Плетенецький, Балабани, Захарія Копистенський, Михаїл Копистенський, Атанасій Кальнофойський були церковно-культурних діячами.

Серед козацтва відіграли визначну роль для української шляхти: Дмитро Вишневецький, Кшиштоф Косинський, Петро Конашевич-«Сагайдачний», Михайло Хмельницький. Згідно з висловом Михайлом Грушевським, шляхта «надавала тон ідеології, займаючи найбільш впливові, провідні позиції в козацькім війську, становлячи – його мозок». [4]

Отже, початком формування української шляхти можна вважати її приєднання до Великого князівства Литовського. На перших етапах свого формування шляхта мала різні поняття і визначення. Відправним пунктом історії української шляхти на мою думку є кінець XIV – початок XV століття коли відбулось різке збільшення чисельності низових прошарків воїнів-землевласників, яке разом з політичними змінами того часу призвело до модифікації тодішньої ієрархії. Зокрема на початковому етапі шляхетське звання міг привласнити собі майже кожен, але не кожен міг його зберегти та підтвердити.

Аннотация. В данном исследования представлена информация о формировании украинской шляхты. Описывается влияние соседних государств на украинском земли при формировании шляхты. Указываются особенности ее формирования на украинских землях. Методологической основой исследования является системный подход, общенаучные (анализа, синтеза, обобщения) и специально-исторические методы. Специфика исследуемой темы предусматривает применение сравнительно-исторического метода.

Ключевые слова: шляхта, украинская шляхта, статус, привилегии, формирования.

Abstract. This study provides information on the formation of the Ukrainian nobility. The influence of the neighboring states on the Ukrainian lands in the formation of the nobility is described. The features of its formation on the Ukrainian lands are indicated. The methodological basis of the study is a systematic approach, general scientific (analysis, synthesis, generalization) and special historical methods. The specificity of the topic under study involves the use of a comparative-historical method.

Key words: nobility, Ukrainian nobility, status, privileges, formation.

СПИСОК ЛІТЕРАТУРИ

1. Семененко В., Потоцький В. Шляхта. Честь та гонор: факти, міфи, коментарі. К., 2014. 672 с.
2. Яковенко Н. М. Українська шляхта з кінця XIV до середини XVII століття. Волинь і Центральна Україна. К., 1993. 472 с.
3. Блануца А. В. Земельні володіння волинської шляхти у другій половині XVI ст. К.: Вид-во Інститут історії України НАН України, 2007. 243 с.
4. Грушевський М. Очерк истории Киевской земли от смерти Ярослава до конца XVI в. К., 1891. С. 458.
5. Грушевський М. Історія України-Руси. Т. 5. Львів, 1905. 688 с.

УДК 34:004.056.5(045)

ЗАГРОЗИ І МОДЕЛІ СИСТЕМИ ГЛОБАЛЬНОЇ ІНФОРМАЦІЙНОЇ БЕЗПЕКИ

А. О. Боднар, О. Г. Турченко

Анотація. Формування інформаційного суспільства, глобалізація, розвиток новітніх технологій та нові виклики сучасності призвели до виникнення нових способів ведення війни та кардинально змінили систему міжнародної безпеки. Суттєво змінились принципи, ресурси і засоби ведення війн. Сучасні виклики та загрози системі глобальної інформаційної безпеки призвели до переосмислення концептуальних і практичних засад міжнародного співробітництва у сфері інформаційної безпеки. В статті аналізуються підходи до розуміння природи та видів загроз, моделі системи глобальної інформаційної безпеки.

Ключові слова: безпека, інформаційна безпека, кіберпростір, загрози, модель

Постановка проблеми. В сучасному світі вже не існує суто збройних міжнародних конфліктів, в яких не використовуються додаткові механізми інформаційного впливу, пропаганди чи інформаційних технологій. Вразливість, взаємопов’язаність, доступність та

незахищеність суб'єктів відносин притаманні системній кризі міжнародної інформаційної безпеки. Як зазначає О. М. Фролова, міжнародне співробітництво у сфері інформаційної безпеки зумовлює необхідність пошуку спільних рішень щодо протидії інформаційним та кіберзагрозам, вироблення спільної стратегії інформаційної безпеки для протидії кібервійнам, інформаційному тероризму та інформаційній злочинності [1]. При цьому не можна не погодитися з О. Г. Додоновим [2, с. 17], що інформаційна безпека є, насамперед, властивістю системи мінімізувати інформаційні загрози. При розгляді проблеми інформаційної безпеки слід спочатку говорити про загрози і вже потім - про захищеність від цих загроз.

Складність забезпечення інформаційної безпеки обумовлена також відсутністю універсального міжнародного договору з питань міжнародної інформаційної безпеки, формально визначених правил, що встановлюють права і обов'язки, здійснення яких забезпечується юридичним механізмом. На сьогодні можна говорити тільки про норми «м'якого права», закріплені у резолюціях Генеральної Асамблеї ООН, які «дозволяють визначити риси, окреслити контури, а у певних випадках і визначити елементи майбутнього механізму міжнародно-правового регулювання міжнародної інформаційної безпеки» [3, с. 40].

Відповідно нагальним та актуальним є питання вироблення дієвих механізмів забезпечення міжнародної інформаційної безпеки.

Дослідженням інформаційної безпеки України займалися В. Беляков, М. Демкова, Л. Задорожня, В. Кирик, А. Крутських, Н. Кушакова-Костицька, А. Леваков, Є. Макаренко, В. Роговець та інші, але низка питань залишилася не висвітленою у науковій літературі; в міжнародному контексті інформаційну безпеку розглядали Н. Винер, Р. Хартлі, К. Шеннон, Н. Рашевський, О. Турченко.

Метою статті є дослідити підходи до розуміння природи загроз глобальній інформаційній безпеці, запропонувати їх систематизацію, охарактеризувати моделі системи глобальної інформаційної безпеки.

Виклад основного матеріалу. Первинною є саме інформаційна загроза. І якщо говорити про інформаційну безпеку як про властивість мінімізувати загрози для певних об'єктів і суб'єктів інформаційної діяльності, то це дає можливість розглядати не загальнометодичні питання інформаційної безпеки, а різні рівні інформаційної взаємодії, інформаційних відносин, виділити методологічні та теоретичні проблеми забезпечення інформаційної безпеки, які необхідно вирішити. А тоді вже визначати засоби, методи протидії інформаційним загрозам, закладати ці методи у відповідні інформаційні системи для адекватного реагування на загрози.

Таким чином, необхідно розмежовувати безпосередні загрози інформаційній безпеці і засоби забезпечення цієї безпеки, що спрацьовують лише при виникненні загроз. Аналізуючи проблему загроз інформаційної безпеки необхідно визначити, що саме може розцінюватися як загроза.

По-перше, загрозу можуть нести лише певні дії (діяльність або бездіяльність), що мають прямий причинно-наслідковий зв'язок із зміною відповідних умов і параметрів інформаційних процесів, які визначають безпечні умови існування суспільства і держави.

По-друге, ці дії повинні бути конкретно-визначеними, а не загальними. По-третє, як зазначає Б. А. Корміч, ще одним фактором має бути рівень суспільної небезпеки цих дій. Безумовно, дії, які можуть розцінюватися як загроза інформаційній безпеці, повинні мати виключно високу суспільну небезпеку, оскільки їх об'єктом є не просто права або законні інтереси певних суб'єктів, а правові відносини щодо забезпечення умов, порушення яких ставить під сумнів саму можливість нормального існування цих суб'єктів [4, с. 195]. Відповідно, замахом на інформаційну безпеку є ті дії, за які законом передбачена відповідальність.

З 1996 року проблема міжнародної інформаційної безпеки була винесена на політичний та міжнародно-правовий рівень. Концепцію міжнародної інформаційної безпеки було обговорено на міжнародній конференції з проблем становлення інформаційного суспільства та глобальної цивілізації (ПАР, 1996 р.). Починаючи з

1998 року питання забезпечення інформаційної безпеки та її загроз майже щорічно знаходяться на порядку денному ООН. Так, в 1998 році Резолюція ГА ООН 53/70 «Досягнення у сфері інформатизації і телекомунікацій в контексті міжнародної безпеки» пропонувала державам-членам ООН продовжити обговорення питань інформаційної безпеки, дати конкретні визначення загроз, запропонувати свої оцінки проблеми, включаючи розробку міжнародних принципів забезпечення безпеки глобальних інформаційних систем. В ній зазначалося, що міжнародна спільнота визнає проблему інформаційної безпеки як багатоаспектний стратегічний напрям взаємодії держав у світі, пропонувалося державам-членам ООН розглянути конкретну типологію інформаційних загроз, визначити критерії проблеми, включаючи розробку міжнародних принципів безпеки глобальних інформаційних систем, внести пропозиції до комплексної доповіді Генерального секретаря ООН для створення міжнародного механізму протидії використанню інформаційних озброєнь та розпалюванню інформаційних війн.

А аналогічна Резолюція ГА ООН 54/49 від 1 грудня 1999 року вперше вказала на загрози міжнародної інформаційної безпеки стосовно не тільки до цивільної, але й до військовій сфері.

На виконання Резолюції Генеральної Асамблеї ООН A/RES/55/28 «Досягнення в сфері інформатизації та телекомунікацій в контексті міжнародної безпеки» від 20 листопада 2000 року, в якій наголошувалося на необхідності вивчення відповідних міжнародних концепцій, спрямованих на зміцнення безпеки глобальних інформаційних та телекомунікаційних систем, була підготовлена Доповідь Генерального секретаря ООН від 3 жовтня 2001 року «Про досягнення в сфері інформатизації та телекомунікацій в контексті міжнародної безпеки», яка визначила і 11 основних факторів (загроз), що створюють небезпеку для основних інтересів особистості, суспільства і держави в інформаційному просторі: цілеспрямований інформаційний вплив на критичні інфраструктури та населення іншої держави; дії, спрямовані на домінування в інформаційному просторі, заохочення тероризму, і власне ведення інформаційних війн тощо.

Можна також зазначити і резолюції A/RES/56/121 від 19 грудня 2001 р. про боротьбу зі злочинним використанням інформаційних технологій, A/RES/57/239 від 20 грудня 2002 р. про створення глобальної культури кібербезпеки, A/RES/58/199 від 23 грудня 2003 р., A/RES/62/17 від 5 грудня 2007 р. і A/RES/64/211 від 21 грудня 2009 р. про створення глобальної культури кібербезпеки і захисту найважливіших інформаційних інфраструктур.

У 2017 році було прийнято доповідь Генерального секретаря «Досягнення у сфері інформатизації та телекомунікацій в контексті міжнародної безпеки», як виконання рекомендацій резолюції A/RES/71/28 від 5 грудня 2016 року щодо інформування країн про свою точку зору з питань загальної оцінки міжнародної інформаційної безпеки та зусиль, які докладають держави.

Щодо протидії кіберзлочиності, то треба вказати також резолюції Економічної і Соціальної Ради ООН «Міжнародне співробітництво у справі щодо попередження і розслідування шахрайства, злочинного неправомірного використання і фальсифікації особистих даних і пов'язаних з ними злочинів, а також переслідування та покарання за них» № 2004/26 від 21 липня 2004 року, – № 2007/20 від 26 липня 2007 року.

Треба вказати і певні регіональні ініціативи: План дій держав-членів Шанхайської організації співробітництва (ШОС) щодо забезпечення міжнародної інформаційної безпеки, затверджений 16 серпня 2007 р. у м. Бішкек, у якому зафіксовано наміри сторін протистояти викликам і загрозам в інформаційній сфері; Угоду між урядами держав-членів ШОС щодо співробітництва у галузі забезпечення міжнародної інформаційної безпеки, яка вступила у дію лише 5 червня 2012 р. [5, с. 157]. Зокрема, у п. 1 Угоди визначено загрози у галузі забезпечення міжнародної інформаційної безпеки; основні напрями, форми й механізми співробітництва та засади захисту інформації.

Додаток 2 ж містить перелік основних загроз у сфері забезпечення міжнародної інформаційної безпеки, їхніх витоків та ознак, а саме: розробка та застосування інформаційної зброї, підготовка і ведення інформаційної війни; інформаційний тероризм; інформаційна злочинність; використання домінуючого положення в інформаційному просторі на шкоду інтересам і безпеці інших держав; поширення інформації, яка завдає шкоду суспільно-політичної та соціально-економічної систем, духовної, моральної і культурної середовищі інших держав; загрози безпечного, стабільного функціонування глобальних і національних інформаційних інфраструктур, що мають природний і (або) техногенний характер.

Якщо узагальнити, то дії, що зачіпають інформаційну безпеку, можна розділити на внутрішні (пов'язані з діяльністю або з факторами, які мають своє походження всередині держави) і зовнішні (фактори або дії, що беруть початок за межами території держави).

Зазначені дії (загрози), в свою чергу, можна класифікувати залежно від змісту цих дій і від характеру і ступеня їх небезпеки для особистості, суспільства, держави і міжнародного співтовариства в цілому:

1. Найбільш небезпечні для держави і міжнародного співтовариства дії, що зачіпають інформаційну безпеку, що здійснюються однією державою або групою держав щодо іншої держави або групи держав. Подібні дії більшістю дослідників об'єднуються в понятті «інформаційна війна»;

2. Небезпечні для держави і суспільства дії, що здійснюються для досягнення політичних, релігійних та інших цілей, для створення обстановки страху в державі або державах. Такі дії здійснюються, як правило, організованими терористичними угрупованнями і отримали назву «інформаційний тероризм»;

3. Дії, що зачіпають інформаційну безпеку, які походять від осіб, які переслідують злочинні цілі, або «інформаційні злочини».

Відсутня система забезпечення інформаційної безпеки на національному рівні унеможливлює надійне її забезпечення не тільки у середині держави, а й на міждержавному рівні. Беручи до уваги масштаб проблеми інформаційної безпеки, розвинуті країни розпочали реалізацію довгострокових державних програм, які спрямовані на забезпечення захисту найважливіших інформаційних структур.

За результатами проведених досліджень експерти з питань безпеки, аналітики НАТО виділили такі моделі системи глобальної інформаційної безпеки:

Модель 1 – створення абсолютної системи захисту країни-інформаційного лідера проти будь-якого виду наступальної інформаційної зброї, що обумовлює об'єктивні переваги в потенційній інформаційній війні, змушує інші країни шукати альянсу у військово-інформаційних діях з країною-інфолідером. При цьому може бути використано систему жорсткого контролю над інформаційним озброєнням противника на підставі потенційних міжнародних документів з інформаційної безпеки.

Погляд на такий розвиток подій покладено у відомому дослідженні Дж. Ная та У. Оуенса «America's Information edge strategy and force planning», 1996 р. («Головна сила Америки – її інформаційні можливості») [6], в якому домінуюча роль в інформаційній революції належить США, а саме у використанні надважливих засобів комунікації та інформаційних технологій (супутникового спостереження, прямого мовлення, швидкісних комп'ютерів, унікальних можливостей в інтегруванні складних інформаційних систем), у політиці стримування і нейтралізації традиційних воєнних загроз та нових видів озброєнь.

Модель 2 – створення значної переваги держави-потенційного ініціатора інформаційної війни в наступальних видах озброєнь, у знешкодженні систем захисту держави-противника засобами інформаційного впливу, координація дій із союзними державами з використанням визначених засобів інформаційної зброї для ідентифікації джерел і типів інформаційних загроз.

Практичне втілення моделі спостерігається в перебігу інформаційної операції «Союзницька сила» (1999 р.), яку США та країни-члени НАТО здійснили проти

Республіки Югославії, коли була сформована безпрецедентна за масштабами система управління інформаційними потоками для проведення військових операцій (спроможність надавати розвідувальну інформацію безпосередньо кожному з учасників бойових дій), масових пропагандистських кампаній з широким спектром інформаційних методик, спрямованого інформаційно-психологічного впливу, потужного використання Internet та комп'ютерного протиборства для модифікації національного інформаційного простору і контролю за інфоінфраструктурою Югославії [7].

Модель 3 – наявність кількох країн-інфолідерів та потенційного протиборства між ними, визначення фактору стримування експансії інформаційних загроз, забезпечення в перспективі домінування однієї з держав у сфері міжнародної інформаційної безпеки з можливостями значного впливу на глобальну інфосферу та переважного права вирішення проблем глобального світопорядку.

Дослідження ЦРУ 90-х років XX століття та на перспективу до 2020 року визначали як основні джерела загроз в кіберпросторі для США тільки дві країни – Росію і Китай. У військовій доктрині збройних сил США (Концепція Force XXI, 1996 р.), було запропоновано дві складові театру воєнних дій – традиційний простір і кіберпростір, а основними об'єктами впливу стали інформаційна інфраструктура і психологічна сфера (human network) противника [8].

Модель 4 – всі конфліктуючі сторони використовують транспарентність інформації для формування ситуативних альянсів, для досягнення переваг локальних рішень, які спроможні заблокувати технологічне лідерство, для використання можливостей інфоінфраструктури на окремих територіях з метою організації внутрішнього конфлікту між опозиційними силами (політичні, сепаратистські, міжнаціональні конфлікти) для проведення міжнародних антитерористичних інформаційних операцій. Так, у рамках міжнародної антитерористичної операції «Помста» (Афганістан, 2001 р.) мета спеціалізованих центрів США, відповідальних за проведення інформаційних операцій, полягала у плануванні психологічних кампаній, реагуванні на зміну ситуації, у підтримці інформаційних ресурсів та безпеки військових сил і цивільного населення, а Північний Альянс вперше в історії застосував статтю 5 Статуту НАТО, яка спрямована на забезпечення загального захисту країн-членів перед викликами зовнішніх загроз; держави ЄС, країни-учасниці ГУАМ підтвердили підтримку дій США в цій акції і консолідацію зусиль міжнародного співтовариства у протиборстві з міжнародним тероризмом у спільній заяві та меморандумі дій.

Таким чином, з наведеного можна зробити наступні *висновки.*

По-перше, загрозу інформаційній безпеці можуть нести лише певні, конкретно-визначені дії (діяльність або бездіяльність), що мають виключно високу суспільну небезпеку і прямий причинно-наслідковий зв'язок із зміною відповідних умов і параметрів інформаційних процесів, які визначають безпечні умови існування суспільства і держави.

По-друге, можна виділити 4 моделі системи глобальної інформаційної безпеки:

– модель 1 – створення абсолютної системи захисту країни-інформаційного лідера (дана модель конструюється залежно від кількості суб'єктів системи безпеки, відповідно виділяються чотири основні моделі, що конкурують між собою: однополярна система безпеки, «концерт держав», багатополярна модель, глобальна (універсальна) модель);

– модель 2 – створення значної переваги держави-потенційного ініціатора інформаційної війни;

– модель 3 – наявність кількох країн-інфолідерів та потенційного протиборства між ними;

– модель 4 – всі конфліктуючі сторони використовують транспарентність інформації для формування ситуативних альянсів.

Аннотация. Формирование информационного общества, глобализация, развитие новейших технологий и новые вызовы современности привели к возникновению новых способов ведения войны и кардинально изменили систему международной безопасности. Существенно изменились принципы, ресурсы

и средства ведения войн. Современные вызовы и угрозы системе глобальной информационной безопасности привели к переосмыслению концептуальных и практических основ международного сотрудничества в сфере информационной безопасности. В статье анализируются подходы к пониманию природы и видам угроз, модели системы глобальной информационной безопасности.
Ключевые слова: безопасность, информационная безопасность, киберпространство, угрозы, модель

Abstract. The formation of the information society, the globalization, the development of advanced technologies and new challenges of modern times have led to the emergence of new methods of warfare and radically changed the system of international security. The principles, resources and means of warfare have changed significantly. Modern challenges and threats to the global information security system have led to a rethinking of the conceptual and practical foundations of international cooperation in the field of inform ation security. The article analyzes the approaches to understanding the nature and types of threats, the model of the global information security system.
Key words: security, global information security, cyberspace, threats, model.

СПИСОК ЛІТЕРАТУРИ

1. Фролова О. М. Роль ООН в системі міжнародної інформаційної безпеки. *Міжнародні відносини. Серія «Політичні науки».* 2018. №18-19. URL : http://journals.iir.kiev.ua/index.php/pol_n/article/view/3468.
2. Інформаційні операції та безпека суспільства: загрози, протидія, моделювання: монографія / В. П. Горбулін, О. Г. Додонов, Д. В. Ланде. К.: Інтертехнологія, 2009. 164 с. URL : http://dwl.kiev.ua/art/gdl/.
3. Войціховський А. В. Формування системи інформаційної безпеки в рамках ООН. Правоохоронна функція держави: теоретикометодологічні та історико-правові проблеми: тези доп. учасників міжнар. наук.-практ. конф. (м. Харків, 17 трав. 2019 р.) / МВС України, Харків. нац. ун-т внутр. справ; Консультат. місія Європейського Союзу. Харків : ХНУВС, 2019. С. 40–42. URL : http://dspace.univd.edu.ua/xmlui/bitstream/handle/123456789/5333/Pravookhoronna%20funktsiia%20derzhavy_konferentsiia_2019.pdf?sequence=1&isAllowed=y.
4. Кормич Б. А. Правова регламентація інформаційної безпеки України . *Держава і право.* 2003. Випуск 17. С.193–198.
5. Гапеєва О. Міжнародна інформаційна безпека – ключовий напрям діяльності Шанхайської організації співробітництва: 2006 – 2017 рр. *Східноєвропейський історичний вісник.* 2017. Випуск 4. С.155–163. URL: file:///C:/Users/Admin/Downloads/111226-245988-1-PB.pdf.
6. Nye J. S. America's Informational edgel Strategy and force planning. URL: http://ics.leeds.ac.uk/papers/vp01.cfm?outfit=pmt&requesttimeout=500&folder=49&paper=155.
7. Гриняев С. Особенности информационной войны во время агрессии НАТО против Югославии (по материалам открытой печати). URL : http://www.narod.ru/warfare/grinyaev/page008.htm.
8. Гриняев С. Н. Информационная война: история, день сегодняшний и перспектива. URL : http://www.narod.ru/warfare/grinyaev/page009.htm.

УДК 34:004.774(045)

ДОМЕННЕ ІМ'Я: АКТУАЛЬНА ПРОБЛЕМАТИКА ПРАВОВОГО РЕЖИМУ

В. М. Борівська, Т. В. Міхайліна

Анотація. У даній статті проаналізовано сучасний стан правового регулювання домену, а саме досліджено законодавство та думки науковців щодо визначення правової природи доменного імені. Разом з тим, виявлено такі проблемні питання як лише фрагментарне правове регулювання домену, що як наслідок породжує нові порушення прав власників доменних імен та неспроможність останніх на відповідний захист. В ході дослідження визначено правову природу домену та необхідність створення спеціального закону з метою правового врегулювання даного питання. Методологічною основою роботи є порівняльно-правовий метод та метод аналізу.
Ключові слова: домен, доменне ім'я, веб-сайт, об'єкт права інтелектуальної власності, мережа Інтернет;

Мережа Інтернет з'явилася лише в другій половині минулого століття, але на цей час починає займати невід'ємну частину нашого життя. Даний факт зумовлює створення окремого механізму правового регулювання відповідних суспільних відносин з урахуванням технічних особливостей мережі.