УДК 342.4:327.7

ПОЛИТИКА ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ НАТО

Тарас ТКАЧУК,
кандидат юридических наук, доцент,
заместитель заведующего кафедрой организации защиты информации с ограниченным доступом
Учебно-научного института информационной безопасности Национальной академии Службы безопасности Украины

АННОТАЦИЯ

Статья посвящена исследованию политики НАТО в сфере обеспечения информационной безопасности. В ходе исследования определяются приоритеты и проблемы политики информационной безопасности НАТО. Также рассматриваются перспективы сотрудничества Украины и НАТО в сфере информационной безопасности.

Ключевые слова: информационная политика, информационная безопасность, безопасность информации, классифицированная информация, кибербезопасность, НАТО.

NATO'S INFORMATION SECURITY POLICY

Taras TKACHUK,
Candidate of Law, Associate Professor, Deputy Head of the Department of Information Security with Restricted Access
of Educational and Scientific Institute of Information Security of the National Academy of the Security Service of Ukraine

SUMMARY

The article is devoted to the study of NATO policy in the field of information security. The study identifies priorities and problems of NATO's information security policy. The article also discusses Ukraine-NATO cooperation in the field of information security.

Key words: information policy, information security, information security, classified information, cybersecurity, NATO.

REZUMAT

Articolul este dedicat studiului politicii NATO în domeniul securității informațiilor. Studiul identifică prioritățile și problemele politicii NATO de securitate a informațiilor. Se iau în considerare și perspectivele cooperării dintre Ucraina și NATO în domeniul securității informațiilor.

Cuvinte cheie: politica de informare, securitatea informațiilor, securitatea informațiilor, informații clasificate, securitatea informatică, NATO.

Постановка проблемы. 8 июня 2017 был принят Закон Украины «О внесении изменений в некоторые законы Украины относительно внешнеполитического курса Украины» [1], которым внесены изменения в Законы Украины «Об основах национальной безопасности Украины» [2] и «Об основах внутренней и внешней политики» [3] в части евроатлантической интеграции. Одним из приоритетов национальных интересов Украины этим Законом определена интеграция в евроатлантическое пространство с целью приобретения членства в Организации Североатлантического договора (НАТО). Окончательно выбрав евроинтеграционный курс, Украина должна ориентироваться на стратегию развития стран Европы в информационной сфере. Наиболее успешным примером воплощения в жизнь оптимальной модели информационного общества страны Европы, входящих в Североатлантический Альянс [4, с. 35].

Актуальность темы исследования. Указанные изменения в законодательстве свидетельствуют об углублении сотрудничества Украины с НАТО для членства в этой организации. При таких условиях приобретает все большее значение координация деятельности органов исполнительной власти, СМИ и т.д. по вопросам сотрудничества с НАТО в информационной сфере. Этот вектор развития внешней политики Украины влияет и на правовое регулирование системы безопасности информации как составной части евроатлантического пространства [5, с. 110], что, в свою очередь, требует глубокого понимания сущности политики информационной безопасности НАТО, а также информационной политики НАТО в целом.

Состояние исследования. Исследования по вопросам информационной безопасности в зарубежных странах в основном посвящены ее военно-политическим и техническим аспектам. Известными специалистами в этой сфере, которые дали рабочие определения информационной безопасности, является У. Швартау и М. Либики. Также в этом контексте следует отметить исследования Т. Ламбо, В. Каналя, К. Андерсон, Г. Диллона. Значительное внимание уделяется вопросам информационной политики в работах Р. Дорфа, Дж. Канингема и М. Манделбаума, посвященных анализу процесса расширения НАТО на Восток. Подробный анализ конкретных информационных операций НАТО проводился такими учеными, как П. Сигел, Дж. Нарел, К. Алларт и др. Исследованием информационной безопасности Украины в контексте мирового опыта и сотрудничества с НАТО занимались И. Беззуб, В. Глуховеря, Л. Задорожня, В. Кирик, О. Костенко, В. Роговец, однако вопросы обеспечения информационной безопасности стран НАТО, в т.ч. с точки зрения перспектив Украины, остаются недостаточно освещенными в научной литературе.

Постановка задачи. Целью статьи является исследование основ политики НАТО в сфере обеспечения информационной безопасности и перспектив сотрудничества Украины и НАТО в этой сфере.

Изложение основного материала. Система информационной политики НАТО является производной от реализации демократического принципа гражданского контроля над военно-политической сферой в условиях участия общественности в международном военно-политическом процессе. С повышением общественного интереса к деятельности Альянса в начале 90-х годов основная роль в производстве информационной деятельности отводится собственным институтам НАТО. Основным органом проведения информационной политики Альянса является Атлантический Совет, который публикует свои решения и заявления для прессы и широкой общественности. Кроме Атлантического совета, информированием общественности занимаются учреждения стран-членов НАТО.

Одну из ведущих ролей в реализации информационной политики Альянса играет Бюро информации и прессы. Оно входит в число структур отдела Генерального секретаря (после пражского саммита в 2002 году его функции выполняет Департамент публичной дипломатии, который обеспечивает информационную деятельность). В ходе реализации различных программ и мероприятий Бюро информации и прессы способствует правительствам стран НАТО и государств-партнеров в расширении понимания общественностью роли и направлений политики НАТО. Бюро поддерживает тесные связи с национальными информационными органами и осуществляет мероприятия, направленные на разъяснение общественности целей, задач и достижений НАТО [6].

Основы политики НАТО по обеспечению безопасности так называемой классифицированной информации изложены в документе СМ (2002) 49 «Безопасность в организации Североатлантического договора (НАТО)» [7]. Классифицирована информация – термин, используемый в законодательстве стран-членов НАТО относительно части «уязвимой» (sensitive) информации, то есть информации, которая уязвима к угрозам, возникающим в связи с несанкционированным доступом к ней, и поэтому нуждается в защите или хотя бы ограничении доступа к ней. НАТО выделяет пять уровней защиты информации с ограниченным доступом (Cosmic TOP Secret (CTS), NATO Secret (NS), NATO Confidential (NC), NATO Restricted (NR), Unclassified but Sensitive) [8].

Документ СМ (2002) 49 [7] устанавливает основные требования к системе обеспечения физической, организационной, процедурной и технической безопасности, в том числе – безопасности информации. Следуя совместным обязательствам, каждая страна-член НАТО предоставляет информации с ограниченным доступом собственную оценку, и, в зависимости от того, как другие члены НАТО выполняют принятые на себя обязательства, определяет, какую именно информацию сделать доступной для Альянса. Поэтому любое отступление со стороны одного или нескольких членов от выполнения их обязательств может привести к сокращению объема и качества передаваемой им информации. Основным принципом безопасности информации в системе НАТО при этом является то, что информация должна сохранять свою степень защиты в течение всего цикла ее обращения, начиная с источника, а контроль за распределением и распространением информации должен обеспечить отсутствие ее утечки.

Сотрудничество между НАТО и странами-партнерами, в том числе с Украиной, в рамках Совета евроатлантического партнерства (СЕАП) и программы «Партнерство ради мира» (ПРМ) [9] также предусматривает определенные обязательства сторон по обмену информацией и обеспечения ее безопасности. В частности, перед обменом любой секретной информацией между страной-участницей ПРМ и НАТО, органы, на которые возлагается обеспечение безопасности информации, должны быть взаимно уверены, что принимающая сторона информации готова обеспечить защиту информации в соответствии с требованиями стороны, которая ее передает.

Украина также проводит активное сотрудничество в области безопасности информации в рамках программы НАТО «Наука ради мира и безопасности» [10]. Ежегодно утверждается и Годовая национальная программа под эгидой Комиссии Украина – НАТО [11-12]. В условиях временной оккупации Россией Автономной Республики Крым и г.Севастополя, проведение в отдельных районах Донецкой и Луганской областей антитеррористической операции и общей ситуации, сложившейся в результате вооруженной агрессии России против Украины, Годовая национальная программа под эгидой Комиссии Украина – НАТО на 2018 год имеет особое значение для обеспечения защиты национальных интересов и безопасности Украины, прежде всего в контексте использования потенциала и практической помощи НАТО и государств – членов в повышении обороноспособности Украины для противодействия агрессии России и реформирования по стандартам НАТО сектора безопасности и обороны.

Важной задачей НАТО является недопущение актов агрессии в киберпространстве, ведь кибератаки учащаются и становятся все более организованными и убыточными для государственных учреждений, предприятий, объектов критической инфраструктуры, а также могут достичь критического уровня, который угрожает национальному и Евроатлантическому процветанию, безопасности и стабильности всего мирового сообщества. Источником таких атак могут быть иностранные военные и разведывательные службы, организованные преступные группировки, террористические и/или экстремистские группы [13]. Так, П. Корниш из лондонского Королевского института иностранных дел приводит следующую классификацию информационных угроз: деятельность хакеров-одиночек; организованная преступность в глобальных сетях; идеологический и политический экстремизм; информационная агрессия государств [14, p. 7-16]. При этом в системе НАТО под кибербезопасностью понимается поддержание состояния готовности к противодействию возможным угрозам высокой интенсивности и принятию наступательных контрмер.

Несмотря на то, что НАТО со времен создания постоянно защищает свои информационные системы, на Пражском саммите в 2002 году этот вопрос был вынесен в круг политических. Принимая во внимание технический прогресс, достигнутый после Пражского саммита, лидеры стран Альянса на Рижском саммите в 2006 году еще раз признали необходимость обеспечения кибернетической безопасности. В то же время,

после кибератак на Эстонию в 2007 году деятельность НАТО в области кибербезопасности преимущественно сосредоточено на защите коммуникационных систем, принадлежащих и использовавшихся Альянсом. Кибернападения 2007 заставили НАТО серьезно задуматься над проблемами обеспечения безопасности киберпространства, в частности, воспринимать угрозы, исходящие из интернет-пространства, как стратегически важные. В дальнейшем НАТО провело тщательную оценку своего подхода к кибербезопасности, по результатам которой в октябре 2007 года был подготовлен доклад министрам обороны стран Альянса, в которой содержались рекомендации по конкретным задачам НАТО, а также новые меры по совершенствованию защиты от кибератак. Официальная политика НАТО в сфере кибербезопасности (NATO Cyber Defence Policy) была одобрена министрами обороны стран-членов НАТО и представлена участникам организации в апреле 2008 г. на саммите в Бухаресте с целью «обеспечить возможности для оказания поддержки стран-союзниц, по его требованию, в противодействии кибератаке» [15].

Количество и сложность кибератак быстро увеличивалось после нападений на Эстонию в 2007 году, и уже летом 2008 г. война в Грузии продемонстрировала, что кибернападения стали основной составляющей военных действий с применением традиционного оружия. Так в 2010 году на Лиссабонском саммите НАТО было решено разработать новую политику НАТО по защите от киберугроз, а также конкретный план действий, который вступил в силу с июня 2011 года. В рамках их реализации НАТО использует процессы оборонного планирования с целью содействия развитию защиты от киберпреступности для союзников, а также для оптимизации взаимодействия, сотрудничества и обмена информацией. НАТО тесно сотрудничает по странами ЕС и с ООН в противодействии опасностям, возникающим в киберпространстве [16].

В Стратегический концепции и Декларации Лиссабонского саммита отмечается, что быстрое развитие и постоянное усложнение кибератак делают защиту информационно-коммуникационных систем стран-членов НАТО такой, от которой зависит будущая безопасность организации, а информационные атаки фигурируют среди самых опасных вызовов и угроз безопасности и процветанию государств-членов альянса. В иерархии вызовов, представленная в данной концепции, угрозы, которые происходят из информационного пространства, расположенные сразу же после распространения оружия массового уничтожения и терроризма. Такое внимание, в свою очередь, обусловлено феноменом секьюритизации, благодаря которому кибербезопасность «эволюционировала с технической дисциплины в стратегический концепт». Сейчас НАТО обеспечивает развитие средств предотвращения, выявления, реагирования и восстановления после атак через создание органа по управлению кибернетической безопасности, Общего Центра передового опыта по защите от киберугроз и Сил реагирования на компьютерные инциденты [18, с. 198-200].

Орган управления кибернетической безопасностью (ОУКБ) отвечает исключительно за согласование деятельности в области киберзащиты в пределах организации. ОУКБ НАТО руководит Комиссия по управлению деятельностью в области киберзащиты, в состав которой входят руководители политических, военных, оперативных и технических органов НАТО, которые отвечают за вопросы киберзащиты. Она является основным консультативным органом Североатлантического совета по вопросам киберзащиты и дает советы странам-членам организации по всем аспектам киберзащиты. ОУКБ НАТО входит в состав Управления новых вызовов безопасности штаб-квартиры НАТО. Центр передового опыта в области киберзащиты (г. Таллинн), получивший в октябре 2008 г. Аккредитации при НАТО, не наделен оперативными функциями и выступает в роли исследовательского и учебного центра, где разрабатываются доктринальные и концептуальные основы кибербезопасности, позиционируясь как «главный источник экспертизы в сфере совместной кибероборонь», которое «аккумулирует, создает и распространяет знания по ключевым вопросам кибербезопасности внутри НАТО, между государствами Альянса и его партнерами». Центр осуществляет научные исследования и подготовку по вопросам ведения информационных операций в виртуальном пространстве. При поддержке со стороны Комитета по планированию использования гражданских систем связи, Центра передового опыта в области борьбы с терроризмом (г. Анкара), а также программы НАТО «Наука ради мира и безопасности», Центр передового опыта в области киберзащиты проводит экспертные переговоры, семинары и обмены информацией с заинтересованными партнерами и международными организациями (например, ЕС и ОБСЕ). В 2015 году Центр опубликовал книгу о кибервойне между Украиной и Россией под названием «Cyber War in Perspective: Russian Aggression against Ukraine», где проводился анализ текущей деятельности в сфере защиты информации и стратегических и тактических последствий кибервойны. На страницах этой книги эксперты, в частности, отмечают, что понятие «кибератака» пока включает цифровую пропаганду, DDoS-кампании, дефейсы web-сайтов, утечки информации вследствие атак, а использование вредоносного программного обеспечения с целью шпионажа [19]. Британский эксперт Р. Хьюз рассматривает ОУКБ и таллиннский Центр как элементы единой организационной системы, где ОУКБ наделен «широкими возможностями по осуществлению электронного мониторинга в «реальном времени» и действует на оперативно-тактическом уровне, тогда как Центр, разрабатывая долгосрочную доктрину НАТО, составляет «интеллектуальную платформу», и является элементом стратегического уровня [20]. На сегодня эксперты Центра рассматривают милитаризацию Интернета как одно из самых опасных трендов мирового киберпространства.

В заявлении по результатам саммита в Варшаве, обнародованном главами государств и правительств, участвовавших в заседании Североатлантического совета в июле 2016 года, отмечается, что кибернападения составляют очевидный вызов безопасности Альянса и могут быть не менее губительными для современных обществ, чем нападения с применением обычных видов оружия. Поэтому киберзащита является частью главной задачи НАТО – коллективной обороны, а киберпространство признается сферой операций, в котором НАТО защищать себя так же эффективно, как делает это в воздухе, на земле и на море. Это повысит способность НАТО по защите и проведению операций в этих сферах, сохранит свободу

действий и решений в любых условиях и будет способствовать обеспечению НАТО широкими возможностями сдерживания и обороны [21].

Проблема обеспечения информационной безопасности НАТО, кроме вопросов технического обеспечения и стратегического планирования, имеет также и политическое измерение. В первую очередь это касается возможности применения статьи 5 Вашингтонского договора [22] к информационным атакам. Наиболее активными протагонистами расширения действия принципа коллективной ответственности в сфере обеспечения информационной безопасности в системе НАТО выступают Эстония и, частично, США. В частности, профессор Дж. Голдгейер отмечает, что по своему определению кибератаки не является «вооруженным нападением», то есть не подпадают под действие статьи 5, однако делает вывод о том, что Альянс «должен объединиться в противодействии атакам, которые угрожают безопасности любого из членов НАТО» [23, p. 4]. Необходимо отметить, что вопросы противодействия угрозам информационной безопасности, в том числе кибербезопасности, относят к сфере «мягкой безопасности» (soft security), в то время как главной задачей НАТО традиционно считают противодействие конвенционным вызовам безопасности – обеспечение «жесткой безопасности» (hard security). Еще одним проблемным фактором, который проявляется на трансатлантическом уровне, является «разделение труда» между членами НАТО, в результате которого одни страны специализируются на темах «мягкой безопасности», тогда как другие проводят «твердые» военные миссии. Следствием этого является различие в подходах противодействия США, Франция, Великобритания и Германия сопоставляют информационной безопасности с военной стратегией, тогда как Эстония, которая не обладает мощным военным потенциалом, подчеркивает ведущую роль гражданского общества и частного сектора [24].

Выводы. На сегодня вступление Украины в НАТО четко определено как один из ключевых факторов государственной политики. С целью получения членства в Альянсе Украина активизирует усилия по всему комплексу реформ, в том числе в сфере обороны и безопасности. Учитывая, что именно информационная безопасность сейчас является одним из важнейших аспектов обеспечения национальной, региональной и международной безопасности в целом, наша страна должна ввести достаточно мер предосторожности и процедур для ее обеспечения в соответствии с положениями политики НАТО в этой сфере, а также соблюсти условия, которые были предложены в плане действий Украина – НАТО. Это предполагает, в частности: обеспечение реализации гарантий доступа к информации; имплементации соответствующего законодательства для устранения препятствий деятельности СМИ; углубление информационного измерения сотрудничества Украина-НАТО, включая парламентское сотрудничество; создание прозрачной и гибкой структуры электронного управления; обеспечение развития способностей воинских частей и подразделений в сфере информационных операций; повышение уровня осведомленности общественности о деятельности НАТО, повышение уровня обеспечения информационной безопасности, кибербезопасности и тому подобное.

Список использованной литературы:

1. Про внесення змін до деяких законів України щодо зовнішньополітичного курсу України: Закон України від 08.06.2017 року. URL: www.zakon.rada.gov.ua/laws/show/2091-19.
2. Про основи національної безпеки України: Закон України від 19.06.2003 року. URL: www.zakon.rada.gov.ua/ laws/show/ 964-15
3. Про засади внутрішньої і зовнішньої політики: Закон України від 01.07.2010 року. URL: www.zakon.rada.gov.ua/ laws/show/ 2411-17
4. Політанський В.С. Світові моделі та фундаментальні принципи інформаційного суспільства. Науковий вісник Ужгородського національного університету: серія «Право». Випуск 43, том 1. 2017. С. 34-39.
5. Костенко О.В. Європейські стандарти правового регулювання обігу інформації з обмеженим доступом у роботі органів прокуратури. Науковий вісник Ужгородського національного університету: серія «Право». Випуск 34, том 3. 2015. С.109-114
6. Background information on the Alliance, its policies, activities and structures:[Online tool]. – Available at: http://www.nato.int/cps/en/natohq/ topics.htm
7. Document C-V(2002)49: Security within tne North Atlantic Treaty Organization (NATO). URL: www.statewatch.org/ news/2006/sep/nato-sec-classifications.pdf
8. Kaija E. Schilde. Cosmic top secret Europe? The legacy of North Atlantic Treaty Organization and cold war US policy on European Union information policy. URL: http://dx.doi.org/10.1080/09662839. 2014.911175
9. Партнерство заради миру: Рамковий документ, підписаний Україною 8 лютого 1994 року, набув чинності для України 8 лютого 1994 року. Офіційний вісник України. 2006. № 48. Ст. 3232.
10. Проблеми застосування в Україні норм інформаційної безпеки НАТО. URL: http://www.db.niss.gov.ua/docs/ polmil/1fgs93.htm (дата звернення 15.09.2017).
11. План дій Україна-НАТО (за матеріалами Національного центру з питань Євроантлантичної інтеграції України). URL: http://www.nceai.gov.ua/plan.phtml (дата звернення 15.09.2017).
12. Про затвердження Річної національної програми під егідою Комісії Україна – НАТО на 2017 рік: Указ Президента України від 08.04.2017 № 103/2017. URL: http://www.president.gov. ua/documents/1032017-21670
13. North Atlantic Treaty Organization. Active Engagement. Modern Defence Strategic Concept For the Defence and Security of The Members of the North Atlantic Treaty Organisation. URL: http://www.nato.int/ lisbon2010/ strategic–concept–2010–eng.pdf
14. Cornish P. Cyber Security and Politically, Socially and Religiously Motivated Cyber Attacks. Brussels: European Parliament, 2014. 34 p.
15. NATO Bucharest Summit Declaration, 3 April 2008. URL: http://www.nato.int/docu/pr/2008/p08-049e.html
16. North Atlantic Treaty Organization. Defending against cyber attacks. URL: http://www.nato.int/cps/en/natolive/topics_49193.htm
17. NATO Lisbon Summit Declaration, 20 Nowember 2010. URL: http://www.nato.int/docu/pr/2010/p10-049e.html

18. Бєлоусова Н.Б., Афанасьєва П.А. Основні вимоги НАТО щодо забезпечення безпеки інформаційного простору. Актуальні проблеми міжнародних відносин. Випуск 102, частина І. 2011. С. 196-202.

19. Центр информационной безопасности НАТО выпустил книгу о кибервойне Украины с Россией. URL: http://www.dut.edu.ua/ru/news-1-574-2267

20. Hughes, R.B. NATO and Cyber Security: Mission accomplished? URL: http://www.carlisle.army.mil/DIME/documents/ NATO%20 and%20 Cyber%20Defence.pdf

21. NATO Warsaw Summit Communiqué, 9 July 2016. URL: http://www.nato.int/cps/en/natohq/official_texts_133169.htm

22. The North Atlantic Treaty. Washington D.C. URL: www.nato.int/cps/ru/natohq/official_text_17120.htm

23. Goldgeier J. The Future of NATO. NATO Science for Peace and Security Series, E: Human and Societal Dynamics. Amsterdam: IOS Press, 2011. Vol. 76. P. 1–12.

24. Kempf A. Considerations for NATO Strategy on Collective Cyber Defense. URL: http://csis.org/blog /considerations-nato-strategy-collective-cyberdefense

ИНФОРМАЦИЯ ОБ АВТОРЕ

Ткачук Тарас Юрьевич – кандидат юридических наук, доцент, заместитель заведующего кафедрой организации защиты информации с ограниченным доступом Учебно-научного института информационной безопасности Национальной академии Службы безопасности Украины

INFORMATION ABOUT THE AUTHOR

Tkachuk Taras Yuryevich – Candidate of Law, Associate Professor, Deputy Head of the Department of Information Security with Restricted Access of Educational and Scientific Institute of Information Security of the National Academy of the Security Service of Ukraine

tarast25@gmail.com

УДК 343.21

СРАВНИТЕЛЬНЫЙ АНАЛИЗ УГОЛОВНОЙ ОТВЕТСТВЕННОСТИ ЗА РЕЙДЕРСТВО В УКРАИНЕ С НЕКОТОРЫМИ ЗАРУБЕЖНЫМИ ГОСУДАРСТВАМИ

Инна ФЕДУЛОВА,
аспирант кафедры уголовного права и криминологии
Львовского государственного университета внутренних дел

АННОТАЦИЯ

Статья посвящена сравнительному анализу уголовного законодательства, направленного на охрану от рейдерских посягательств в Украине, с законодательством некоторых зарубежных государств, в частности Казахстана, Молдовы и России. Осуществляется попытка проанализировать особенности составов преступлений, которые предусматривают ответственность за такие посягательства, выявить как позитивные черты, так и пробелы, сравнить их с составом преступления, что предусмотрен ст. 206-2 УК Украины. Также освещаются проблемные вопросы, связанные с применением отмеченных статей на практике. Кроме того, вносятся предложения относительно усовершенствования отечественной уголовно-правовой нормы на основе опыта зарубежных государств.

Ключевые слова: рейдерство, хозяйственное общество, завладение имуществом юридического лица, состав преступления, уголовно-правовая конструкция.

COMPARATIVE ANALYSIS OF CRIMINAL RESPONSIBILITY FOR RAIDERSHIP IN UKRAINE WITH SOME FOREIGN COUNTRIES

Inna FEDULOVA,
Postgraduate Student at the Department of Criminal Law and Criminology
of Lviv State University of Internal Affairs

SUMMARY

The article is devoted to the comparative analysis of criminal legislation aimed at protecting against raidership in Ukraine with the legislation of some foreign countries, in particular Kazakhstan, Moldova and Russia. Attempts are made to analyze the peculiarities of the offences comprised of liability for such attacks, to identify both positive features and gaps, and compare them with the composition of the crime provided by Article 206-2 of the Criminal Code of Ukraine. The article also highlights problematic issues related to the application of these articles in practice. In addition, proposals are made to improve the domestic criminal law provisions on the basis of the experience of these foreign countries.

Key words: raidership, business enterprise, acquiring property of legal entity, offence, criminal-law construction.

REZUMAT

Articolul este dedicat unei analize comparative a legislației penale menite să protejeze împotriva încălcărilor raider în Ucraina cu legislația unor state străine, în special Kazahstan, Moldova și Rusia. Se face o încercare de a analiza caracteristicile infracțiunilor care includ responsabilitatea pentru astfel de atacuri, identifica atât caracteristicile pozitive și spațiilor, pentru a le compara cu compoziția infracțiunii, cu condiția ca Codul penal st.206-2 al Ucrainei. De asemenea, au fost evidențiate problemele problematice asociate cu aplicarea articolelor menționate în practică. În plus, se fac propuneri de îmbunătățire a normelor de drept penal intern pe baza experienței statelor străine.

Cuvinte cheie: raid, entitate de afaceri, achiziționarea de active ale unei persoane juridice, constituie o crimă, de construcție penală-legală.

Постановка проблемы. Противоправное завладение имуществом предприятия, учреждения, организации создает реальную угрозу национальным и экономическим интересам государства и требует формирования эффективной