have legal professional knowledge in general and sufficient legal awareness, in particular due to the lack of proper legal education and law enforcement practice. Since there are such problems, the problem of improper quality of legislation is logical. This is especially apparent in cases where the law is not clearly formulated, obscure, contains ambiguous notions, contradictions. The situation is complicated by the lack of mandatory scientific expertise of the bills. All this together, it seems, does not allow to properly ensure the observance of the scientific principles of legislative technique, the implementation in law of each of the principles of law at the scientific level, while ensuring, without fail, their harmonious combination.

Keywords: legislative technique, law on criminal liability, quality of legislation

Денисов С.Ф.
Академія Державної пенітенціарної служби, завідувач кафедри кримінального, кримінально-виконавчого права та кримінології,доктор юридичних наук, професор

Пузиревський М.В.
Академія Державної пенітенціарної служби, начальник кабінету кафедри тактико-спеціальної підготовки

Denisov S.F.
Academy of the State Penitentiary Service, Head of the Department of Criminal, Criminal Execution and Criminology, Doctor of Law, Professor

Puzirevsky M.V.
Academy of the State Penitentiary Service, Head of the department of tactical training

ПРОБЛЕМНІ ПИТАННЯ СТВОРЕННЯ СИСТЕМИ ЗАХИСТУ КРИТИЧНОЇ ІНФРАСТРУКТУРИ В УКРАЇНІ

На теперішній час тенденції стрімкого розвитку світового політичного і економічного простору, а також внутрішні соціально-економічні проблеми спонукають вітчизняного законодавця до перегляду сучасних підходів розвитку сектора національної безпеки та оборони, що не є можливим без урахування світових тенденцій у сфері міжнародної безпеки.

Драматичні події 2014–2018 років в Україні актуалізували для країни питання захисту інфраструктури, об'єктів та систем важливих для життєдіяльності суспільства та сформували потребу створення системи захисту критичної інфраструктури на теренах нашої держави.

Саме тому, з метою імплементації в національне законодавство положень Директиви Європейського Союзу № 2008/114/ЕС від 08 грудня 2008 р. «Про ідентифікацію і позначення Європейських важливих інфраструктур та оцінку необхідності вдосконалення їх захисту» [1] та Резолюції Ради Безпеки Організації Об'єднаних Націй № S/RES/2341 (2017) від 13 лютого 2017 р. «Загрози міжнародному миру та безпеці, створювані терористичними актами» [2], Розпорядженням Кабінету Міністрів України № 1009-р від 06 грудня 2017 р. було схвалено «Концепцію створення дер-

жавної системи захисту критичної інфраструктури» (далі – Концепція) [3].

Слід відзначити, що прийняття даної Концепції поставило за мету визначити основні напрями, механізми та строки комплексного правового врегулювання питань захисту критичної інфраструктури та створити систему державного управління у сфері захисту критичної інфраструктури – Національну систему захисту критичної інфраструктури.

Так, з урахуванням потреб національної безпеки і необхідності запровадження системного підходу до розв'язання проблеми на загальнодержавному рівні, саме створення системи захисту критичної інфраструктури є одним із пріоритетів у реформуванні сектору оборони і безпеки України.

Варто наголосити, що основними проблемними питаннями, що потребують невідкладного розв'язання Національною системою захисту критичної інфраструктури на теперішній час, є:

- відсутність державного органу, відповідального за координацію дій у сфері захисту критичної інфраструктури, єдиної загальнодержавної системи захисту критичної інфраструктури;
- відсутність єдиних критеріїв та методології віднесення об'єктів інфраструктури до критичної інфраструктури, порядку їх паспортизації та категоризації, єдиної методології проведення оцінки загроз критичній інфраструктурі, а також відсутність спеціального правоохоронного органу, відповідального за проведення аналізу та оцінки загроз критичній інфраструктурі внаслідок проведення іноземними державами економічної експансії та дискримінаційної політики, недопущення заподіяння шкоди економічному і науково-технічному потенціалу держави, а також організацію та вжиття відповідних заходів протидії;
- невизначеність повноважень, завдань і відповідальності центральних органів виконавчої влади та інших державних органів у сфері захисту критичної інфраструктури, а також прав, обов'язків та відповідальності власників (розпорядників) об'єктів критичної інфраструктури;
- недостатність та неузгодженість нормативно-правового регулювання з питань захисту систем і об'єктів критичної інфраструктури, зокрема відсутність спеціального закону про критичну інфраструктуру та її захист, недостатній рівень міжнародного співробітництва у сфері захисту критичної інфраструктури;
- нерозвиненість державно-приватного партнерства у сфері захисту критичної інфраструктури та невизначеність джерел фінансування заходів із захисту критичної інфраструктури [3].

У свою чергу, забезпечення захисту критичної інфраструктури в майбутньому, на нашу думку, передбачається вирішувати за такими ключовими напрямами:

1. Визначення пріоритетних секторів критичної інфраструктури, органів державної влади, які відповідатимуть за формування та реалізацію державної політики щодо її захисту.

2. Налагодження обміну інформацією між суб'єктами державної системи захисту критичної інфраструктури про загрози критичній інфраструктурі, характеристики систем захисту об'єктів критичної інфраструктури, механізми і процедури реагування на загрози.

3. Покращення системи моніторингу стану об'єктів критичної інфраструктури, аналізу та прогнозування загроз критичній інфраструктурі, визначення шляхів та способів зменшення ризиків, пов'язаних з функціонуванням критичної інфраструктури, впровадження інноваційних розробок та удосконалення існуючих засобів забезпечення безпеки та захисту об'єктів критичної інфраструктури, запобігання виникненню на них надзвичайних ситуацій.

4. Посилення кримінально-правової відповідальності за порушення законної діяльності об'єктів критичної інфраструктури.

5. Розвитку міжнародного співробітництва з питань захисту критичної інфраструктури та інтеграції України до міжнародних систем захисту критичної інфраструктури.

6. Розроблення та затвердження критеріїв та методології віднесення об'єктів (незалежно від їх форми власності) до переліку критичної інфраструктури.

7. Створення нормативно-правових та організаційних механізмів захисту критичної інфраструктури шляхом розроблення й прийняття Законів України «Про критичну інфраструктуру та її захист», «Про національну безпеку України» та «Про інформаційну безпеку».

8. Створення відділу з вивчення проблем протидії злочинності у сфері захисту критичної інфраструктури на базі Міжвідомчого науково-дослідного центру з проблем боротьби з організованою злочинністю при Раді національної безпеки і оборони України.

9. Удосконалення механізмів державно-приватного партнерства у сфері захисту критичної інфраструктури для підвищення безпеки та забезпечення стійкості критичної інфраструктури з визначенням зобов'язань держави та власників (розпорядників) об'єктів критичної інфраструктури.

Очевидним є те, що зазначена нами проблематика є питанням національної безпеки держави, що володіє атомними електростанціями, розгалуженою мережею газо- і нафтопроводів, транспортною системою та масою найважливіших виробничих комплексів, тому найближчим часом доцільним буде внесення відповідних змін до вітчизняного законодавства, а також реалізація заходів, спрямованих на захист об'єктів критичної інфраструктури.

Таким чином, створення Національної системи захисту критичної інфраструктури має стати одним із пріоритетних напрямків вдосконалення сектора безпеки і оборони України, що в обов'язковому порядку вимагатиме нормативно-правового регулювання основних принципів її функціонування, впровадження єдиних підходів до організації управління об'єктами системи, визначення засад взаємодії залучених до захисту критичної інфраструктури державних органів та суб'єктів господарювання, суспільства і громадян, представників наукового середовища. Все вищевикладене в майбутньому сприятиме удосконаленню механізмів забезпечення національної безпеки та посилить потенціал нашої держави стосовно інтеграційних поступів до Євроатлантичного альянсу та Європейського Союзу.

1. *Про ідентифікацію і позначення Європейських важливих інфраструктур та оцінку необхідності вдосконалення їх захисту: Директива Європейського Союзу від 08.12.2008 р. № 2008/114/ЕС. URL: http://eur-lex.europa.eu/legal-content/EN/TXT/?uri=celex:32008L0114 (дата звернення: 10.04.2018).*
2. *Загрози міжнародному миру та безпеці, створювані терористичними актами: Резолюція Ради Безпеки Організації Об'єднаних Націй від 13.02.2017 р. № S/RES/2341 (2017). URL: http://www.un.org/ru/sc/documents/resolutions/2017.shtml (дата звернення: 10.04.2018).*
3. *Про схвалення Концепції створення державної системи захисту критичної інфраструктури: Розпорядження Кабінету Міністрів України від 06.12.2017 р. № 1009-р. Офіційний вісник України. 2018. № 7. Ст. 271.*

Денисов С.Ф., Пузиревський М.В. Проблемні питання створення системи захисту критичної інфраструктури в Україні

На теперішній час тенденції стрімкого розвитку світового політичного і економічного простору, а також внутрішні соціально-економічні проблеми спонукають вітчизняного законодавця до перегляду сучасних підходів розвитку сектора національної безпеки та оборони, що не є можливим без урахування світових тенденцій у сфері міжнародної безпеки.

Створення Національної системи захисту критичної інфраструктури має стати одним із пріоритетних напрямків вдосконалення сектора безпеки і оборони України, що в обов'язковому порядку вимагатиме нормативно-правового регулювання основних принципів її функціонування, впровадження єдиних підходів до організації управління об'єктами системи, визначення засад взаємодії залучених до захисту критичної інфраструктури державних органів та суб'єктів господарювання, суспільства і громадян, представників наукового середовища.

Ключові слова: критична інфраструктура, система захисту критичної інфраструктури

Denisov S.F., Puzirevsky M.V. Problematic issues of creating a critical infrastructure protection system in Ukraine

Currently, the trends of rapid development of the world political and economic space, as well as internal socio-economic problems, urge domestic legislators to revise modern approaches to the development of the national security and defense sector, which is not possible without taking into account global trends in international security.

Creation of the National Critical Infrastructure Protection System should become one of the priority directions of improvement of the security and defense sector of Ukraine, which will necessarily require regulatory legal regulation of the basic principles of its functioning, introduction of unified approaches to the organization of management of objects of the system, determination of the principles of interaction of the involved to protect the critical infrastructure of state bodies and business entities, society and citizens, representatives of the scientific environment.

Key words: critical infrastructure, critical infrastructure protection system

Денисова Т.А.

Академія Державної пенітенціарної служби України, помічник ректора з наукової та науково-методичної роботи, д.ю.н., професор, заслужений юрист України

Denisova T.A.

Academy of the State Penitentiary Service of Ukraine, Assistant to the Rector for Scientific and Methodological Work, Doctor of Law, Professor, Honored Lawyer of Ukraine

ЗАГРОЗИ ТЕРОРИСТИЧНОГО ХАРАКТЕРУ ОБ'ЄКТАМ КРИТИЧНОЇ ІНФРАСТРУКТУРИ: ВІД ІСТОРІЇ ДО СУЧАСНИХ РЕАЛІЙ

Терор і тероризм мають давню історію і супроводжують людство на всіх етапах його розвитку: Стародавній Рим та раннє християнство, Візантія та Арабський халіфат ... В окремих випадках терор і тероризм можуть поставити народи на межу фізичного винищення. Тероризм визнається світовим співтовариством як один з найнебезпечніших викликів сучасності. Події останнього часу показують, що діяльність терористичних організацій, набуваючи принципово нових рис, стає все більш витонченою і цинічною. Змінюються стратегічні напрямки силових ударів, вдосконалюється тактика сучасних терористичних угруповань. Для досягнення своїх цілей терористи все частіше вибирають мішенями не державні й військові об'єкти, не політичних лідерів, а звичайних громадян: туристів, відвідувачів магазинів, культурно-спортивних заходів, ресторанів, кафе тощо. Це призводить до зростання числа невинних людських жертв. Сьогоднішній теракт ставить завданням номер один – психологічно вразити якомога більше населення, залякати громадян, посіяти паніку і розбрат. Терміни «тероризм» і «терор» почали широко використовуватися ще за часів Французької буржуазної революції (1789-1794 рр.) і сьогодні існує понад 100 таких визначень.

Зміст поняття «тероризм» має також законодавче закріплення. Так, у Законі України «Про боротьбу з тероризмом» зазначається, що «тероризм – це суспільно небезпечна діяльність, яка полягає у свідомому, цілеспрямованому застосуванні насильства шляхом захоплення заручників, підпалів, вбивств, тортур, залякування населення та органів влади, або вчинення інших посягань на життя чи здоров'я людей або погрози вчинення злочинних дій з метою досягнення злочинних цілей »[1]. Практично ана-

логічне визначення міститься і в національній Концепції боротьби з тероризмом [2]. Аналізуючи норми законодавства можна стверджувати, що до терористичної діяльності віднесені діяння, що представляють загрозу суспільній безпеці і створюють колективну небезпеку для людей. В.П. Ємельянов відносить до категорії цих злочинів тероризм, терористичний акт і інші злочини, якщо ці дії відбуваються публічно, спрямовані на залякування населення з метою впливу на прийняття будь-якого рішення чи відмови від нього [3]. Чинним КК України передбачена відповідальність за підготовку до вчинення терористичних актів або публічні заклики до вказаних дій, створення терористичної групи чи терористичної організації, сприяння вчиненню терористичного акту, а також за фінансування тероризму (ст.ст. 258 - 258-5 КК України).

Сьогодні накопичено значний міжнародний досвід дослідження і протистояння терористичним проявам. Він свідчить про те, що запобігти діям терористичних організацій, а тим більше діям терориста-одинака, практично неможливо, але все ж, при своєчасному проведенні контрзаходів, така можливість існує. Найбільш дієвим способом є агентурне проникнення в терористичні організації для виявлення планів з підготовки терористичних актів і їх виконавців. Адже, незважаючи на суворі заходи конспірації, що вживаються терористами, в підготовці таких терактів бере участь багато людей: ведеться прихована розвідка об'єкта, вивчається обстановка навколо нього, готується план, проводяться тренування, виготовляються вибухові пристрої і т.п. Існують і інші досить ефективні заходи превентивного характеру, хоча необхідно визнати, і це підтверджується останнім сплеском терористичних проявів, міждержавне співробітництво спецслужб з протидії тероризму знаходиться на недостатньому рівні.

Одним з найнебезпечніших проявів терористичної діяльності є терористичний акт відносно об'єктів критичної інфраструктури, до переліку яких відносяться паливно-енергетичні комплекси в різних країнах світу. Під час нападу на АЕС члени терористичної організації, швидше за все, спробували б провести пошкодження його систем життєзабезпечення з метою розплавлення реакторної зони. Найгіршим з можливих результатів терористичної акції стало б повторення Чорнобильської катастрофи, що призвела до шкоди здоров'ю тисяч людей, значних сільськогосподарських, експлуатаційних втрат, втрат джерел енергії та витрати на ліквідацію наслідків. Громадяни України, як і інших країн, досі відчувають відлуння цієї трагедії. Навіть в умовах запобігання значного викиду радіоактивності, довгострокова зупинка енергоблоку здатна викликати ве-

ликі економічні і соціально-політичні втрати. Хочу нагадати, що саме 26 квітня 1986р. в Україні вшановують пам'ять за загиблими на Чорнобильській АЕС. Лише за статистикою, що й приблизно не відобразила усієї трагічної ситуації, протягом перших місяців загинули 31 ліквідатор, більш ніж 600 тис. отримали значну дозу опромінювання, а близько 120 тис. були евакуйовані з 30-кілометрової зони відчуження [4].

Загострення боротьби з терористичними проявами в світі обумовлює необхідність розробки загальнодержавних, і на їх основі, галузевих заходів щодо захисту від посягань міжнародних терористичних організацій, висуває особливі вимоги до здійснення державних заходів щодо забезпечення безпеки радіаційно-ядерних об'єктів. Боротьба з ядерним тероризмом вимагає роботи з багатьох напрямків. Треба відзначити, що важливою є робота правоохоронних органів і спеціальних служб з нейтралізації терористичних груп. Цілком нагальною є система заздалегідь підготовлених заходів по обмеженню збитку і ліквідації наслідків можливих ядерних подій. Головним же елементом зі стримування і припинення збройного нападу на ядерний об'єкт є його система фізичного захисту, невід'ємною частиною якого є підрозділи з охорони.

Складність вирішення проблеми обумовлена, в першу чергу тим, що антитерористичний захист як вид діяльності, знаходиться в стадії становлення, свого часу йому не приділялася належна увага, особливо в частині розробки і комплексного аналізу питань забезпечення антитерористичного захисту об'єктів паливно-енергетичного комплексу і довгострокового прогнозування їх стану. Повертаючись до Закону України «Про боротьбу з тероризмом» можна вказати, що на його основі Кабінетом Міністрів України затверджено «Положення про єдину державну систему запобігання, реагування і припинення терористичних актів і мінімізації їх наслідків» [5]. Дане Положення визначає механізм функціонування ЕГС, запобігання, реагування і припинення терористичних актів і мінімізації їх наслідків, рівень терористичних загроз і заходів реагування суб'єктів боротьби з тероризмом на загрозу вчинення терористичного акту. Завданнями ЕГС є: запобігання терористичній діяльності, в тому числі забезпечення своєчасності виявлення та усунення причин і умов, що сприяють вчиненню терористичних актів; інформування населення про рівні загроз вчинення або вчинення терористичного акту; забезпечення безпеки об'єктів можливих терористичних посягань.

Загальновідомо, що захист об'єктів паливно-енергетичного комплексу здійснюється з вимогами чинного законодавства. Для посилення охорони цих об'єктів постійно підтримується взаємодія з територіальними

органами СБУ, МВС, Державної служби України з надзвичайних ситуацій з моніторингу ситуацій в місцях дислокації об'єктів. Однак, в даний час необхідно вживати заходів, спрямованих на забезпечення надійної охорони особливо важливих промислових об'єктів, запобігання втрат, недопущення втручання сторонніх осіб в роботу важливих для економіки держави технологічних комплексів. Також необхідно удосконалювати роботу з охорони лінійної частини та стаціонарних об'єктів магістральних трубопроводів за рахунок використання новітніх технологій, зокрема космічного та авіаційного спостереження. Оскільки космічна галузь в Україні знаходиться практично у занепаді, варто у цьому напрямку співпрацювати з міжнародними партнерами. Для розширення взаємодії доцільно створювати міжвідомчі робочі групи для відпрацювання технічних завдань, розробку цільових програм для забезпечення безпеки функціонування особливо важливих об'єктів, в тому числі лінійної частини магістральних і промислових трубопроводів.

Виходячи з вищевикладеного, можна зробити висновок, що протидія терористичним актам на об'єктах паливно-енергетичного комплексу має здійснюватися шляхом підвищення рівня ефективності та надійності захисту діючих або споруджуваних, потенційно небезпечних об'єктів, уразливих у терористичному відношенні і забезпеченні їх сталого функціонування. Однак, щоб усунути причини і умови, що сприяють розгортанню терористичної діяльності, необхідні не тільки законодавчі зміни. Питання, пов'язані з тероризмом, потрібно вирішувати, в першу чергу, на міждержавному рівні. У зв'язку з цим, необхідний комплекс спільних заходів в соціально-економічній, політичній сферах, в релігійному середовищі, пошук усунення етнічних протиріч, в інформаційному просторі та міжнародних відносинах.

На жаль, досвід протидії тероризму показує, що не може бути будь-якого надійного захисту від цього зла. Тільки спільний, всебічний комплекс загальнодержавних заходів загальної та спеціальної превенції може мінімізувати терористичні загрози.

1. *Закон України «Про боротьбу з тероризмом» від 20.03.2003 № 638-IV. [Електронний ресурс]. Законодавство України. Режим доступу: http://zakon2.rada.gov.ua/laws/show/638-15. Назва з екрану.*
2. *Про Концепцію боротьби з тероризмом: Указ Президента України від 25.04.2013р. № 230/2013 // Урядовий кур'єр. 2013 р. № 80.*
3. *Ємельянов В.П. Понятійний апарат у сфері правової протидії тероризму: теоретичне та практичне значення / В.П. Ємельянов // Форум права. 2011. № 1. С. 348-361. [Електронний ресурс]. Режим доступу:*

http://www.nbuv.gov.ua/ejournals/FP/2011-1/11evptpz.pdf. Назва з екрану.

4. *Бабосов Е. М. Боль Чернобыля // Социологические исследования. 1992. № 6. С. 14-21.*
5. *Постанова Кабінету Міністрів України від 18.02.2016 № 92 «Про затвердження Положення про єдину державну систему запобігання, реагування і припинення терористичних актів та мінімізації їх наслідків». [Електронний ресурс]. Законодавство України. Режим доступу: http://www.kmu.gov.ua/control/ru/cardnpd?docid=248852549. Назва з екрану.*

Денисова Т.А. Загрози терористичного характеру об'єктам критичної інфраструктури: від історії до сучасних реалій

Тероризм визнається світовим співтовариством як один з найнебезпечніших викликів сучасності. Події останнього часу показують, що діяльність терористичних організацій, набуваючи принципово нових рис, стає все більш витонченою і цинічною. Змінюються стратегічні напрямки силових ударів, вдосконалюється тактика сучасних терористичних угруповань. Для досягнення своїх цілей терористи все частіше вибирають мішенями не державні й військові об'єкти, не політичних лідерів, а звичайних громадян: туристів, відвідувачів магазинів, культурно-спортивних заходів, ресторанів, кафе тощо.

Протидія терористичним актам на об'єктах паливно-енергетичного комплексу має здійснюватися шляхом підвищення рівня ефективності та надійності захисту діючих або споруджуваних, потенційно небезпечних об'єктів, уразливих у терористичному відношенні і забезпеченні їх сталого функціонування. Однак, щоб усунути причини і умови, що сприяють розгортанню терористичної діяльності, необхідні не тільки законодавчі зміни. Питання, пов'язані з тероризмом, потрібно вирішувати, в першу чергу, на міждержавному рівні. У зв'язку з цим, необхідний комплекс спільних заходів в соціально-економічній, політичній сферах, в релігійному середовищі, пошук усунення етнічних протиріч, в інформаційному просторі та міжнародних відносинах.

Ключові слова: тероризм, терористичні загрози, критична інфраструктура

Denisova T.A. Threats to the terrorist nature of critical infrastructure objects: from history to current realities

Terrorism is recognized by the world community as one of the most dangerous challenges of our time. Recent events show that the activities of terrorist organizations, gaining fundamentally new features, are becoming more sophisticated and cynical. The strategic directions of power shocks are changing, tactics of modern terrorist groups are being improved. In order to achieve their goals, terrorists increasingly target not state and military objects, not political leaders, but ordinary citizens: tourists, shoppers, cultural and sporting events, restaurants, cafes, etc.

Counteraction to terrorist acts at the objects of the fuel and energy complex should be carried out by increasing the level of efficiency and reliability of protection of

existing or under construction, potentially dangerous objects, vulnerable to terrorist attacks and ensuring their sustainable functioning. However, in order to eliminate the causes and conditions conducive to the development of terrorist activities, not only legislative changes are required. Questions related to terrorism need to be resolved, first of all, at the interstate level. In this regard, a complex of joint activities in the socio-economic, political spheres, in the religious environment, the search for the elimination of ethnic contradictions, in the information space and in international relations is necessary.

Keywords: terrorism, terrorist threats, critical infrastructure

Дорохіна Ю.А.

Таврійський національний університет ім. В.І. Вернадського, професор кафедри кримінально-правових дисциплін Навчально-наукового гуманітарного інституту, д.ю.н., доцент

Dorokhina Yu.A.

Taurian National University V.I. Vernadsky, Professor of the Department of Criminal-Legal Disciplines of Educational and scientific humanitarian institute, D.Sc., associate professor

РОЗВИТОК СИСТЕМИ ЗАХИСТУ КРИТИЧНОЇ ІНФОРМАЦІЙНОЇ ІНФРАСТРУКТУРИ В УКРАЇНІ

Гарантування безпеки та стійкості національної критичної інфраструктури є приорітетним напрямом безпекової політики України, оскільки критична інфраструктура забезпечує життєвоважливі для населення, суспільства та держави опції, без яких неможливо безпечне існування та забезпечення належного рівня національної безпеки.

Критична інформаційна інфраструктура розглядається як основний компонент у критичній інфраструктурі багатьох держав, що знаходить відображення у відповідних підходах до визначення цього поняття. Головні причини критичності інформаційної складової інфраструктури випливають зі стрімкого поширення інформаційних технологій у всіх сферах нашого життя та, відповідно, до зросту уразливостей і потенційних загроз різного характеру. Очевидно, що за таких умов забезпечення безпеки кібертехнологій у критичних інфраструктурах (інфраструктурах державного управління, фінансового, банківського, транспортного, енергетичного, ресурсного, комунального та продуктового забезпечення) сучасного суспільства стає одним з головних питань.

Попри очевидну необхідність у розвитку системи захисту критичної інформаційної інфраструктури, доцільно вказати, що низка первинних (першочергових) питань до сьогодні стоять на порядку денному. До таких питань доцільно віднести й проблему відсутності поняття «критична інформаційна інфраструктура» у законодавстві як України, так і багатьох держав. Проте така ситуація пояснюється тим, що інформаційна складова входить до обсягу поняття інфраструктури взагалі (тобто критичної інфраструктури) і не виокремлюється як певна ланка. Перевагою концеп-

туального підходу, основаного на понятті – «критична інфраструктура», є можливість системного вирішення питання захисту критично важливих для життєдіяльності держави, безпеки її громадян та довкілля систем і об'єктів та створення можливостей для більш ефективного управління ризиками на глобальному, регіональному та національному рівнях.

На сучасному етапі розвиток системи захисту критичної інформаційної інфраструктури на національному рівні забезпечується поступовими кроками Уряду нашої держави щодо розробки оптимальної державної системи захисту критичної інфраструктури України. Так, Уряд прийняв Концепцію створення державної системи захисту критичної інфраструктури нашої держави (далі – Концепція), яка була розроблена Мінекономрозвитку разом з Національним інститутом стратегічних досліджень та Службою безпеки України. Нагадаємо, що 6 грудня 2017 р. розпорядженням № 1009-р Кабінет Міністрів України згадану Концепцію було схвалено.

Концепція є основою для створення державної системи захисту об'єктів критичної інфраструктури, порушення роботи яких може завдати шкоди національним інтересам України. У ній наведено визначення усіх ключових понять та запропоновано механізм взаємодії державних органів. В Уряді переконані, що створення такої системи захисту дозволить забезпечити стійкість до загроз усіх видів. Тобто Концепція закладає якісно новий рівень державного управління у цій сфері та передбачає сучасні підходи до управління безпековими ризиками, оптимізоване використання наявних ресурсів, гнучкість та швидкість реагування на інциденти та кризи.

До об'єктів критичної інфраструктури віднесено підприємства та установи, які є стратегічно важливими для функціонування економіки і безпеки держави, суспільства та населення, виведення з ладу або руйнування яких може мати вплив на національну безпеку і оборону, природне середовище, призвести до значних матеріальних та фінансових збитків, людських жертв. Термін «критична інфраструктура» вживається у такому значенні – об'єкти, системи та ресурси, фізичні чи віртуальні, що забезпечують функції та послуги, порушення яких призведе до найсерйозніших негативних наслідків для життєдіяльності населення, суспільства, соціально-економічного розвитку, обороноздатності держави та забезпечення національної безпеки.

Наступним кроком у створенні системи захисту критичної інфраструктури (у тому ж числі інформаціної) є розробка та розгляд законопроекту «Про критичну інфраструктуру та її захист», який має визначити

держоргани, відповідальні за забезпечення здійснення заходів відносно пріоритетних секторів критичної інфраструктури, у тому числі сектору телекомунікації і зв'язку.

Важливим також є активізація міжнародного співробітництва у сфері захисту критичної інфраструктури, на що поряд із посиленням спроможності національних урядів забезпечувати захист критичної інфраструктури, звертає увагу резолюція Ради безпеки ООН щодо захисту критичної інфраструктури від терористичних атак № 2341 від 13 лютого 2017 р..

Вбачається, що в сучасних умовах на перший план щодо розбудови якісної системи захисту критичної інформаційної інфраструктури для нашої держави виходить забезпечення безпеки в інформаційній сфері, тобто кібербезпеки. У зв'язку з цим 5 жовтня 2017 р. Верховна Рада України ухвалила Закон «Про основні засади забезпечення кібербезпеки України», який вступить у силу через шість місяців з дня його опублікування. Згаданий Закон є новаторським документом, оскільки закріплює на законодавчому рівні багато важливих визначень: кіберзагроза, кібершпіонаж, кіберзлочинність, кібератака, а також визначає необхідність впровадження єдиної (універсальної) системи індикаторів кіберзагроз з урахуванням міжнародних стандартів з питань кібербезпеки і кіберзахисту.

Законом передбачено, що до об'єктів критичної інфраструктури можуть бути віднесені підприємства й установи, які: ведуть діяльність і надають послуги в галузях хімічної промисловості, енергетики, транспорту, ІКТ, банківському та фінансовому секторі, електронних комунікацій; надають послуги у сфері життєзабезпечення населення; є комунальними, аварійними і рятувальними службами; включені до переліку підприємств, що мають стратегічне значення для економіки.

Цей нормативно-правовий акт відкриває нові можливості для впорядкування ситуації в інформаційній сфері. Незважаючи на тривалі дискусії і побоювання певних експертів щодо можливості появи надмірного контролю від держави в кіберсфері, цей Закон дає змогу в перспективі перевести розвиток вітчизняного інформаційного простору на якісно новий рівень [1].

Завдання захисту критичної інфраструктури зміщують фокус уваги на попередження кризових ситуацій, пов'язаних із її функціонуванням. У зв'язку з цим слід підкреслити, що до існуючих систем протидії абсолютно правильно додано й нову систему боротьби із кіберзагрозами, яка формується на виконання Стратегії кібербезпеки України. Таким чином, саме попередження кризових ситуацій має стати ключовою складовою у побудові системи заходів щодо протидії кіберзагрозами, оскільки у

сучасному суспільстві практично всі інфраструктури, які забезпечують його життєдіяльність, використовують інформаційні технології (кібертехнології), які в свою чергу відіграють критичну роль практично в будь-якій інфраструктурі.

Доцільно відмітити, що захист критичної інформаційної інфраструктури − це не просто оновлення термінів в чинному законодавстві, це впровадження нового підходу. Основними його складниками є створення безпекового партнерства між всіма зацікавленими сторонами, організація комплексної оцінки загроз такої інфраструктурі та їх впливу на рівень національної безпеки в окремих її складових, створення механізму моніторингу та попередження кризових ситуацій, що пов'язані із функціонуванням кіберпростору.

1. *Рудь І. Закон про кібербезпеку: основні положення, оцінки експертів та розвиток вітчизняного інформаційного простору [Електронний ресурс] / І. Рудь // Україна: події, факти, коментарі. – 2017. – № 19. – С. 42–48. – Режим доступу: http://nbuviap.gov.ua/images/ukraine/2017/ukr19.pdf.*

Дорохіна Ю.А. Розвиток системи захисту критичної інформаційної інфраструктури в Україні

Гарантування безпеки та стійкості національної критичної інфраструктури є приорітетним напрямом безпекової політики України, оскільки критична інфраструктура забезпечує життєвоважливі для населення, суспільства та держави опції, без яких неможливо безпечне існування та забезпечення належного рівня національної безпеки.

Критична інформаційна інфраструктура розглядається як основний компонент у критичній інфраструктурі багатьох держав, що знаходить відображення у відповідних підходах до визначення цього поняття. Головні причини критичності інформаційної складової інфраструктури випливають зі стрімкого поширення інформаційних технологій у всіх сферах нашого життя та, відповідно, до зросту уразливостей і потенційних загроз різного характеру.

Захист критичної інформаційної інфраструктури − це не просто оновлення термінів в чинному законодавстві, це впровадження нового підходу. Основними його складниками є створення безпекового партнерства між всіма зацікавленими сторонами, організація комплексної оцінки загроз такої інфраструктурі та їх впливу на рівень національної безпеки в окремих її складових, створення механізму моніторингу та попередження кризових ситуацій, що пов'язані із функціонуванням кіберпростору.

Ключові слова: критична інфраструктура, система захисту критичної інфраструктури

Dorokhina Y.A. Development of critical informational infrastructure protection system in Ukraine

The guarantee of the security and stability of the national critical infrastructure is a priority direction of the security policy of Ukraine, since critical infrastructure provides vital options for the population, the society and the state, without which it is impossible to secure the existence and ensure an adequate level of national security.

Critical information infrastructure is considered as the main component of the critical infrastructure of many countries, which is reflected in the relevant approaches to defining this concept. The main reasons for the criticality of the information component of the infrastructure stem from the rapid spread of information technology in all spheres of our lives and, accordingly, the growth of vulnerabilities and potential threats of various nature.

Protecting critical information infrastructure is not just an update of the terms in the current legislation, it is the introduction of a new approach. Its main components are the creation of a security partnership between all stakeholders, the organization of a comprehensive assessment of the threats to such infrastructure and their impact on the level of national security in its separate components, the creation of a mechanism for monitoring and preventing crises associated with the functioning of cyberspace.

Key words: critical infrastructure, critical infrastructure protection system

Житний О.О.
Харківський національний університет імені В. Н. Каразіна, завідувач кафедри кримінально-правових дисциплін, д.ю.н., професор

Zhitnyi O.O.
Kharkiv National University named after V. N. Karazin, Head of the Department of Criminal-Legal Disciplines, D.Sc., Professor

Ємельяненко В.В.
Національний юридичний університет імені Ярослава Мудрого, доцент кафедри кримінального права № 2, к.ю.н., доцент;

Yemelyanenko V.V.
National Law University named after Yaroslav the Wise, Associate Professor, Department of Criminal Law No. 2, candidate of science, associate professor

МІСЬКИЙ ПІДЗЕМНИЙ ТРАНСПОРТ МЕГАПОЛІСУ ЯК ОБ'ЄКТ КРИТИЧНОЇ ІНФРАСТРУКТУРИ (КРИМІНОГЕННІСТЬ ТА КРИМІНОЛОГІЧНА БЕЗПЕКА)

Транспортна інфраструктура великого міста є розгалуженим, складним комплексом матеріальних об'єктів, транспортних засобів, засобів зв'язку, програмного забезпечення, трудових, фінансових і земельних ресурсів. Одним із її важливих елементів є метрополітен. Сьогодні в Україні ці транспортні системи мають три мегаполіси – міста Дніпро, Київ та Харків.

Метрополітен є складовою єдиної транспортної системи, видом міського електричного транспорту, призначеного для перевезення громадян за встановленими маршрутами. Критерії, сформульовані Міжнародним союзом громадського транспорту (Union Internationale des Transports Publics) дозволяють вказати, що метрополітен – це: а) залізниця, б) призначена бути складовою частиною мережі, що дозволяє перевозити велику кількість пасажирів в межах урбанізованої зони; в) на рейкових транспортних засобах із зовнішнім управлінням; г) що знаходиться у просторі, який повністю перебуває в її користуванні; д) цілком або частково розташована у тунелях. З урахуванням цих загальних характеристик метрополітену слід наголосити на тому, що як об'єкт критичної інфра-

структури (регіонального масштабу) й вид громадського транспорту він є не лише джерелом підвищеної небезпеки в загальному розумінні останнього. Йому притаманні й такі властивості, які сприяють можливості вчинення кримінальних правопорушень. Одні з таких криміногенно значимих чинників тотожні загрозам, які генеруються в ході експлуатації будь-якого виду транспорту (зокрема, залізничного й громадського), інші – близькі до криміногенних небезпек, характерних для місць постійного великого скупчення людей, а деякі – специфічні.

По-перше, криміногенно небезпечною є висока концентрація людей (пасажирів) на площах, об'єктивно обмежених фізичними параметрами внутрішніх приміщень метрополітену й вагонів потягів (так, щодобовий обсяг перевезень Харківського метрополітену становить понад 550 тис. пасажирів, щорічно він перевозить близько 210 млн. пасажирів, а за всю експлуатаційну діяльність підприємства було перевезено майже 9 млрд. пасажирів). Зазначена обставина вимагає належної організації безпечного перебування й переміщення людей у приміщеннях, запобігання злочинам і правопорушенням, які можуть заподіювати шкоду особі, власності, громадському порядку, громадській безпеці.

Найбільш відомими у світі злочинами, які скоювалися на територіях метрополітенів, є терористичні акти, в яких злочинці використовували саме вказану вище особливість цього вижду транспорту. Перший в історії терористичний акт в метрополітені було вчинено 30 жовтня 1883 р. в Лондоні: 40 пасажирів потягу метро одержали поранення поблизу станції «Пред-стріт» (Praed Street, нині Paddington), коли невідомий кинув вибуховий пристрій з вікна вагону першого класу у вікно вагону третього класу. У метрополітенах колишнього СРСР перший терористичний акт було вчинено 8 січня 1977 р. в Москві. Вибухові пристрої спрацювали в потягу метро між станціями «Ізмайлівська» і «Першотравнева». В результаті загинуло 7 людей. Одним з найбільш відомих терористичних актів в метро відбувся 20 березня 1995 року в Токіо. Члени екстремістської релігійної організації «Аум Синрикьо» розпилили нервово-паралітичну речовину зарин у п'яти потягах метрополітену. У результаті загинуло 13 осіб, істотно постраждали 50, тимчасовий розлад здоров'я одержали майже 1 тис осіб, за медичною допомогою звернулися майже 6,3 тис. людей.

По-друге, слід вказати на високі швидкості переміщення транспортних засобів – локомотивів та вагонів метрополітену. Звідси – висока інертність цих об'єктів, зменшення ступеню їх підконтрольності при гальмуванні та виконанні маневрів, що є небезпечними факторами при їх експлуатації. Наприклад, довжина гальмівного шляху (для порожнього

й для навантаженого режимів) під час гальмування восьмивагонного й менше составів до повного зупинення при швидкості на початку гальмування 80 км/год становить від 150 до 350 метрів (залежно від типу вагону та гальмівного пристрою). Зазначена властивість зумовлює небезпеку заподіяння суспільно небезпечних наслідків (загибель людей, заподіяння шкоди здоров'ю, майнові збитки) від зіткнень і сходжень з рейок рухомого складу, пошкодження колій і споруд, пристроїв електропостачання, електромеханічних пристроїв. Такі наслідки можуть виникнути перш за все унаслідок порушення правил безпеки руху працівниками метрополітену, порушення правил ремонту чи експлуатації відповідних механізмів (зокрема, локомотивів), встановлення протиправного контролю за цим транспортним засобом (наприклад, його захоплення, викрадення, перехоплення управління шляхом втручання в роботу комп'ютерних систем тощо), а також порушення правил користування метрополітеном пасажирами, а також умисного використання вказаних властивостей для заподіяння шкоди особі (наприклад, потерпілого умисно штовхають на рейки).

Третьою криміногенно значимою обставиною є простий і швидкий доступ до отримання послуги перевезення метрополітеном. Він не передбачає ідентифікації клієнта (документ, що посвідчує особу, надається нею лише у випадках користування пільгою на проїзд). Тому потяги метро є не лише швидким, зручним і дешевим засобом проїзду з одного в інший район міста, але і засобом перевезення загальнонебезпечних предметів, предметів і речовин, заборонених у обігу (зброя, боєприпаси, вибухові і легкозаймисті речовини, вибухові пристрої, наркотичні засоби, психотропні речовини). Втім, сама наявність деяких із цих речовин значно посилює криміногенну небезпеку на аналізованому об'єкті. Це передусім стосується занесення на територію метрополітену вибухових, горючих, отруйних речовин. Так, в світовій статистиці злочинів, які вчинялися в метро, найбільшу кількість жертв спричинив не терористичний акт чи диверсія, а дії самовбивці, який 18 лютого 2003 р. в м. Тегу (Південна Корея) намагався покінчити з собою в потягу. Він проніс каністру із легкозаймистою рідиною і запалив її у вагоні під час руху потяга по станції. У пожежі загинуло 192 людини, 152 отримали поранення.

Четвертий криміногенно небезпечний чинник визначається перебуванням великої кількості людей і матеріальних цінностей на глибині від кількох до кількох десятків метрів, що вимагає дотримання вимог безпеки експлуатації приміщень, будівель, споруд, колій, убезпечення їх від руйнуючої дії природних і техногенних факторів.

П'ята криміногенно значима обставина – висока вартість майна, земельних ресурсів, які належать метрополітену, обіг значної кількості фінансових ресурсів в діяльності підприємства, що характеризує їх як потенційні предмети посягань, спрямованих проти власності.

Очевидно, наведений перелік не є завершеним і в ході подільних досліджень його може бути продовжено.

Згідно з даними МВС України, стан правопорядку в Харківському метрополітені сьогодні підтримується на досить високому рівні. Так, у 2017 р. за фактами вчинення злочинів на його території (у вестибюлях, на платформах, у вагонах потягів, в переходах, на станціях, на ескалаторах, на сходах, біля станцій, біля виходів) почато 160 кримінальних проваджень. Найпоширенішими злочинами були: крадіжка (48 проваджень), зберігання наркотичних речовин (42 провадження), умисне легке тілесне ушкодження (20 проваджень), незаконне зберігання зброї (16 проваджень). Водночас, спроба оцінити метрополітен як «джерело підвищеної кримінологічної небезпеки» призводить до висновків про надзвичайну важливість вдосконалення системи забезпечення антикримінальної безпеки цього об'єкта, тобто утримання його у такому стані, який би виключав або унеможливлював чи мінімізував можливість вчинення злочинів як проти осіб, які перебувають на його території, так і проти його технічних, матеріальних і віртуальних складових.

Спеціальні заходи забезпечення кримінологічної безпеки в метрополітені мають бути спрямовані як на усунення загальних криміногенних загроз, так і на мінімізацію загроз специфічних. Їхнє ранжування дозволяє стверджувати, що наразі найбільшою суспільною небезпекою характеризується вчинення терористичних актів та диверсій у метрополітені. Як об'єкт критичної інфраструктури це підприємство (його матеріальні і віртуальні компоненти) можуть бути предметом таких злочинів, як диверсія, умисне (необережне) пошкодження чи знищення майна в особливо великих розмірах тощо. Очевидно, що масовість користування метрополітеном вимагає широкого використання перш за все технічних засобів контролю й нагляду. Для попередження правопорушень на території метрополітену, вчинюваних пасажирами, станції та вагони мають бути обладнані відеонаглядом із функцією розпізнавання обличчя (як відомо, наявності камер спостереження – сам по собі вагомий стримуючий фактор). У свою чергу, це вимагає створення бази даних осіб, які обґрунтовано підозрюються у причетності до злочинів проти громадського порядку чи громадської безпеки, чи у вчиненні злочинів на території метрополітену. Таким чином, мають бути поєднані можливості техніки із досві-

дом фахівця з безпеки. Для запобігання таким криміногенним загрозам, як терористичний акт, хуліганство, перевезення небезпечних предметів і речовин тощо всі входи до станцій метрополітену обов'язково мають бути обладнані детекторами радіоактивних і вибухових речовин, індикаторами диму, арочними мобільними багатозонними металошукачами. Доцільно забезпечити кнопки виклику поліції на станціях й у вагонах.

Практика проведення оглядів всіх пасажирів на вході до метрополітену навряд чи є ефективною. Зокрема, таким чином певний час діяли зарубіжні правоохоронці (у Петербурзі й Лондоні). Однак, від такого заходу довелося досить швидко відмовитися (виявилося, що в такому разі в десятки разів знижується пропускна здатність цього виду транспорту, виникають тисячні черги пасажирів, що зумовлює затримки роботи підприємства, невдоволення клієнтів та втрату прибутку). Тому, наприклад, у Петербурзі поліція перейшла на здійснення вибіркових оглядів. У Великобританії після теракту 7 липня 2005 року, коли було вбито 52 людини і більше 700 було поранено, почали проводитися повні огляди, стало більше охоронців. Було впроваджено спеціальні камери стеження, які реагували на залишені без догляду речі, видаючи сигнали тривоги. Через рік було утворено спеціальний підрозділ, який об'єднав оперативних працівників поліції, співробітників метрополітену та слідчих у сили антитерористичного реагування. Втім, досить швидко правоохоронні органи визнали, що заходи безпеки не мають 100-відсоткоої гарантії виявлення правопорушника. Тому слідчі сконцентрувалися не стільки на заходах безпеки, а на відстежу ванні дій потенційних терористів.

Для запобігання заподіяння шкоди життю і здоров'ю людей у випадку надзвичайних подій не території метрополітену (особливо це стосується тієї частини пасажирів, які перебувають на перонах, у вестибюлях) важливе значення має поінформованість пасажирів про раціональну поведінку під час таких ситуацій. Відомі випадки, коли більше жертв заподіював не сам терористичний акт, а паніка пасажирів.

Житний О.О., Ємельяненко В.В. Міський підземний транспорт мегаполісу як об'єкт критичної інфраструктури (криміногенність та кримінологічна безпека)

Транспортна інфраструктура великого міста є розгалуженим, складним комплексом матеріальних об'єктів, транспортних засобів, засобів зв'язку, програмного забезпечення, трудових, фінансових і земельних ресурсів. Одним із її важливих елементів є метрополітен. Сьогодні в Україні ці транспортні системи мають три мегаполіси – міста Дніпро, Київ та Харків.

Метрополітен є складовою єдиної транспортної системи, видом міського електричного транспорту, призначеного для перевезення громадян за встановленими маршрутами.

Для запобігання заподіяння шкоди життю і здоров'ю людей у випадку надзвичайних подій не території метрополітену (особливо це стосується тієї частини пасажирів, які перебувають на перонах, у вестибюлях) важливе значення має поінформованість пасажирів про раціональну поведінку під час таких ситуацій.

Ключові слова: міський підземний транспорт, критична інфраструктура

Zhitny O.O., Yemelianenko V.V. Urban Underground Transport of Megapolis as an Object of Critical Infrastructure (Criminogenicity and Criminological Security)

The transport infrastructure of a large city is a branched, complex complex of material objects, vehicles, communication facilities, software, labor, financial and land resources. One of its important elements is the subway. Today in Ukraine these transport systems have three metropolitan areas: the cities of Dnipro, Kyiv and Kharkiv.

The subway is part of a unified transport system, a kind of urban electric transport, designed to carry citizens along established routes.

In order to prevent damage to life and health of people in the event of an emergency, it is not the territory of the subway (especially with regard to the part of passengers on platforms, in the lobbies), the awareness of passengers about rational behavior in such situations is important.

Key words: urban underground transport, critical infrastructure

Орловська Н.А.

Національна академія Державної прикордонної служби України імені Богдана Хмельницького, професор кафедри кримінального права та процесу, д.ю.н., професор

Orlovska N.A.

National Academy of the State Border Guard Service of Ukraine named after Bogdan Khmelnytsky, Professor of the Department of Criminal Law and Process, D.Sc., Professor

ДЕЯКІ ПИТАННЯ ВИЗНАННЯ РІШЕНЬ ЄСПЛ ЯК СУДОВИХ ПРЕЦЕДЕНТІВ У КРИМІНАЛЬНОМУ ПРАВІ УКРАЇНИ

Визначеність із питанням судового прецеденту у кримінальному праві сьогодні стає надзвичайно важливою, адже годі сподіватися на формування універсальних законодавчих приписів: позитивне право вимушено підходить до різних людей з однією міркою, тому воно не може охопити усі конфліктні ситуації, що мають місце в житті. На відміну від нормативних установлень судовий прецедент – це намагання максимально наблизити право (а не лише закон!) до потреб учасників правовідносин.

Прецедентом слід вважати досвід застосування законодавства, виражений у рішеннях вищих судових органів або судів, єдиних у своєму роді, по конкретних справах. Прецедентне рішення має відповідати низці ознак, серед яких, зокрема, формування та функціонування прецеденту на основі чинного законодавства, спрямованість на ліквідацію пробілів у праві та однакове тлумачення оціночних понять у законодавстві, писаний (офіційний) характер прецеденту тощо.

Важливо розрізняти правову позицію вищої судової інстанції та прецедент:

правова позиція – це зауваження суду щодо певної обставини/сукупності обставин у кримінальному провадженні (зокрема, правовою позицією можна вважати думку Пленуму Верховного Суду України, виражену у постанові від 06.04.2001 р. стосовно достовірності показань потерпілого та свідків);

прецедент містить правоположення - якісно нове правило у регулюванні відносин. Рішення стають правоположеннями, коли набувають обов'язкового характеру, забезпечуються авторитетом вищого судового

органу, його здатністю відміняти всі ті рішення, що суперечать цим право положенням (прикладом прецеденту можна вважати правоположення щодо специфіки встановлення малозначності, викладене у постанові Верховного Суду України у праві №5-221кс15 від 24.12.2015 р.). Окрім власне висновку відповідної судової інстанції, прецедентне значення мають доводи й обґрунтування, що містять відповідні правоположення.

У кримінальному праві переважно маємо справу з обов'язковим прецедентом тлумачення, який утворює правила правозастосування, що є обов'язковими при вирішенні всіх аналогічних справ. Ці правила є зобов'язальними приписами, які виступають невід'ємною частиною кримінально-правового регулювання.

Особливу увагу доцільно приділити питанню щодо прецедентного значення рішень ЄСПЛ.

Ратифікувавши Конвенцію про захист прав людини і основоположних свобод 1950 року та низки протоколів, Україна визнала обов'язковою юрисдикцію ЄСПЛ в усіх питаннях, що стосуються тлумачення і застосування Конвенції. На підставі ст.17 Закону України «Про виконання рішень та застосування практики Європейського суду з прав людини» суди застосовують при розгляді справ Конвенцію про за¬хист прав людини та основоположних свобод від 04.11.1950 р. та практику ЄСПЛ як джерело права. Цей прямий припис не містить будь-яких галузевих виключень.

При цьому слід звернути увагу на два аспекти:

держави не можуть відмовитись від дотримання міжнародного договору на тій підставі, що він суперечить національному праву (ст.ст. 27, 46 Віденської конвенції про право міжнародних договорів). Обов'язкове врахування норм міжнародного права також випливає зі ст. 9 Конституції України та ч. 1 ст. 19 Закону «Про міжнародні договори України». Однак суди можуть враховувати лише ту прецедентну практику ЄСПЛ, яка не суперечить Конституції України (згідно ст.9 Конституції України укладення міжнародних договорів, які суперечать Конституції України, можливе лише після внесення відповідних змін до Конституції України);

Оскільки Україна визнає юрисдикцію ЄСПЛ в усіх питаннях, що стосуються тлумачення і застосування ЄКПЛ, то обов'язковими для врахування є рішення не тільки щодо України, а й щодо інших держав.

Однак виникає питання у тому разі, коли рішення ЄСПЛ суперечать положенням кримінального законодавства у частині визнання певного діяння як злочинного, його караності, та інших обставин пов'язаних із кримінальною відповідальністю – чи є такі рішення прецедентами? якщо так, як вони співвідносяться з ч.3 ст.3 КК?

Вбачається, у таких випадках слід зважати на дві обставини:

1. ЄСПЛ постійно наголошує на необхідності зважати на специфічність, неповторність конкретної ситуації у різних державах, якщо вирішується питання про те, дотримано певне право або порушено, тобто Конвенція тлумачиться обов'язково у світлі актуальних умов сьогодення, тобто тих, які існують в конкретній державі на момент розгляду конкретної справи.

2. ЄСПЛ широко застосовує автономне тлумачення, яке полягає в тому, що ЄСПЛ не вважає обов'язковим для себе те значення, яке певний термін має в рамках правової системи окремої держави, що є стороною Конвенції. Прикладом можуть бути справи «Гурепка проти України», «Надточій проти України», «Корнєв і Карпенко проти України», у яких термін «кримінальне правопорушення» ЄСПЛ застосував до адміністративних та митних деліктів. При цьому ЄСПЛ виходив з таких обставин як суворість правообмежень, яким було піддано особу («в силу суворості санкцій дана справа є кримінальною» - «Гурепка проти України», у якій йшлося про застосування до позивача адміністративного арешту терміном 7 діб), як системний зв`язок митного та кримінального права («в силу пов'язаності між собою митних та кримінальних правопорушень дана справа є кримінальною» - «Надточій проти України»).

Чи можна, з огляду на це, вважати, що ЄСПЛ суттєво розширив межі кримінально-правового регулювання як щодо кола правовідносин, які можуть бути об`єктами кримінально-правової охорони/об`єктами злочинів, так і щодо кола покарань? На наш погляд, ні. Акцент було зроблено на захисті прав людини та її основоположних свобод у тих сферах, які межують з кримінально-правовою за характером суспільної небезпечності правопорушень та суворістю правообмежень. Саме в силу наближеності до кримінально-правового регулювання, до способів кримінально-правового впливу в зазначених галузях особа, винна у вчинені відповідних правопорушень, потребує додаткового захисту.

Іншими словами, у випадках, що наведені, рішення ЄСПЛ входять в джерельну базу адміністративного та митного, але не кримінального права.

Поряд із цим доречно поставити питання по тих випадках, коли прецедентне рішення ЄСПЛ просто не може бути застосоване національними судами. Для прикладу візьмемо рішення «Ласло Маг`яр проти Угорщини» (від 20.08.2014 р.), у якому зазначено, що довічно ув'язнений має право знати на самому початку свого строку, що він має робити для того, щоб стосовно нього було розглянуто питання про дострокове звільнен-

ня, за яких умов такий перегляд має бути здійснений, включаючи, коли він буде чи може бути здійснений. При цьому ЄСПЛ висловив сумнів у тому, що інститут президентського помилування сам по собі (якщо він не доповнений правом на умовно-дострокове звільнення) відповідає ст.3 Конвенції.

Але зрозуміло, що застосування у якості прецеденту такого рішення – взагалі не справа суду. На цьому наголошує ЄСПЛ, який у п.71 свого рішення зазначає, що «зазначена справа розкриває системну проблему… Характер порушення ст.3 Конвенції свідчить про те, що для належного виконання даного рішення держава-відповідач має реформувати, бажано законодавчими засобами, систему перегляду довічного позбавлення волі».

Таким чином, у даному випадку маємо правоположення, яке на сьогодні не може застосовуватися без відповідної процедури імплементації в національне кримінальне законодавство України (воно відноситься до категорії несамовиконуваних). І оскільки пріоритет міжнародного права над національним «зв'язує» не лише правозастосувача, а й законодавця, слід поставити питання про перегляд ст.81 КК у контексті зазначеного рішення ЄСПЛ. З цього випливає, що це рішення має ознаки нормативного прецеденту, який змінює обсяг кримінально-правового регулювання.

Але у переважній більшості рішення ЄСПЛ – це обов'язковий прецедент тлумачення, що фактично утворює правила правозастосування. При цьому обов'язковим для українського правозастосувача при застосуванні кримінально-правових норм є не тільки саме підсумкове рішення (тобто рішення в цілому) ЄСПЛ по тлумаченню конвенційних положень, але й правова позиція ЄСПЛ, покладена в основу такого рішення.

Орловська Н.А. Деякі питання визнання рішень ЄСПЛ як судових прецедентів у кримінальному праві України

Визначеність із питанням судового прецеденту у кримінальному праві сьогодні стає надзвичайно важливою, адже годі сподіватися на формування універсальних законодавчих приписів: позитивне право вимушено підходить до різних людей з однією міркою, тому воно не може охопити усі конфліктні ситуації, що мають місце в житті. На відміну від нормативних установлень судовий прецедент – це намагання максимально наблизити право до потреб учасників правовідносин.

Рішення ЄСПЛ – це обов'язковий прецедент тлумачення, що фактично утворює правила правозастосування. При цьому обов'язковим для українського правозастосувача при застосуванні кримінально-правових норм є не тільки саме підсумкове рішення (тобто рішення в цілому) ЄСПЛ по тлумаченню кон-

венційних положень, але й правова позиція ЄСПЛ, покладена в основу такого рішення.

Ключові слова: прецедент, рішення ЄСПЛ

Orlovskaya N.A. Some issues of recognition of decisions of the ECtHR as judicial precedents in the criminal law of Ukraine

Determination of the issues of the judicial precedent in criminal law today is becoming extremely important, since one can not hope for the formation of universal legislative requirements: positive law is forced to approach different people with one measure, so it can not cover all the conflicting situations that take place in life. Unlike normative settings, the judicial precedent is an attempt to bring the right to the rights of the participants of the legal relationship as close as possible.

The ECtHR judgment is a mandatory precedent for interpretation, which in fact forms rules of law enforcement. At the same time, the mandatory application of criminal law for a Ukrainian legal practitioner is not only the final decision (that is, the decision as a whole) of the ECtHR on the interpretation of the Convention's provisions, but also the legal position of the ECtHR, which is the basis of such a decision.

Key words: precedent, decisions of the ECtHR

Фріс П.Л.

доктор юридичних наук, професор, завідувач кафедри кримінального права навчально-наукового юридичного інституту ДВНЗ «Прикарпатський національний університет ім.В.Стефаника», Заслужений діяч науки і техніки України, Академік АН ВО України

Fris P.L.

Doctor of Law, Professor, Head of the Department of Criminal Law at the Educational and Scientific Law Institute of the Precarpathian National University named after V. Stefanyk, Honored Worker of Science and Technology of Ukraine, Academician of the Academy of Higher Education of Ukraine

ПРЕЦЕДЕНТ У КРИМІНАЛЬНОМУ ПРАВІ УКРАЇНИ – ПРОБЛЕМНІ ПИТАННЯ

Будучи, як юрист, сформованим у радянській системі юридичної освіти, автор тривалий час не замислювався над питанням про джерела кримінального права, вважаючи, що нормативний акт є найдосконалішим його джерелом. Радянська теорія кримінального права не визнавала прецедент, оскільки вбачала в ньому загрозу посягання на верховенство власної диктатури, у тому числі в можливостях впливати на судові рішення в кримінальних справа. Прецедент влада ототожнювала із судовим свавіллям, яким визнавалось усе, що не перебувала в кордонах «генеральної лінії партії».

Разом із цим реально прецедент існував, да і не тільки існував, а і фактично перебував «під охороною» судових органів. Правда, щоб бути чесним слід зазначити, що «радянський прецедент», як і усе радянське, був своєрідним, не тим класичним, який існує в англо-саксонські правовій родині. Радянській судовий прецедент був спрямований на убезпечення єдності правозастосування у тому його розумінні, яке відповідало пануючій ідеології.

Це забезпечувалось через обов'язковість врахування в діяльності усіх судів СРСР рішень Пленуму Верховного суду СРСР, а у союзних республіках – рішень пленумів їх Верховних судів. Однак на практиці це мало більш розширене застосування при якому обов'язковими, фактич-

но, були також рішення колегії з кримінальних справ Верховного суду по конкретним кримінальним справам, які розглядались нею або в касаційному порядку, або в порядку нагляду.

На сьогоднішній день виникає ряд питань:

а). чи потрібен прецедент національній правовій системі?

б). чи існує в Україні сьогодні прецедент?

Відповідаючи на перше питання слід зазначити, що і як науковець і як практик вважаю прецедент необхідним джерелом права. Це обумовлюється рядом обставин серед яких слід назвати: необхідність забезпечення єдності правозастосування, обмеження свавілля законодавчої влади у питаннях правотворення[1].

Як відомо, українська система права належить до континентальної системи, яка заснована на римській правовій традиції в якій закон займав пануюче місце. В англо-саксонській правовій сім'ї основним є саме судовий прецедент (хоча закон існує поруч з ним).

У чому ж різниця?

Закон розрахований на регуляцію типових ситуацій тоді як прецедент конкретний – регулює індивідуальну ситуацію з її характерними рисами і ознаками.

Так що є кращим? Напевне ні те ні друге. Кожна з цих форм має свою позитивні і негативні якості. Закон заснований переважно на дедукції, а прецедент на індукції. Тому закон мусить бути лаконічним у формулюванні, щоб була можливість інтерпретацій фактів — підведення їх під норму. Прецедент же навпаки — містить деталізовані формулювання норми, які несформульовані у вигляді дефініцій, а розлиті по тексту рішення і екстрагуються спеціалістами з правозастосування. Отже, закон — інформативно економний, але неточний у правозастосуванні, а прецедент точно описує регульовану ситуацію, але дуже неекономний щодо юридичної техніки. (А. Ю. Малєєв).

Аналіз переваг та вад обидвох систем призводить до висновку про необхідність запровадження гнучкою системи джерел, яка поєднувала б елементи статутного та прецедентного права. У такій системі закону (статуту) відводилась би роль регуляції фундаментальних питань, а пре-

1 Немає сенсу доводити, що рівень законодавчого свавілля, пов'язаного з аґравованою оцінкою можливостей кримінально-правової боротьби зі злочинністю, перетворив чинний КК України в монстра, який незрозумілий не тільки громадянам, яким він, фактично, адресований і практикам, які повинні його застосовувати, а і науковцям, у тому числі авторам його первинної редакції.

цедент би здійснював регуляцію на рівні індивідуальних типових актів поведінки.

Відповідаючи на друге питання, теж слід дати позитивну відповідь.

Почнемо з того, що фактично, прецедент вже існує в українській правовій системі.

Судовий прецедент ОФІЦІЙНО існує у нас починаючи з 2006 року, з моменту прийняття Закону України № 3477-IV від 23.02.2006 р «Про виконання рішень та застосування практики Європейського суду з прав людини». У ст. 17 названого закону прямо вказано на те, що: «... Суди застосовують при розгляді справ Конвенцію (995_004) та практику Суду як джерело права ...».

При цьому, слід особливо звернути увагу на слова «Конвенцію та практику Суду», так як завдяки такій службової частини мови, як союзу «і», застосовуючи принцип буквального тлумачення правової норми, означає, що це пов'язані між собою поняття і представляють одне ціле, невіддільна один від одного. Тобто згідно з цим буквальному визначенням, яке в Законі України, судова практика Європейського суду з прав людини, є прямим похідним, наслідком і складовою частиною Конвенції і не може існувати окремо від Конвенції про захист прав людини і основних свобод, а Конвенція не може існувати і функціонувати без відповідних рішень Європейського суду з прав людини. Додаткові підстави такого твердження міститься і в ст. 19 Конвенції про захист прав людини і основних свобод, де дослівно сказано наступне: «... Для забезпечення дотримання Високими Договірними Сторонами їхніх зобов'язань за Конвенцією та протоколами до неї створюється Європейський суд з прав людини ...».

Тому Європейський суд з прав людини і всі його рішення (практика Суду), як невід'ємна і складова частина Конвенції, має той же статус і силу, що і всі інші положення Конвенції про захист прав людини і основних свобод, яка ратифікована Законом України № 475 / 97-ВР від 17.07.97.

Таким чином, відповідно до вищезазначеного, безпосередньо беручи до уваги ст. 17 Закону України № 3477-IV, Конвенція і практика Суду (саме в цьому конкретному поєднанні), мають силу міжнародного договору, згода на обов'язковість якого було дана Верховною Радою України і які зафіксовані у відповідних статтях Законів України № 475/97-ВР від 17.07.97г. і № 3477-IV від 23.02.2006 р.

Залишається питання про оцінку в якості прецеденту рішень Великої палати Верховного Суду та рішень касаційного кримінального суду по

питанням забезпечення єдності застосування кримінального права та рішень по конкретних кримінальних справах.

Вважаємо що і на це питання слід дати позитивну відповідь. Але з деякими зауваженнями. З точки зору теорії кримінального права вони не подібні до прецедентного права, яке існує в країнах англо-саксонської правової сім'ї, де рішення суду утворює правову норму, оскільки лише конкретизує її шляхом тлумачення, а не утворює (деклароторна теорія прецедента) [1, с.45-47].

Одночасно слід зауважити, що ці рішення є орієнтиром для прийняття рішень усіма судами по конкретних справах, як, по великому рахунку, часто подібні між собою. Місцеві та апеляційні суди ніколи не приймуть рішення по кримінальній справі яке суперечить позиції Верховного Суду по подібній кримінальній справі. Таке суперечне рішення одразу буде «запрограмоване» на скасування. Таким чином рішення

в) І останнє - чи потрібний нам класичний судовий прецедент у кримінальному праві?

Впровадження судового прецеденту можливо лише при впровадження реального суду присяжних, а не тої пародії на нього, яка передбачена чинним КПК.

Впровадження судового прецеденту у кримінальному праві викличе необхідність вузької спеціалізації. В Америці в рік видається близько 500 томів рішень судів по конкретних справах, що забезпечує єдність правозастосування, а прецедент виступає в якості своєрідного гаранта законності.

При дотриманні правил вироблених у країнах з демократичною судовою гілкою влади (а маю надію, що в Україні вона, в решті-решт, буде створена), саме прецедентна система здатна стати фундаментом справедливого правосуддя.

1. Р. Кросс. Прецедент в английском праве. М., 1985. С. 45— 47

Фріс П.Л. Прецедент у кримінальному праві України – проблемні питання

Радянська теорія кримінального права не визнавала прецедент, оскільки вбачала в ньому загрозу посягання на верховенство власної диктатури, у тому числі в можливостях впливати на судові рішення в кримінальних справа. Прецедент влада ототожнювала із судовим свавіллям, яким визнавалось усе, що не перебувала в кордонах «генеральної лінії партії».

Закон мусить бути лаконічним у формулюванні, щоб була можливість інтерпретацій фактів — підведення їх під норму. Прецедент же навпаки — містить деталізовані формулювання норми, які несформульовані у вигляді дефініцій, а розлиті по тексту рішення і екстрагуються спеціалістами з правозастосування.

Отже, закон — інформативно економний, але неточний у правозастосуванні, а прецедент точно описує регульовану ситуацію, але дуже неекономний щодо юридичної техніки.

Ключові слова: прецедент, кримінальне право, джерела кримінального права

Fris P. L. The precedent in the criminal law of Ukraine is problematic issues

The Soviet theory of criminal law did not recognize the precedent, since it saw the threat of an encroachment on the supremacy of its own dictatorship, including the ability to influence judicial decisions in a criminal case. The precedent was identified by the authorities with judicial arbitrariness, which recognized everything that was not at the borders of the «general line of the party».

The law must be concise in the wording so that there is a possibility of interpreting the facts - bringing them to the norm. The precedent, on the contrary, contains detailed rules of wording, which are not formulated in the form of definitions, but are spilled in the text of the decision and extracted by law enforcement experts. Thus, the law is informatively economical, but inaccurate in law enforcement, and the precedent accurately describes the regulated situation, but very uneconomical in terms of legal technology.

Key words: precedent, criminal law, sources of criminal law

Хавронюк М.І.
доктор юридичних наук, професор, професор кафедри кримінального та кримінального процесуального права Національного університету «Києво-Могилянська академія»

Khavronuk M.I.
Doctor of Law, Professor, Professor of the Department of Criminal and Criminal Procedural Law of National University «Kyiv-Mohyla Academy»

«НЕВІДВОРОТНІСТЬ» ВІДПОВІДАЛЬНОСТІ ЗА КОРУПЦІЙНІ ЗЛОЧИНИ: СТАТИСТИКА, ЯКА НЕ БРЕШЕ

Наскільки ефективно здійснюється правоохоронна діяльність у сфері протидії корупції, неможливо виміряти і з'ясувати без детальних статистичних даних. Лише на їх основі можна говорити про успіхи чи провали у справі протидії корупції. Але, як доводить офіційна статистика, для переважної більшості латентних корупціонерів невідворотною відповідальність так і не стала.

За два роки активної діяльності НАБУ, станом на 31 грудня 2017 р., судами винесено лише 19 обвинувальних вироків у завершених цим органом провадженнях і лише близько 107 таких проваджень щодо 165 обвинувачених перебувало на цей час на розгляді в судах. Причини такої невисокої ефективності – у складному процесі становлення нового антикорупційного органу, завантаженості і залежності судів, тривалій відсутності єдиної судової практики, а головне – «палицях у колеса» НАБУ, які охоче вставляють і злочинці на високих посадах, і їхні покровителі в правоохоронних органах, навіть, як з'ясувалось у квітні 2018 року – і в Спеціалізованій антикорупційній прокуратурі. Як результат – у третині з-поміж 127 проваджень, переданих НАБУ до суду, розгляд по суті не розпочався, а у 48 провадженнях навіть не було підготовчого засідання. Деякі провадження чекають своєї черги рік-півтора [1].

За весь час діяльності НАЗК цим органом, станом на 1 березня 2018 р., направлено до судів 152 протоколи про адміністративні правопорушення, пов'язані з корупцією (статті 172-4–172-9 Кодексу України про адміністративні правопорушення. За цими протоколами судами засуджено лише 35 осіб (23,0%). Дещо кращою за цим показником є статистика

Національної поліції – цей орган виявився ефективнішим, ніж НАЗК як спеціальний антикорупційний орган: у 2017 р. Національною поліцією направлено до судів 5040 протоколів про зазначені правопорушення і за 2150 з них суди наклали стягнення (42,7%).

Водночас загальна картина щодо протидії корупції – ще більш песимістична. Рівень судимості за найбільш небезпечні і поширені корупційні злочини за останні сім років впав майже у 6 разів, зокрема: за заволодіння майном шляхом зловживання службовим становищем (частини 2–5 ст. 191 КК України) – зі 1641 засудженої особи у 2010 р. до 204 засуджених осіб у 2017 р., тобто у 8 разів, за одержання неправомірної вигоди (хабара) – з 774 осіб у 2010 р. до 218 осіб у 2017 р., тобто у 3,5 рази, а за зловживання владою або службовим становищем (ст. 364 КК України) – з 708 осіб у 2010 р. до 16 осіб у 2017 р., тобто в 44 рази!

Стрімко зростає відсоток виправданих за ці злочини. Наприклад, якщо у 2010–2012 рр. він становив від 0,2 до 1,1%, то в 2016–2017 рр. – від 4,0 до 16,7%! Це при тому, що загалом суди виправдовують не більше 0,3% всіх осіб, які постають перед судом.

В останні чотири роки серед засуджених за корупційні злочини переважна більшість звільняється від покарання (за службове зловживання – більше 90%). Серед тих, кого покарано, більшість (49,9%) отримала штраф. Незважаючи на те, що позбавлення права обіймати посади є обов'язковим додатковим покаранням за ці злочини, 10–20% засуджених залишаються на своїх посадах. Отже, вчинивши тяжкий корупційний злочин, особа може зі своїх корупційних доходів сплатити відносно невеликий штраф (наразі його максимально можливий розмір – 25,5 тис. грн.) і має можливість далі вчиняти аналогічні злочини.

Реальне позбавлення волі загрожує лише одиницям. Так, за заволодіння майном шляхом зловживання службовим становищем (частини 2–5 ст. 191 КК України) у 2017 р. засуджено до цього виду покарання лише 39 осіб, за зловживання владою або службовим становищем (ст. 364 КК України) – 2, за одержання неправомірної вигоди – 24, за її надання – 4 особи. Оскільки таке покарання схоже на випадковість, то і страху воно не викликає.

Таблиця 1. Деякі статистичні дані щодо судимості за найбільш поширені корупційні злочини (2010-2017) [2]

РОКИ	Справи закрито щодо осіб / виправдано осіб із числа тих, що постали перед судом	Засуджено осіб	у т.ч. із числа засуджених			
			засуджено до позбавлення волі / до штрафу	звільнено від покарання	засуджено до позбавлення права обіймати посади як додаткового покарання	призначено більш м'яке покарання, ніж передбачено законом
Заволодіння майном шляхом зловживання службовим становищем (частини 2–5 ст. 191 КК України)						
2010	388 (19%)/ 6 (0,3%)	1641 (80,6%)	130 (7,9%) / 122 (7,4%)	1349 (82,2%)	839 (51,1%)	394 (24,0%)
2011	569 (26,6%)[1] / 8 (0,4%)	1560 (73,0%)	215 (13,8%) / 170 (10,9%)	1104 (70,8%)	1014 (65,0%)	326 (20,1%)
2012	415 (22,7%) / 3 (0,2%)	1411 (77,1%)	263 (18,6%) / 104 (7,4%)	961 (68,1%)	978 (69,3%)	356 (25,2%)
2013	248 (18,6%) / 12 (0,9%)	1072 (80,5%)	132 (12,3%) / 104 (9,7%)	814 (75,9%)	905 (84,4%)	245 (22,9%)
2014	265 (22,9%) / 14 (1,2%)	876 (75,9%)	91 (10,4%) / 66 (7,5%)	689 (78,6%)	637 (72,7%)	149 (17,0%)
2015	163 (21,8%) / 13 (1,7%)	571 (76,5%)	59 (10,3%) / 47 (8,2%)	448 (78,5%)	446 (78,1%)	83 (14,5%)
2016	111 (26,3%) / 17 (4,0%)	294 (69,7%)	39 (13,3%) / 25 (8,5%)	208 (70,7%)	237 (80,6%)	43 (14,6%)
2017	95 (29,4%) / 24 (7,4%)	204 (63,2%)	33 (16,2%) / 6 (2,9%)	150 (73,5%)	176 (86,3%)	17 (8,3%)
Зловживання владою або службовим становищем (ст. 364 КК України)						
2010	397 (35,8%) / 4 (0,4%)	708 (63,8%)	45 (6,3%) / 85 (12,0%)	559 (79,0%)	374 (52,8%)	195 (27,5%)
2011	499 (39,6%) / 4 (0,3%)	757 (60,1%)	131 (17,3%) / 81 (10,7%)	502 (66,3%)	506 (66,8%)	169 (22,3%)
2012	370 (40,2%) / 8 (0,9%)	543 (58,9%)	79 (14,5%) / 53 (9,8%)	378 (69,6%)	390 (71,8%)	121 (22,3%)
2013	115 (25,8%) / 14 (3,1%)	317 (71,1%)	38 (12,0%) / 14 (4,4%)	253 (79,8%)	252 (79,5%)	48 (15,1%)

2014	137 (48,7%) / 11 (3,9%)	133 (47,3%)	14 (10,5%) / 9 (6,8%)	102 (76,7%)	105 (78,9%)	14 (10,5%)
2015	64 (56,6%) / 6 (5,3%)	43 (38,0%)	4 (9,3%) / 2 (4,6%)	33 (76,7%)	37 (86,0%)	1 (2,3%)
2016	46 (59,7%) / 9 (11,7%)	22 (28,6%)	0 / 1 (4,5%)	20 (90,9%)	20 (90,9%)	1 (4,5%)
2017	24 (50%)[1] / 8 (16,7%)	16 (33,3%)	2 (12,5%) / 1 (6,2%)	11 (68,7%)	13 (81,2%)	0
Прийняття пропозиції, обіцянки або одержання неправомірної вигоди службовою особою (ст. 368 КК України)						
2010	126 (13,8%) / 10 (1,1%)	774 (85,1%)	99 (12,8%) / 175 (22,6%)	488 (63,0%)	464 (59,9%)	163 (21,1%)
2011	273 (26,0%) / 9 (0,9%)	767 (73,1%)	131 (17,1%) / 182 (23,7%)	429 (55,9%)	559 (72,9%)	151 (19,7%)
2012	103 (11,7%) / 5 (0,6%)	702 (79,7%)	137 (19,5%) / 183 (26,1%)	363 (51,7%)	594 (84,6%)	130 (18,6%)
2013	49 (6,2%)/ 7 (0,9%)	731 (92,9%)	103 (14,0%) / 193 (26,4%)	420 (57,5%)	638 (87,3%)	99 (13,5%)
2014	34 (7,0%) / 11 (2,3%)	439 (90,7%)	41 (9,3%) / 134 (30,5%)	267 (60,8%)	376 (85,7%)	45 (10,2%)
2015	8 (2,0%) / 11 (2,8%)	375 (95,2%)	59 (15,7%) / 178 (47,5%)	128 (34,1%)	334 (89,1%)	30 (8,0%)
2016	18 (5,9%) / 21 (6,9%)	264 (87,2%)	30 (11,4%) / 196 (74,2%)	29 (11,0%)	238 (90,1%)	11 (4,2%)
2017	13 (5,2%) / 18 (7,2%)	218 (87,5%)	24 (11,0%) / 163 (74,8%)	16 (7,3%)	194 (89,0%)	2 (0,9%)
Пропозиція, обіцянка або надання неправомірної вигоди службовій особі (ст. 369 КК України)[2]						
2010	36 [14] (27,9%) / 0	93 (72,1%)	1 (1,1%) / 33 (91,7%)	19 (20,4%)	-	3 (3,2%)
2011	38 [4] (43,2%) / 0	50 (56,8%)	3 (6,0%) / 27 (54,0%)	18 (36,0%)	-	2 (4,0%)
2012	13 [5] (13,7%) / 0	82 (86,3%)	1 (1,2%) / 29 (35,4%)	44 (53,7%)	-	6 (7,3%)
2013	16 [11] (16,8%) / 0	79 (83,2%)	4 (5,1%) / 37 (46,8%)	34 (43,0%)	-	5 (6,3%)
2014	46 [41] (30,2%) / 1 (0,6%)	106 (69,2%)	7 (15,2%) / 38 (35,8%)	56 (52,8%)	-	12 (11,3%)

2015	42 [34] (24,0%) / 1 (0,6%)	123 (70,4%)	3 (2,4%) / 79 (64,2%)	35 (28,4%) -	5 (4,0%)
2016	25 [21] (21,0%) / 2 (1,7%)	92 (77,3%)	1 (1,1%) / 84 (91,3%)	4 (4,3%) -	1 (1,1%)
2017	19 [15] (13,4%) / 5 (3,5%)	123 (86,6%)	4 (3,2%) / 110 (89,4%)	6 (4,9%) -	0

При тому, що кількість засуджених за корупційні злочини за сім років впала на 600%, кількість слідчих та прокурорів, які їх розслідують, практично не зменшилась, а кількість кримінальних проваджень про основні корупційні злочини, що перебувають у провадженні, зменшилась лише на 8,6%.

До суду з обвинувальними актами прокурори направили: у 2015 р. – 4737, у 2016 р. – 4386 і в 2017 р. – 5606 проваджень про ці злочини. Але згідно із судовою статистикою в ці ж роки суди засудили лише: у 2015 р. – 1112 особу, у 2016 р. – 672 осіб, а в 2017 р. – 561 особу, тобто у 4–6–10 разів менше, ніж судами було одержано кримінальних проваджень (хоча лише 20% таких злочинів були груповими).

Яка насправді доля щороку зникаючих на шляху з прокуратури до суду кількох тисяч проваджень, статистиці невідомо. Але очевидним стає те, що КК України відкриває широкі можливості для «підвішування на гачок» статей про корупційні злочини багатьох осіб, а КПК України – не менш широкі можливості для їх «зняття з гачка» у корупційний же спосіб. Відтак, боротьба з корупцією є профанацією.

Із зазначеного випливають висновки про потребу запровадження єдиної (а не окремих судової та прокурорської) прозорої системи кримінальної статистики і різкого зменшення дискреції суддів, прокурорів, слідчих (зокрема через усунення корупціогенних факторів в КК і КПК України), підвищення їхньої підконтрольності та відповідальності, насамперед дисциплінарної за участі громадськості в дисциплінарних провадженнях. Без таких заходів, сама по собі заміна в процесі судової реформи одних суддів чи прокурорів на інших і звичайних судів на спеціалізовані антикорупційні суди, не здатна щось суттєво змінити в системі кримінальної юстиції.

Із того факту, що кількість засуджених за корупційні злочини за сім років впала на 600%, можна зробити висновок про теоретичну можли-

Таблиця 2. Деякі статистичні дані щодо руху кримінальних проваджень у найбільш поширених корупційних злочинах (2013-2017) [3]

	Обліковано злочинів	Злочинів, в яких повідомлено про підозру	Злочинів, за якими провадження направлені до суду з обвинувальним актом	Злочини, за якими провадження закрито за пунктами 1, 2, 4, 6 ст. 284 КПК
Заволодіння майном шляхом зловживання службовим становищем (частини 2–5 ст. 191 КК України)				
2013	13193	7926	7440 (56,4%)	5983 (45,3%)
2014	10397	5651	4892 (47,0%)	3002 (28,9%)
2015	10211	4989	3672 (36,0%)	2255 (22,1%)
2016	9787	4741	3545 (36,2%)	1641 (16,8%)
2017	10756 (з них 112 – НАБУ)	5923 (з них 6 – НАБУ)	4701 (43,7%) (з них 2 – НАБУ)	1660 (15,4%) (з них 7 – НАБУ)
Зловживання владою або службовим становищем (ст. 364 КК України)				
2013	3810	697	636 (16,7%)	6753 (177,2%)
2014	2567	312	233 (9,1%)	2352 (91,6%)
2015	3078	261	187 (6,1%)	1847 (60,0%)
2016	3360	133	99 (2,9%)	1587 (47,2 %)
2017	3995 (з них 131 – НАБУ)	248 (з них 5 – НАБУ)	189 (4,7%) (з них 2 – НАБУ)	1662 (41,6%) (з них 20 – НАБУ)
Прийняття пропозиції, обіцянки або одержання неправомірної вигоди службовою особою (ст. 368 КК України)				
2013	1683	1114	1060 (63,0%)	1687 (100,2%)
2014	1535	990	859 (56,0%)	969 (63,1%)
2015	1588	909	730 (46,0%)	985 (62,0%)
2016	1578	758	594 (37,6%)	1069 (67,7%)
2017	2086 (з них 103 – НАБУ)	680 (з них 29 – НАБУ)	481 (23,1%) (з них 9 – НАБУ)	878 (42,1%) (з них 33 – НАБУ)
Пропозиція, обіцянка або надання неправомірної вигоди службовій особі (ст. 369 КК України)				
2013	351	264	202 (57,5%)	315 (89,7%)
2014	390	282	183 (46,9%)	428 (109,7%)
2015	286	190	148 (51,7%)	389 (136,0%)
2016	430	207	148 (34,4%)	416 (96,7%)
2017	556 (з них 26 – НАБУ)	299 (з них 9 – НАБУ)	235 (42,2%) (з них 4 – НАБУ)	312 (56,1%) (з них 4 – НАБУ)

вість пропорційного скорочення кількості слідчих, а особливо прокурорів (слід нагадати, що заплановане згідно із Законом від 2 липня 2015 р. зменшення кількості прокурорів з 1 січня 2018 року до 10000 осіб було скасоване Законом від 7 грудня 2017 р., і їхня загальна чисельність може

сягати 15000 осіб – по одному на кожних 2670 осіб. Для порівняння: у 80-мільйонній Німеччині працює лише 4 тисячі прокурорів [4] – по одному на кожних 20000 осіб).

Також із Табл. 2 видно, що частка корупційних злочинів, які в 2017 р. обліковані НАБУ, в яких НАБУ повідомило про підозру і які НАБУ направило до суду з обвинувальними актами, є поки що мізерною. Так, із 5606 чотирьох основних корупційних злочинів (статті 191, 364, 368 і 369 КК), за якими провадження направлені до суду з обвинувальним актом в 2018 р., детективи НАБУ направили до суду 17 проваджень, що становить 0,3%. Крім того, ними направлено до суду ще 4 кримінальних провадження – щодо злочинів, передбачених статтями 209 і 369-2 КК. Отже, цей орган досудового розслідування свій потенціал на повну силу ще не використовує.

1. НАБУ: Зі 127 справ, переданих до суду, у третині досі не почався розгляд // https://www.pravda.com.ua/news/2018/05/2/7179279/

2. Судова статистика: https://court.gov.ua/inshe/sudova_statystyka/

3. Прокурорська статистика: https://www.gp.gov.ua/ua/stat.html

4. Хавронюк М. Прокуратура по німецькі: закону немає, а орднунг є // http://www.zakonoproekt.org.ua/prokuratura-po-nimetsjki-zakonu-nemaje-a-ordnungh-je_.aspx

Хавронюк М.І. «Невідворотність» відповідальності за корупційні злочини: статистика, яка не бреше

Наскільки ефективно здійснюється правоохоронна діяльність у сфері протидії корупції, неможливо виміряти і з'ясувати без детальних статистичних даних. Лише на їх основі можна говорити про успіхи чи провали у справі протидії корупції. Але, як доводить офіційна статистика, для переважної більшості латентних корупціонерів невідворотною відповідальність так і не стала.

Із того факту, що кількість засуджених за корупційні злочини за сім років впала на 600%, можна зробити висновок про теоретичну можливість пропорційного скорочення кількості слідчих, а особливо прокурорів (слід нагадати, що заплановане згідно із Законом від 2 липня 2015 р. зменшення кількості прокурорів з 1 січня 2018 року до 10000 осіб було скасоване Законом від 7 грудня 2017 р., і їхня загальна чисельність може сягати 15000 осіб – по одному на кожних 2670 осіб.

Ключові слова: корупційні злочини, невідворотність кримінальної відповідальності

Khavronuk M.I. «Inevitability» of responsibility for corruption crimes: statistics that are not lying

The effectiveness of law enforcement activities in the field of combating corruption can not be measured and determined without detailed statistical data. It is only on their basis that we can talk about successes or failures in the fight against

corruption. But, according to official statistics, the overwhelming majority of latent corruptors did not inevitably take responsibility.

From the fact that the number of convicted persons for corruption crimes fell by 600% over the seven years, it can be concluded that the theoretical possibility of a proportional reduction in the number of investigators, and in particular prosecutors (it should be reminded that the reduction of the number of prosecutors planned in accordance with the Law of July 2, 2015) from January 1, 2018, up to 10,000 people were repealed by the Law of December 7, 2017, and their total number can reach 15,000 people - one for every 2670 people.

Key words: corruption crimes, inevitability of criminal responsibility

Харченко В.Б.

Харківський національний університет внутрішніх справ, завідувач кафедри кримінально-правових дисциплін факультету № 6, доктор юридичних наук, професор

Kharchenko V.B.

Kharkiv National University of Internal Affairs, Head of the Department of Criminal Law Disciplines, Faculty No. 6, Doctor of Law, Professor

ОБ'ЄКТИ ПРАВА ІНТЕЛЕКТУАЛЬНОЇ ВЛАСНОСТІ ЯК ОБ'ЄКТИ КРИТИЧНОЇ ІНФРАСТРУКТУРИ: ОЦІНКА РИЗИКІВ І ЗАГРОЗ

Відповідно до п. 17 ч. 1 ст. 92 Конституції, Закон України «Про основи національної безпеки» [8] визначає основні засади державної політики, спрямованої на захист національних інтересів і гарантування в Україні безпеки особи, суспільства і держави від зовнішніх і внутрішніх загроз в усіх сферах життєдіяльності. Вказаний нормативний акт визначає національну безпеку як захищеність життєво важливих інтересів людини і громадянина, суспільства і держави, за якої забезпечуються сталий розвиток суспільства, своєчасне виявлення, запобігання і нейтралізація реальних та потенційних загроз національним інтересам. Таким чином, безпека втілює у собі всі сфери різних галузей життєдіяльності й розвитку людини, суспільства і держави та визначає їх захищеність від внутрішніх та зовнішніх загроз. Місце, роль та пріоритет кожного із елементів національної безпеки визначаються обставинами, що реально складаються у певний період часу. Національна безпека будь-якої держави являє собою системну категорію права, політичної економії та політології, що тісно пов'язана з категоріями економічної незалежності та економічного суверенітету. З свого боку, економічна безпека держави являє собою стан рівноваги і соціально-орієнтованого розвитку національної економічної системи, що досягається реалізацією сукупності форм та методів економічної політики [4].

Саме показники економічної безпеки держави відображають причинно-наслідковий зв'язок між економічною могутністю країни, її воєнно-економічним потенціалом та національною безпекою, які натепер немож-

ливо уявити без утвердження інноваційної моделі розвитку, створення і використання різноманітних об'єктів права інтелектуальної власності. Найбільш запитаним об'єктом права інтелектуальної власності, без якого не можна уявити сталий розвиток нашого суспільства та національної економіки, є програмне забезпечення. Тому у всьому світі робляться акценти захисту національної безпеки в цілому та економічної безпеки держави зокрема від кіберзлочинності. Ще Барак Обама, перебуваючи на посаді Президента США, доручив Національному інституту стандартів і технологій (National Institute of Standards and Technology, NIST) розробити стратегію та шляхи захисту інфраструктури від несанкціонованого втручання. Зазначалося, що посилення кіберзахисту спрямоване на покращення інформаційної взаємодії між урядом та промисловими структурами, апгрейд систем кібербезпеки, а також захисту інфраструктури країни [1].

Подальший розвиток ситуації у кіберпросторі засвідчив обґрунтованість таких побоювань. У третьому абзаці обвинувального висновку спеціального прокурора Роберта Мюллера, оприлюдненого 16 лютого поточного року, висунуто формальні звинувачення 13 російським громадянам і 3 організаціям, які: «... свідомо і навмисно увійшли в змову... з метою втручання в політичний і виборчий процес США, включно з президентськими виборами 2016 року» [5].

У штаб-квартирі Європолу також відкрито Європейський центр боротьби з кіберзлочинністю. Нова структура зосередила свою роботу на виявленні незаконної он-лайн діяльності, відбитті атак на електронні банківські системи, боротьбі із злочинами, що посягають на інфраструктуру та інформаційну систему в країнах ЄС [3]. Зазначене питання є настільки важливим для економічної безпеки найбільш розвинених країн світу, що у доповіді Пентагону вказується на рішучість США застосовувати військову силу для боротьби з кібернетичними загрозами національним інтересам у різних сферах, і перш за все – в галузі економічної безпеки [9].

В Україні у 2005 році між Міністерством освіти і науки України та компанією «Microsoft Ireland Operations Limited» був укладений договір про легалізацію комп'ютерних програм виробництва компанії «Microsoft» у всіх органах державної влади [2]. Згідно з п. 4 додатку 1 до цього договору, обсяги закупівель лише протягом 2005–2007 років визначалися на рівні 120 тисяч примірників комп'ютерної програми «Windows XP Professional Upgrade (Ukrainian LIP) GOVT» та 120 тисяч примірників комп'ютерної програми «Microsoft Office 2003 Win32 Ukrainian Standard GOVT» щороку. Виходячи з п'ятирічного терміну дії зазначеного догово-

ру (до 1 січня 2010 року), прогноз обсягів закупівель зазначених програмних продуктів складав 600 тис. примірників за ціною 280 дол. США за один комплект (ОС + офісний пакет), що становить 168 млн. дол. США. Відповідні домовленості між керівництвом компанії «Microsoft» та Урядом України мають місце і на сьогодні.

Окремо слід наголосити, що зазначені витрати з державного бюджету жодним чином не вирішували проблеми забезпечення ліцензійними комп'ютерними програмами. По-перше, вказаних вище двох програмних продуктів недостатньо для повноцінної роботи будь-якого комп'ютера. По-друге, через незначний термін ефективного використання комп'ютерної програми (3–4 роки), на момент закінчення строку договору вже встановлені програмні продукти потребуватимуть заміни на нові версії. І так до нескінченності, що і підтвердило керівництво держави у 2017 році. Уряди інших країн вирішують аналогічні проблеми створюючи власний інтелектуальний продукт, що дозволяє не тільки розв'язати питання на дострокову перспективу, а й залучати до створення об'єктів права інтелектуальної власності вітчизняних фахівців. Світовий досвід вказує, що оптимальним шляхом є надання різного роду податкових пільг відповідним ІТ підприємствам та їх інвесторам, суб'єктам малого бізнесу, пільгового кредитування за рахунок коштів, передбачених спеціальними державними програмами.

Саме тому прийняття Закону України «Про державну підтримку індустрії програмної продукції» [7] було спрямоване на формування в нашій державі сприятливих умов розвитку індустрії програмної продукції України, утворення високопродуктивних робочих місць, залучення інвестицій, збільшення обсягів випуску високотехнологічної продукції, стимулювання наукомісткого експорту та імпортозаміщення, реалізацію науково-технічного потенціалу України. Зазначене набуває особливої актуальності у зв'язку з тим, що на думку віце-президента незалежної дослідницької компанії FORRESTER (Нідерланди) Ендрю Паркера у Білорусі, Росії та Україні є гарні шанси збільшити свою присутність на європейському ринку програмного забезпечення [10]. Але, безумовно, така економічна політика нашої держави, спрямована на захист національної безпеки та національних інтересів України, не могла залишитися поза увагою та реагуванням з боку транснаціональних корпорацій, що сьогодні утримують монопольне становище на ринку програмного забезпечення.

Міжнародний Альянс Інтелектуальної Власності вказав на надзвичайно високий рівень «цифрового та фізичного піратства» та запропону-

вав закріпити за Україною статут «Prioriy Foreign Country», який визначатиме що країна офіційно стане «піратом № 1» у світі [6]. Разом з тим, International Intellectual Property Alliance (IIPA) є громадським об'єднанням (приватною коаліцією), заснованою у 1984 році з метою лобіювання власних інтересів в уряді США та забезпечення захисту об'єктів, охоронюваних авторським правом цієї країни, в своїх економічних інтересах. На сьогодні ця організація об'єднує понад 1900 американських компаній, що виробляють та поширюють об'єкти авторське право, і в першу чергу, ділове та розважальне програмне забезпечення. Одночасно, корпорація Microsoft заявила, що готова надати Україні суттєві знижки щодо щорічної підписки на використання її програмних продуктів, яка обійдеться нашій державі «всього» у 100 млн. грн. Якщо ж корпорація звернеться до міжнародних судів з приводу порушення її прав, мова йтиме, як мінімум, про 1 млрд. грн. [11].

Безумовно, Указ Президента Украини № 133/2017 про введення в дію рішення Ради національної безпеки і оборони України від 28 квітня 2017 року «Про застосування персональних спеціальних економічних та інших обмежувальних заходів (санкцій)» певним чином вирішив питання залежності національної безпеки України від програмного забезпечення та інтернет-ресурсів Російської Федерації. Водночас, саме питання державної системи захисту об'єктів критичної інфраструктури, пов'язане з використанням об'єктів права інтелектуальної власності інших держав, жодним чином не було вирішено. За роки незалежності в Україні не було створено ані власного програмного забезпечення, що убезпечує діяльність об'єктів критичної інфраструктури, ані власних антивірусних програм, які б мали таку саме мету, ані хоча б якої національної соціальної мережі, яка б могла використовуватися з метою убезпечення національної безпеки від втручання іноземних держав.

Наостанок, замість класичних висновків або пропозицій наприкінці доповіді, виникає бажання задати питання: «Що буде з Україною, якщо завтра з ранку жоден з комп'ютерів, обладнаних програмним забезпеченням іноземного походження, відмовиться працювати?». Фахівці-програмісти такого сценарію подальшого розвитку протистояння щодо об'єктів авторського права не виключають.

1. Барак Обама доручив розробити стандарти кібербезпеки // URL : http:// osvita.mediasapiens.ua/material/15261 (дата звернення: 17.04.2018).

2. Договір між МОН України та компанією «Microsoft Ireland Operations Limited» від 1 трав. 2005 р. // База даних «Законодавство Укра-

їни»/ВР України. URL: http://zakon.rada.gov.ua/cgi-bin/laws/main.cgi?nreg=998_216 (дата звернення: 15.04.2018).

3. Європу вирішили захистити від хакерів // Online Експрес : URL: http://www.expres.ua/video/2013/01/10/80228 (дата звернення: 15.04.2018).

4. Єрмошенко М. М. Національні економічні інтереси : реалізація і захист URL: http://nam.kiev.ua/ape/n_01_1-2/yermosh.htm (дата звернення: 17.04.2018).

5. Докази втручання Росії у вибори президента США. URL: https://www.radiosvoboda.org/a/29048425.html (дата звернення: 15.04.2018).

6. Правообладатели объявляют Украину «пиратом №1» в мире // ИАП «КОММЕНТАРИИ» : URL: http://comments.ua/ht/386840-pravoobladateli-obyavlyayut-ukrainu.html (дата звернення: 17.04.2018).

7. Про державну підтримку індустрії програмної продукції : Закон України від 16 жовт. 2012 р. № 5450-VI // Офіційний вісник України. – 2012. – № 85. – Ст. 3448.

8. Про основи національної безпеки : Закон України від 19 черв. 2003 р. № 964-IV // Відомості Верховної Ради України. – 2003. – № 39. – Ст. 351.

9. США оставляют за собой право применять военную силу для борьбы с кибер-атаками // «ZN,UA» : URL: http://zn.ua/TECHNOLOGIES/ssha_ostavlyayut_za_soboy_pravo_primenyat_voennuyu_silu_dlya_borby_s_kiber-atakami.html (дата звернення: 12.04.2018).

10. У Бєларусі, Росії та Україні є шанси // Журнал «Інтелектуальна власність» : URL: http://www.intelvlas.com.ua/2011-05-20-15-22-05/11279 (дата звернення: 10.04.2018).

11. Украину потянут в суды за «пиратство» // ИАП «КОММЕНТАРИИ» : URL: http://comments.ua/ht/378269-ukrainu-potyanut-sudi.html (дата звернення: 11.04.2018).

Харченко В.Б. Об'єкти права інтелектуальної власності як об'єкти критичної інфраструктури: оцінка ризиків і загроз

Безпека втілює у собі всі сфери різних галузей життєдіяльності й розвитку людини, суспільства і держави та визначає їх захищеність від внутрішніх та зовнішніх загроз. Місце, роль та пріоритет кожного із елементів національної безпеки визначаються обставинами, що реально складаються у певний період часу. Національна безпека будь-якої держави являє собою системну категорію права, політичної економії та політології, що тісно пов'язана з категоріями економічної незалежності та економічного суверенітету. З свого боку, економічна безпека держави являє собою стан рівноваги і соціально-орієнтованого розвитку національної економічної системи, що досягається реалізацією сукупності форм та методів економічної політики.

Саме питання державної системи захисту об'єктів критичної інфраструктури, пов'язане з використанням об'єктів права інтелектуальної власності інших держав, жодним чином не було вирішено. За роки незалежності в Україні не було створено ані власного програмного забезпечення, що убезпечує діяльність об'єктів критичної інфраструктури, ані власних антивірусних програм, які б мали таку саме мету, ані хоча б якої національної соціальної мережі, яка б могла використовуватися з метою убезпечення національної безпеки від втручання іноземних держав.

Ключові слова: інтелектуальна власність, об'єкт критичної інфраструктури

Kharchenko V.B. Objects of intellectual property rights as objects of critical infrastructure: assessment of risks and threats

Security embodies all spheres of various fields of life and development of man, society and the state and defines their security from internal and external threats. The place, role and priority of each of the elements of national security are determined by circumstances that actually form in a certain period of time. The national security of any state is a systemic category of law, political economy and political science, which is closely linked to the categories of economic independence and economic sovereignty. For its part, the economic security of the state is a state of equilibrium and socially oriented development of the national economic system, which is achieved by the implementation of a set of forms and methods of economic policy.

It is a matter of the state system of protection of objects of critical infrastructure, connected with the use of objects of intellectual property rights of other states, in any way it was not resolved. During the years of independence, Ukraine has not created any own software that protects the critical infrastructure objects or its own antivirus programs that would have the same purpose or at least a national social network that could be used to safeguard the national security from interference by foreign states.

Keywords: intellectual property, object of critical infrastructure

Шаблистий В.В.
доктор юридичних наук, доцент, професор кафедри кримінального права та кримінології Дніпропетровського державного університету внутрішніх справ

Shablysty V.V.
Doctor of Law, Associate Professor, Professor of the Department of Criminal Law and Criminology of Dnipropetrovsk State University of Internal Affairs

НЕЗАКОННИЙ/ЗАКОННИЙ ОБІГ ЗБРОЇ, БОЙОВИХ ПРИПАСІВ, ВИБУХОВИХ РЕЧОВИН ТА ВИБУХОВИХ ПРИСТРОЇВ В УКРАЇНІ ЯК ФОНОВЕ ЯВИЩЕ ДЛЯ ПОСЯГАНЬ НА ОБ'ЄКТИ КРИТИЧНОЇ ІНФРАСТРУКТУРИ

Загальновідомо, з 2007 року в Україні відсутній передбачений законом дозвіл/заборону щодо поводження зі зброєю, бойовими припасами, вибуховими речовинами та вибуховими пристроями. Мова йде про ст. 263 КК України [1], яка до 2007 року охороняла встановлений порядок обігу зброї. Враховуючи російську збройну агресію проти України, постійні замахи проросійських терористів за допомогою вибухівки та кібератак на об'єкти критичної інфраструктури (сукупності об'єктів, які є стратегічно важливими для економіки і безпеки держави, суспільства, населення та порушення функціонування яких може завдати шкоди життєво важливим національним інтересам України) [2], відсутність правового поля може звести нанівець усю запобіжну діяльність спецслужб у цій сфері.

Уже по суті академічний (такий, що має обов'язково бути у кожному підручнику з кримінального права) висновок П.Л. Фріса містить таке. Відсутність нормативного регулювання порядку обігу зброї в Україні виключає можливість суб'єкта бути ознайомленим із межами законності/незаконності власної поведінки. Відсутність усвідомлення цього свідчить про неможливість притягнення до кримінальної відповідальності, оскільки таке притягнення порушуватиме фундаментальний принцип кримінального права, яким є принцип суб'єктивного ставлення у провину. Безпосереднім об'єктом злочину, передбаченого ст. 263 КК України,

є суспільні відносини у сфері обігу зброї в Україні. Відповідно до вимог п. 7 ст. 92 Конституції України, регулювання правового режиму власності на зброю повинно бути здійснено спеціальним законом України, який зараз відсутній. Отже, об'єкт злочину, передбачений ст. 263 КК України, відсутній, а отже і склад злочину також [3].

Практика застосування ст. 263 КК України характеризується досить неоднозначними тенденціями.

Так, в Єдиному державному реєстрі судових рішень станом на квітень 2018 року мною виявлено 23 тис. 690 електронних копій обвинувальних (з низ 10 виправдувальних) вироків судів за ст. 263 КК України. Не може не звернути увагу на себе той факт, що більше 14 % з цих рішень судів – одна Дніпропетровська область, у якій тільки за 2017 рік винесено 422 рішення.

Зокрема, 06 травня 2014 року Новоодеський районний суд Миколаївської області виправдав раніше судимого (шість разів) ОСОБУ_1. Органом досудового розслідування згідно обвинувального акту, направленому до суду 14 квітня 2014 р., ОСОБА_1 обвинувачується в тому, що у невстановлені час та дату він знаходився на околиці м. Нова Одеса Миколаївської області – біля кар'єру, де на смітнику знайшов металевий виріб, ззовні схожий на холодну зброю – тонфу. В цей же час, ОСОБА_1, посягаючи на захищеність життєво важливих інтересів людини та громадянина, суспільства і держави, маючи умисел на придбання, шляхом привласнення знайденого, холодної зброї, без передбаченого законом дозволу (курсив мій – В.Ш.), підібрав вказану холодну зброю, яка складається з ударної частини, держака темляком та додаткового бокового держака [4].

Думається, що тут суд аргументував своє рішення саме відсутністю ознак носіння холодної зброї, проте боротьба правоохоронних органів за ефективність та результат своє роботи просто вражає. Важко навіть уявити реальну кількість надуманих обвинувальних вироків судів про незаконне поводження зі зброєю осіб, які вже неодноразово порушували різні кримінально-правові заборони. На жаль, виправдувальних лише 10, проте кількість та характеристика засуджених за вчинення злочину, передбаченого ст. 263 КК України, свідчить про те, що їх має в сотні разів більше.

За офіційними даними Державної судової адміністрації України, протягом 2011-2017 років за ч. 1 ст. 263 КК України виправдано 33 особи (по роках відповідно 3, 4, 1, 4, 10, 6, 7 осіб); за ч. 2 ст. 263 КК України – всього три особи (по одній особі 2012 рік, 215 рік та 2016 рік); за ч. 1 ст. 263 КК України за 2011 рік засуджено 3412 осіб; за 2012 рік – 4160 осіб;

за 2013 рік – 2117 осіб; за 2014 рік – 2315 осіб; 2015 рік – 2309 осіб; 2016 рік – 849 осіб; 2017 рік – 2106 осіб; за ч. 2 ст. 263 КК України за 2011 рік засуджено 2492 особи; за 2012 рік – 2894 осіб; за 2013 рік – 1768 осіб; за 2014 рік – 1200 осіб; 2015 рік – 729 осіб; 2016 рік – 228 осіб; 2017 рік – 557 осіб.

Як бачимо, лише протягом останніх семи років судами винесено 27 тис. 138 обвинувальних вироків, що свідчить про неповноту електронного реєстру судових рішень. Також не може не звернути увагу той факт, з 2013 року кількість засуджених зменшується в рази. Більш того, лише за у 2017 році 1604 особи були звільненні від покарання з випробуванням за ч. 1 ст. 263 КК України (більше 76 %!); з великим ступенем ймовірності стверджую, що значна частина таких рішень мали б бути виправдувальними вироками.

Так, 19.02.2018 року Печерський районний суд м. Києва виніс виправдувальний вирок за ч. 2 ст. 263 КК України. Суд констатував, що держава не вправі застосовувати до особи процесуальний примус у вигляді кримінальної відповідальності за відсутність дозволу, передбаченого законом, поки немає закону, який передбачає отримання цього дозволу. Суд приходить до висновку про відсутність наразі Закону України, який би передбачав отримання дозволу на носіння холодної зброї. Відповідно слідчий та прокурор не зазначили в обвинувальному акті, на підставі якого Закону України обвинувачений мав отримати дозвіл для носіння холодної зброї [5].

Враховуючи викладене, постає питання про спроможність спеціальних служб України запобігати посяганню на об'єкти критичної інфраструктури з метою нанести шкоду Україні – дуже часто ці злочини супроводжуються застосуванням вогнепальної зброї та різними вибуховими пристроями, обіг яких нічим не регулюється. Може мати місце ситуація, коли таких осіб неможливо буде притягнути до відповідальності навіть при їх затриманні із відповідними предметами.

Так, результати інтерв'ювання близько 300 працівників Національної поліції України (слідчих, оперуповноважених, дільничних офіцерів поліції та патрульних), які проходили курси підвищення кваліфікації та спеціалізації у Дніпропетровському державному університеті внутрішніх справ протягом лютого-квітня 2018 року свідчать про таке. Вже зараз має місце ситуація, коли від слідчого в усній формі вимагають закрити кримінальне провадження про незаконний обіг зброї, проте виключно у випадках, коди підозрюваний має належний матеріальний стан та соці-

альне положення. Стосовно інших пересічних громадян – виключно обвинувальні акти до суду.

Вважаю, що вихід можливий через застосування принципу верховенства права.

02 травня 2016 року Верховна Рада Україна прийняла два закони: «Про статус суддів та судоустрій» та «Про внесення змін до Конституції України (щодо правосуддя)». Принцип верховенства права став ключовим при здійсненні правосуддя, що надає суду по суті необмежені дискреційні повноваження, оскільки вони тепер можуть керуватися і неписаними правилами, що було неможливим при дії принципу законності [6, с. 156-157].

Отже, немає таких звичаїв українського народу як демонстративно та агресивно поводитися із зброєю, бойовими припасами, вибуховими речовинами та вибуховими пристроями. Саме таким чином можна заповнити прогалину у законодавстві – до прийняття закону України «Про зброю» суспільні відносини у сфері обігу зброї можуть регулюватися шляхом реалізації принципу верховенства права. Його також слід застосовувати виважено – так, як це зроблено у наведеному рішенні Печерського районного суду м. Києва.

Питання про загальний дозвіл на придбання короткоствольної нарізної вогнепальної зброї мною спеціально не ставилося, оскільки це предмет одвічних дискусій.

1. *Кримінальний кодекс України: Закон від 05.04.2001 р. № 2341-III. URL: http://zakon3.rada.gov.ua/laws/show/2341-14.*
2. *Концепція створення державної системи захисту критичної інфраструктури, схваленої розпорядженням Кабінету Міністрів України від 6 грудня 2017 р. № 1009-р. URL: http://ivano-frankovsk.cf/index.phtml.*
3. *Не може бути кримінальної відповідальності за незаконне поводження із зброєю (ст. 263 КК України): науковий висновок П.Л. Фріса. URL: http://kafedr.at.ua/publ/mnenie_ehksperta/ne_mozhe_buti_kriminalnoji_vidpovidalnosti_za_nezakonne_povodzhennja_zi_zbroeju_st_263_kk_naukovij_visnovok/2-1-0-418.*
4. *Матеріали Єдиного державного реєстру судових рішень. URL: http://reyestr.court.gov.ua/Review/38565132.*
5. *Матеріали Єдиного державного реєстру судових рішень. URL: http://reyestr.court.gov.ua/Review/72347132*
6. *Шаблистий В.В. Конституційні основи реформування кримінального законодавства. Становлення та розвиток правової держави: пробле-*

ми теорії та практики: матеріали VIII Всеукраїнської науково-практичної конференції. Миколаїв: НУК, 2016. С. 156-160.

Шаблистий В.В. Незаконний/законний обіг зброї, бойових припасів, вибухових речовин та вибухових пристроїв в Україні як фонове явище для посягань на об'єкти критичної інфраструктури

Враховуючи російську збройну агресію проти України, постійні замахи проросійських терористів за допомогою вибухівки та кібератак на об'єкти критичної інфраструктури (сукупності об'єктів, які є стратегічно важливими для економіки і безпеки держави, суспільства, населення та порушення функціонування яких може завдати шкоди життєво важливим національним інтересам України), відсутність правового поля може звести нанівець усю запобіжну діяльність спецслужб у цій сфері.

Немає таких звичаїв українського народу як демонстративно та агресивно поводитися із зброєю, бойовими припасами, вибуховими речовинами та вибуховими пристроями. Саме таким чином можна заповнити прогалину у законодавстві – до прийняття закону України «Про зброю» суспільні відносини у сфері обігу зброї можуть регулюватися шляхом реалізації принципу верховенства права.

Ключові слова: Незаконний/законний обіг зброї, бойових припасів, вибухових речовин та вибухових пристроїв, фонове явище, критична інфраструктура

Shablysty V.V. Illegal / lawful circulation of weapons, ammunition, explosives and explosive devices in Ukraine as a background phenomenon for attacks on objects of critical infrastructure.

Given the Russian armed aggression against Ukraine, constant attacks on pro-Russian terrorists by means of explosives and cyber attacks on critical infrastructure objects (a set of objects that are strategically important for the economy and security of the state, society, population and whose operation might cause damage to the vital the national interests of Ukraine), the absence of a legal field can nullify all preventive activities of special services in this area.

There are no such practices of the Ukrainian people as demonstrating and aggressive handling of weapons, combat supplies, explosives and explosive devices. This way it is possible to fill the gap in the legislation - before the adoption of the Law of Ukraine «On Weapons», the social relations in the sphere of arms circulation can be regulated through the implementation of the rule of law principle.

Key words: Illegal / lawful circulation of weapons, ammunition, explosives and explosive devices, background phenomenon, critical infrastructure

Юзікова Н.С.

доктор юридичних наук, доцент, професор кафедри адміністративного і кримінального права Дніпровського національного університету імені Олеся Гончара

Yusikova N.S.

Doctor of Law, Associate Professor, Professor of the Department of Administrative and Criminal Law of Dniprovsky National University named after Oles Gonchar

ПЕРСПЕКТИВИ ВИКОРИСТАННЯ ШТУЧНОГО ІНТЕЛЕКТУ У СИСТЕМІ ЗАХИСТУ КРИТИЧНОЇ ІНФРАСТРУКТУРИ В УКРАЇНІ

Актуальність кримінологічних досліджень факторів, що детермінують злочинність, загострюють криміногенну ситуацію, і відповідно пошук інноваційних ефективних заходів запобігання новим проявам злочинності у контексті сучасних глобалізаційних процесів, потужних кібератак набуває першочергового значення. Небезпека, руйнівні наслідки соціального, особистісного та техногенного характеру, які спричиняє злочинність вимагають сучасних специфічних заходів реагування та протидії.

Кризова ситуація, в якій опинилася держава, негативно впливає на зміну суспільних цінностей, розшарування населення за рівнем доходів, призводить до дисфункціональності соціальних інститутів та моральної дезорієнтації частини суспільства.

Екологічні катастрофи, загрози терористичної, екстремістської діяльності та радикалізації терористичного руху, кіберзлочинність негативно відзеркаліються на функціонуванні об'єктів критичної інфраструктури держави, а відповідно на рівні безпеки суспільства. Це, у свою чергу, потребує особливої уваги з боку держави до своєчасного виявлення ризиків, загроз і забезпечення невідкладного реагування на них, а також формування належної системи захисту критичної інфраструктури, що ґрунтується на відповідному інформаційному полі, має належне правове та технічне забезпечення.

Чим більше інформації у арсеналі правоохоронних органів та наукової спільноти, тим краще розуміння природи небезпеки, вчасного визначення загроз і ризиків та більше можливостей для особливих заходів системи захисту критичної інфраструктури в Україні та світі.

Залучення України до міжнародного обміну інформацією щодо критичних інфраструктур є прийнятним для української превентивної діяльності. Це сприятиме своєчасному розпізнанню загроз, які з'явилася у зв'язку із стрімким розвитком технологій, активною міграцією та ризиками окремих радикально налаштованих громадян, терористичних груп та угрупувань.

Підґрунтя ефективного захисту критичних інфраструктур, відповідно до Директиви «Про європейські критичні інфраструктури та заходи по їх захисту» від 08.12.2008 року, становить розробка загальних методик ідентифікації та класифікації ризиків, загроз та уразливих місць у активах інфраструктури. Крім того їх захист потребує взаємодії, координації і співробітництва на національному рівні та на рівні держав-членів ЄС [1]. Принципи запровадження Європейської програми захисту критичної інфраструктури охоплюють: субсидіарність, взаємодоповнення, конфіденційність, співробітництво, пропорційність, поетапний підхід [2] Крім того, Європейська Комісія рекомендувала країнам ЄС вжити низку заходів спрямованих на захист критичної інфраструктури, більшість з яких знайшли відображення у Концепції створення державної системи захисту критичної інфраструктури, схваленій розпорядженням Кабінету Міністрів України від 6.12.2017р.

Аналізуючи правове забезпечення захисту критичної інфраструктури європейських країн Д.Бірюков зазначає, що на сьогодні концепція захисту критичної інфраструктури імплементована як в загальноєвропейському законодавстві, так і в національних законодавствах окремих країн – членів ЄС. Загальноєвропейською критичною інфраструктурою вважається та, що має транскордонне, в межах ЄС, значення [3]. При цьому, автор слушно зауважує, що Україна за своїм географічним розташуванням є частиною енергетичного та транспортного панєвропейського простору та відповідно пов'язана із європейською критичною інфраструктурою, що відкриває можливості для співпраці у сфері захисту критичної інфраструктури між вповноваженими органами влади України та країн ЄС.

Відповідно до постанови Кабінету Міністрів «Про затвердження порядку формування переліку інформаційно-телекомунікаційних систем об'єктів критичної інфраструктури держави» від 23.08.2016р. під критичною інфраструктурою розуміється сукупність об'єктів інфраструктури держави, які є найбільш важливими для економіки та промисловості, функціонування суспільства та безпеки населення і виведення з ладу або руйнування яких може мати вплив на національну безпеку і оборону,

природне середовище, призвести до значних фінансових збитків та людських жертв.

Критична інфраструктура США - це основа, на якій базуються економіка, безпека і здоров'я країни. Критична інфраструктура підтримує американський спосіб життя і зміцнює національну конкурентоспроможність. Інфраструктура зберігає здорову економіку, утримуючи мільйони працюючих і підтримуючи й розвиваючи інноваційні технології сприяє поліпшенню добробуту американців. Інфраструктура країни складається з 16 секторів. Найбільш важливими є об'єкти, що стосуються сфери водопостачання, енергетики, транспорту і палива. Національна інфраструктура (Nation) також включає кібер-технологію. Департамент внутрішньої безпеки США наголошує, що значна кількість активів інфраструктури США наближається до кінця їх запланованих термінів життя. Скорочення бюджету в федеральних, державних і місцевих органах влади обмежує фінансування для інспекцій інфраструктури, технічного обслуговування, модернізації і ремонту. У деяких критично важливих секторах інфраструктури нестача робочої сили в найближчі десятиліття, ймовірно, буде заважати зусиллям, спрямованим на впровадження і підтримку критичної модернізації інфраструктури. Ризик відмови в системах транспортування, енергії, води та стічних вод, а також в секторах гребель, швидше за все, зросте протягом наступних 10 років. При цьому, забезпечення безпеки і стійкості критично важливої інфраструктури є національним пріоритетом, який вимагає планування і координації державного управління та приватного сектора на всіх рівнях. Поліпшення доріг, мостів, водних систем, електричних мереж та інших життєво важливих інфраструктурних систем вимагає інновацій, інвестицій та спільних зобов'язань [4].

Ефективний захист передбачає використання новітніх технологій та останніх інноваційних досягнень людства. До яких безперечно належить розвиток и запровадження у різні сфери штучного інтелекту. Дослідження та інтеграція зарубіжного досвіду у цій сфері є найкращою інвестицією у формування вітчизняних форм і напрямів захисту критичної інфраструктури в Україні, сприятиме своєчасному виявленню ризиків, загроз.

Штучний інтелект визначається як наука та технологія, що охоплює автоматизацію розумної поведінки та пов'язана зі створенням інтелектуальних машин, комп'ютерних програм. Метою штучного інтелекту виступає створення технічних систем, які здатні вирішувати завдання не розрахункового характеру і виконувати дії, що вимагають переробки змістовної інформації притаманної людській розумовій діяльності. Одним з важливих завдань штучного інтелекту є створенні інтелектуальних

роботів здатних автономно здійснювати операції по досягненню цілей, поставлених людиною із можливістю корективи дій.

Кібербезпека виступає базовим фактором у сучасній системі захисту критичної інфраструктури. Кібератака у травні минулого року «WannaCry» слугувала нагадуванням про небезпеку, що створюється шкідливими програмами та спричинила мільйонні збитки [5]. Захист критичної національної інфраструктури особливо важливий, оскільки вдала кібератака на об'єкти критичної інфраструктури таких галузей як енергетика, хімічна промисловість, транспорт, екологія, продовольство та інші стратегічно важливі для функціонування економіки і безпеки держави, суспільства й громади сфери, впливає на національну безпеку і оборону, природне середовище та може призвести до фінансових збитків та людських жертв. Важливо зауважити, що у сучасному світі руйнівні наслідки кіберзагроз продовжують зростати. Крім того, глобальний вплив онлайн-ресурсів, мережі Інтернет та її складових представляє зростаючий масив ризиків та уразливих місць у активах інфраструктури для кіберзлочинців, які можуть їх використовувати.

Thales AI-powered Cybels Sensor tool забезпечує сучасний захист від кібератак на об'єкти критичної інфраструктури. Cybels Sensor шляхом умонтування штучного інтелекту постійно спостерігає за будь якими джерелами атаки. Експерти лабораторії Thales фіксують новітні види шкідливих програм. При цьому архітектура програмного забезпечення Cybels Sensor виявляє загрозу та маскує цю сигнатуру, щоб кіберзлочинці не знали про викриття та виявлення вірусу, тим самим ускладнюючи злочинцю можливість обійти захист.

Агентство національної безпеки Франції вивчає систему захисту Thales, при цьому La Poste (Французька поштова служба) використовує датчик виявлення кібератак Cybels Sensor.

Cybels Sensor загружений поведінковими алгоритмами, які здатні відмічати будь-яку активність, що штучний інтелект вважає ненормальною. Також він здатний аналізувати кожен файл, що проходить крізь мережу, досліджуючи і виявляючи можливі загрози, шкідливі програми та інші аномалії.

Створення кібербезпечного простору для захисту критичної інфраструктури охоплює: з одного боку, інформацію про особу від якої може бути кіберзагроза, з іншого, знання про різні форми небезпеки, що проявляються у шпіонських програмах, вірусах, троянських програмах, фільтрації, розкритті даних тощо.

Інформація щодо профілю, мотивації, стратегії злочинців дає можливість розрізняти рівень загрози об'єкти посягання, а відповідно обирати форму і ступінь захисту. Розрізняють декілька типів осіб, що здійснюють кібератаку: групи активістів-анонімів, які здійснюють атаки на компанії з політичних ідеологічних або соціальних мотивів; молодь, яку приваблює можливість самоствердження шляхом втручання та проникнення у систему захисту підприємств, установ; кібер-терористи, які посягають на стратегічні об'єкти, компрометуючи владу, порушуючи безпеку у державі та переслідуючи інші цілі; кібер-злочинці, які викрадають або вимагають гроші, шукають шляхи незаконного збагачення; цілеспрямовані найманці (кібер-пірати), які здійснюють вторгнення, створюючи загрозу та фінансуються з метою викрадення інформації або дестабілізації ситуації [6].

Для протидії цим численним та швидкоплинним загрозам експерти з кібербезпеки Thales надають зацікавленим підприємствам, установам, агентствам з безпеки у оборонній, енергетичній, морській, фінансовій та інших сферах консалдінгові послуги й рішення, що адаптовані до конкретної ситуації загрози, ризику чи уразливих місць. Фахівці з кібернетики Thales здійснюють аналіз профіля об'єкту захисту підприємств з метою виявлення потенційних шляхів атак, засобів розповсюдження, виявлення кола можливих агресорів. Здійснюється моніторинг, виявлення та реагування для відповідної матриці загроз щодо кожного підприємства. Зміст стратегії захисту критичної інфраструктури охоплюється наступним: навіть самі темні провулки можна зробити безпечними, якщо знати де сяє світло.

1. *Council Directive 2008/114/EC «On the identification and designation of European critical infrastructures and the assessment of the need to improve their protection». – [Електронний ресурс]. – Режим доступу : http:// eur-lex.europa.eu/*
2. *Communication from the commission on a European Programme for Critical Infrastructure Protection // Commission of the European Communities (COM/2006/786 final) 786. – [Електронний ресурс]. – Режим доступу : http://eur-lex.europa.eu/*
3. *Бірюков Д. Концепція захисту критичної інфраструктури як елемент загальноєвропейської безпекової політики // Наукові записки. Випуск – 6(68). [Електронний ресурс]. – Режим доступу: - http://www.ipiend.gov.ua/uploads/nz/nz_68/birukov_kontseptsia.pdf*

4. *Critical Infrastructure DHS 2025 Strategic Risk Assessment. [Електронний ресурс]. – Режим доступу: https://publicintelligence.net/dhs-ocia-critical-infrastructure-2025/*
5. *Leveraging artificial intelligence to maximize critical infrastructure cybersecurity. [Електронний ресурс]. – Режим доступу: https://www.thalesgroup.com/en/worldwide/security/magazine/leveraging-artificial-intelligence-maximize-critical-infrastructure*
6. *Threat intelligence: forewarned is forearmed. [Електронний ресурс] . – Режим доступу: https://www.thalesgroup.com/en/worldwide/security/magazine/threat-intelligence-forewarned-forearmed*

Юзікова Н.С. Перспективи використання штучного інтелекту у системі захисту критичної інфраструктури в Україні

Кризова ситуація, в якій опинилася держава, негативно впливає на зміну суспільних цінностей, розшарування населення за рівнем доходів, призводить до дисфункціональності соціальних інститутів та моральної дезорієнтації частини суспільства.

Екологічні катастрофи, загрози терористичної, екстремістської діяльності та радикалізації терористичного руху, кіберзлочинність негативно відзеркалюються на функціонуванні об'єктів критичної інфраструктури держави, а відповідно на рівні безпеки суспільства. Це, у свою чергу, потребує особливої уваги з боку держави до своєчасного виявлення ризиків, загроз і забезпечення невідкладного реагування на них, а також формування належної системи захисту критичної інфраструктури, що ґрунтується на відповідному інформаційному полі, має належне правове та технічне забезпечення.

Чим більше інформації у арсеналі правоохоронних органів та наукової спільноти, тим краще розуміння природи небезпеки, вчасного визначення загроз і ризиків та більше можливостей для особливих заходів системи захисту критичної інфраструктури в Україні та світі.

Ключові слова: штучний інтелект, захист критичної інфраструктури

Yusikova N.S. Perspectives of using artificial intelligence in critical infrastructure protection system in Ukraine

The crisis situation in which the state was, negatively affects the change of social values, the stratification of the population by income, leads to dysfunctionality of social institutions and moral disorientation of a part of society.

Environmental disasters, threats of terrorist activity, extremist activity and the radicalization of the terrorist movement, cybercrime are negatively reflected in the functioning of critical infrastructure objects of the state, and accordingly, at the level of social security. This, in turn, requires the state to pay particular attention to timely detection of risks, threats and emergency response, as well as appropriate legal and technical support for the establishment of a proper critical infrastructure protection system based on the relevant information field.

The more information in the arsenal of law enforcement and the scientific community, the better understanding of the nature of danger, the timely identification of threats and risks, and more opportunities for special measures of the critical infrastructure protection system in Ukraine and in the world.

Key words: artificial intelligence, protection of critical infrastructure

Зміст

Зміст

Наукове видання

Міжнародний журнал
ПРАВО І СУСПІЛЬСТВО

International Journal
LAW & SOCIETY

В редакції авторів наукових статей

Комп'ютерна верстка і правка Ігор КОЗИЧ

Підписано до друку 27.06.2018.
Формат 70x100. Папір офсетний.
Гарнітура «Times New Roman».
Ум.друк.арк. 12,65. Обл.-вид.арк. 13,75. Вид № в61315/18.
Тираж 100 прим.

Виготовлювач друкарня «Фоліант»
(ПП Віконська О.В.), м.Івано-Франківськ,
вул. Старозамкова, 2, тел./факс
(0342) 50-21-65; (багатоканальний)
Свідоцтво суб'єкта іидавничої справи Серія ІФ №24
foliant.drukarnja@gmail.com