СЕКЦІЯ 5
ПУБЛІЧНЕ УПРАВЛІННЯ У СФЕРІ ДЕРЖАВНОЇ БЕЗПЕКИ ТА ОХОРОНИ ГРОМАДСЬКОГО ПОРЯДКУ

ЗАГРОЗИ ІНФОРМАЦІЙНОЇ БЕЗПЕКИ ОСОБИСТОСТІ У СФЕРІ НАЦІОНАЛЬНОЇ БЕЗПЕКИ УКРАЇНИ ТА ЇЇ ПРИКОРДОННОМУ СЕКТОРІ

THREATS TO THE INDIVIDUAL INFORMATION SECURITY IN THE FIELD OF NATIONAL SECURITY OF UKRAINE AND ITS BORDER SECTOR

УДК 351.746.1
DOI https://doi.org/10.32843/pma2663-5240-2022.27.17

Кукін І.В.
к. наук з держ. упр.,
докторант кафедри
прикордонної безпеки
Національна академія
Державної прикордонної служби
України імені Богдана Хмельницького

У статті розглянуто питання щодо визначення загроз інформаційної безпеки особистості та їх класифікації. Зазначено, що одним зі шляхів забезпечення інформаційної безпеки може бути вжиття заходів імунізації соціуму від шкідливої або небезпечної інформації як альтернатива заходам протидії розповсюдження небезпечної інформації.
Наведено авторське визначення загрози й ризику інформаційної безпеки особистості в системі національної безпеки та її прикордонному секторі. Серед основних джерел загроз інформаційної безпеки особистості акцентовано увагу на реальних можливостях спотворення інформації мережевим сервісом автоматичного перекладу текстів. Зазначені загрози розглянуто на реальному прикладі.
Розглянуто загрози, що породжуються недосконалим визначенням норм права. Показаний зв'язок інформаційних загроз із діяльністю людини. Наведено рекомендації щодо класифікації інформаційних загроз особистості залежно від вагомості впливу на стан безпеки відповідно до ступеня відповідальності правопорушника та видів небезпек.
Зазначено, що, зважаючи на принципові відмінності об'єктів, що потребують захисту від шкідливого або небезпечного інформаційного впливу країни-агресора, потребується відокремлення розгляду в системі національної безпеки держави проблем інформаційної безпеки особистості й інформаційної безпеки суспільства та держави.
Акцентовано увагу на необхідності вдосконалення мотиваційних факторів щодо добровільної участі громадян у виявленні загроз інформаційній безпеці. Запровадження в умовах стрімкого розвитку систем штучного інтелекту сучасних підходів щодо стандартизації та верифікації програмного забезпечення, яке використовується для автоматичного перекладу текстів, поширення інформації з питань історії, теорії та практики конституціоналізму, державного будівництва, міжнародної політики, виконання міжнародних договорів, поширення державної статистики й висвітлення політичного життя суспільства. Усунення передумов до поширення небезпечної інформації шляхом використання Інтернет-сервісів, що надаються провайдерами країни-агресора.
Ключові слова: *загроза, ризик, інформаційна безпека, інформаційна безпека особистості, національна безпека, прикордонна безпека.*

The article considers the issue of identifying threats to the individual information security and their classification. It is noted that one of the ways to ensure information security may be to take measures to immunize society from harmful or dangerous information, as an alternative to measures to combat the spread of dangerous information.
The author's definition of the threat and risk of the individual information security in the national security system and its border sector is given. Among the main sources of threats to the individual information security, attention is focused on the real possibilities of information distortion by the network service of automatic translation of texts. These threats are considered on a real example.
Threats arising from imperfect definition of legal norms are considered. The connection of information threats with human activity is shown. Recommendations for the individual information threats classification depending on the severity of the impact on the security situation according to the degree of the offender responsibility and the dangers types.
It is noted that due to the fundamental differences between the objects that need protection from harmful or dangerous informational influence of the aggressor country, it is necessary to separate the consideration in the national security system of information security and information security of society and the state.
Emphasis is placed on the need to improve the motivational factors for voluntary participation of citizens in identifying threats to information security. Introduction of modern approaches to standardization and verification of software used for automatic translation of texts, dissemination of information on the history, theory and practice of constitutionalism, state building, international policy, implementation of international treaties, dissemination of state statistics and coverage political life of society. Eliminate the preconditions for the dissemination of dangerous information through the use of Internet services provided by the providers of the aggressor country.
Key words: *threat, risk, information security, the individual information security, national security, border security.*

Постановка проблеми в загальному вигляді. Відповідно до пункту 4 статті 3 Закону України «Про національну безпеку», в Україні передбачено вжиття заходів щодо забезпечення інформаційної безпеки [1]. Вирішення цього завдання потребує ідентифікації загроз для більш результативного використання ресурсів суб'єктів сектору безпеки і оборони для захисту національних інтересів і національної безпеки України.

Продовження Російською Федерацією інформаційної агресії проти України потребує розвитку теорії та практики забезпечення інформаційної безпеки держави. Одним зі шляхів її забезпечення може бути імунізація соціуму від шкідливої або небезпечної інформації як альтернатива заходам блокування та компрометації ворожої інформації.

Досвід протистояння російській агресії показує, що найбільш негативними наслідками інформаційної вразливості людини є спроби руйнування конституційного ладу, територіальної цілісності, поширення тероризму, організованої злочинності тощо. Загрози інформаційної безпеки можуть також походити й від громадян України, оскільки будь-яка людина не застрахована від прийняття помилкових рішень, які можуть спричинити шкідливі або небезпечні наслідки. Це потребує дослідження загроз інформаційної безпеки особистості. Їх визначення дає змогу вдосконалити державну інформаційну політику та визначити комплекс заходів в інтересах забезпечення національної безпеки держави та її сталого розвитку.

Аналіз останніх досліджень і публікацій. У контексті забезпечення національної безпеки проблеми інформаційної безпеки досліджувалися І. Романовим, І. Рижовим, В. Городновим, М. Литвиним, Д. Іщенком, В. Кириленком, І. Тонконогом, Н. Чалою, О. Поплавською, Т. Чулітською, І. Матоніте, І. Слісарчуком, О. Мітенкою, І. Мельником та іншими авторами. Переважна кількість досліджень стосується забезпечення інформаційної безпеки суспільства та держави. Разом із тим у сучасній демократичній державі людина визнається найвищою соціальною цінністю. Це потребує дослідження загроз, які безпосередньо впливають на стан інформаційної безпеки особистості.

Мета статті – визначення загроз інформаційної безпеки особистості в інтересах забезпечення національної безпеки держави.

Виклад основного матеріалу. Основні загрози національній безпеці України в політичній, державній, воєнній, економічній, екологічній, правовій, соціальній сферах відображаються в розподілі повноважень і завданнях різних складників сектору безпеки і оборони України. Погоджуємося з думкою, що забезпечення державної безпеки передбачає врегулювання законодавством і реалізацію прав людини та громадянина за умовою гарантування й захисту національних інтересів [2].

На думку І. Мельника, формування інформаційної політики в умовах гібридної війни потребує розвитку інтеграційних здібностей державних інституцій, адаптація їх до загроз, підвищення професійних навичок персоналу органів державної влади [3, с. 139]. У сучасних умовах відношення між державою та громадянським суспільством набуває нових форм на основі компромісів. Легітимізація держави відбувається через взаємодію із суспільством. Набуває актуальності поєднання відповідальності громадян та органів державної влади [4, с. 90]. Останні події в Республіці Білорусь стали прикладом загроз від узурпації влади, радянських принципів державного будівництва, популізму [5, с. 540].

Відповідно до Закону України, національна безпека визначає «захищеність державного суверенітету, територіальної цілісності, демократичного конституційного ладу та інших національних інтересів України від реальних та потенційних загроз» [1]. Визначення національних інтересів потребує обов'язкового врахування й узгодження інтересів людини, суспільства та держави. Основні з них пов'язані із забезпеченням державного суверенітету, розвитком держави, необхідністю створення безпечних умов життєдіяльності громадян. Для суб'єктів прикордонної безпеки – це забезпечення територіальної цілісності; нормативне врегулювання організації діяльності правоохоронних органів; протидія тероризму, нелегальній міграції, контрабандній діяльності, незаконному використанню інформації. Їх виконання пов'язане з необхідністю здійснення протидії відповідним загрозам [6, с. 10].

Проблема забезпечення інформаційної безпеки особистості існувала на всіх історичних етапах розвитку людської цивілізації. Свідчення цього можна знайти в стародавніх релігійних текстах, зокрема в Торі, Ветхому Заповіті, давньоіндійському епосі – Махабхараті тощо. Наприклад, у Корані міститься обов'язкові для всіх правила поведінки. Зокрема, заборона гри в азартні ігри (розпалюють ворожнечу, спричиняють розточення майна) [7, с. 47], обов'язковість залучення свідків під час укладання договорів (попередження конфліктів) [7, с. 64], заборона займатися діяльністю, якої людина не навчена (запобігання негативним наслідкам діяльності людини) [7, с. 335], заборона брати своїх родичів помічниками (протидія корупції) [7, с. 225]. У комедії В. Шекспіра (1564–1616 роки) «Приборкання норовливої» відображено панівне на той час ставлення до жінок. З іншого боку, показано покращення життя головної героїні після того, як вона зрозуміла, що люди часто «оголошують війну тоді, як на колінах слід благати миру» [8, с. 277].

Наведені приклади ототожнюються зі способами передачі знань між поколіннями людей

для запобігання негативним наслідкам їхньої діяльності. У демократичному суспільстві переважаючу роль відіграють норми права. Вони характеризуються суспільною користю, справедливістю, відповідністю реальним потребам суспільства, забезпечують законність і правопорядок.

Юридичні норми мають бути сформульовані й доведені до суспільства таким чином, щоб визначення об'єкту, об'єктивної та суб'єктивної сторони правопорушення не викликало сумніву щодо настання безумовної відповідальності за протиправну діяльність. Це сприятиме їхньому позитивному впливу на особисту й суспільну свідомість.

Сьогодні в законодавстві України існує низка недостатньо врегульованих питань, що знижують ефективність протидії протиправній діяльності. Наприклад, Конституцією України проголошено принцип єдиного громадянства [9]. У Законі України «Про громадянство України» подвійне громадянство заборонено. Відповідальності за це не встановлена [10]. У Кримінальному кодексі України та Кодексі України про адміністративну відповідальність також відсутній опис зазначеного об'єкта правопорушення. Це виключає розгляд таких фактів як правопорушень.

Серед загроз державній безпеці через набуття громадянами України громадянства іншої держави І. Слісарчук та О. Мітенко називають витік наукового потенціалу, передумови до витоку відомостей з обмеженим доступом, формування позицій впливу в інтересах іноземної держави, задоволення територіальних претензій, зниження обороноздатності держави, ухилення від проходження військової служби [11].

В умовах поширення пандемії (COVID-19) виникла потреба формування в людей нової обов'язкової поведінки, що полягає в необхідності захисту інтересів інших осіб від себе шляхом дотримання карантинних обмежень. Після уточнення Законом України «Про внесення змін до Кодексу України про адміністративні правопорушення щодо запобігання поширенню коронавірусної хвороби (COVID-19)» об'єкта правопорушення, що передбачений статтею 44-3 («Порушення правил щодо карантину людей») Кодексу України про адміністративні правопорушення [12], протягом декількох місяців поспіль спостерігалася стійка тенденція зменшення кількості захворілих осіб.

Разом із тим удосконалення норм застосування карантинних обмежень залишається досі актуальним. Потребує уточнення перелік громадських місць, розширення переліку осіб, які мають право складати протоколи про адміністративні правопорушення (зокрема члени громадського формування з охорони громадського порядку й державного кордону; командири (начальники) військових частин (установ, закладів); командири підрозділів, які уповноважені на те командирами (начальниками) військових частин (установ, закладів); посадові особи органів залізничного транспорту; посадові особи військової інспекції безпеки дорожнього руху Військової служби правопорядку у Збройних Силах України; уповноважені посадові особи центрального органу виконавчої влади, який забезпечує реалізацію державної політики з питань безпеки на наземному транспорті [13]).

Погоджуємося з думкою В. Корпаня, що найбільші загрози інформаційній безпеці спричиняють навмисні дії зацікавлених осіб. Вони можуть бути пов'язані з роботою апаратної, програмної та комунікаційної складових комп'ютерної системи [14]. Небажаний інформаційний вплив на людину може бути здійснений зміною алгоритму роботи комп'ютерної програми її розробником або комп'ютерним вірусом. Для зміни тексту на екрані монітору зловмисниками можуть бути використані спеціальні, так звані недруковані символи [15].

Шкода або небезпека особі може бути нанесена шляхом прихованого збору даних про унікальні особливості комп'ютерів, статистики попередніх пошукових запитів. Зазначена інформація дає змогу проводити оцінку політичних симпатій користувача для умисного й дозованого надання йому інформації. Сукупність спеціально підібраної комп'ютерною системою інформації може впливати на свідомість людини, викривлення історичної пам'яті, формування політичних симпатій, розпалювання ворожнечі між певними групами людей, які відрізняються доходами, освітою, політичною зрілістю, мовними, територіальними й іншими ознаками.

Використання в комп'ютерних системах технологій штучного інтелекту дає змогу як приховувати, так і надавати в автоматичному режимі кожному користувачу унікальну викривлену, додану або певним чином інтерпретовану інформацію залежно від змісту електронного пошукового запиту та попередньо накопичених даних про конкретну людину.

Серед стримуючих євроатлантичну інтеграцію України факторів є недостатня обізнаність громадян України щодо основних норм законодавства, особливостей діяльності органів державної влади та місцевого самоврядування європейських країн, певний мовний бар'єр. Також для перешкоджання вибору Україною

європейського вектору Російська Федерація намагається поширювати дезінформацію серед громадян України й міжнародної спільноти. Особливо небезпечні дезінформаційні впливи в прикордонних регіонах, де різняться оцінки спільних історичних подій.

В умовах сучасного розвитку технологій машинного перекладу текстів будь-яка людина може легко долати мовний бар'єр і самостійно розширювати свої знання про особливості законодавства, функціонування публічної влади інших країн, правила перетину державного кордону іноземної держави та перебування на її території. Зазначене програмне забезпечення може бути використано спецслужбами країни-агресора.

Це зумовлено низькою факторів. По-перше, без знання іноземної мови важко виявити розбіжності перекладу й оригіналу тексту. По-друге, досвід використання програмних додатків мережі Інтернет для перекладу побутової лексики може створювати в людини ілюзію якості й універсальності зазначеного інструмента. По-третє, таку дезінформацію складно виявити, оскільки вона генерується на унікальний запит користувача та не зберігається в мережі Інтернет. По-четверте, важко довести в судовому порядку суб'єктивну сторону правопорушення. По-п'яте, модифікація програми-перекладача може бути проведена з використанням шкідливого програмного забезпечення сторонньою особою з території іншої держави.

Такі загрози вже набули актуальності. У мережі Інтернет розміщена електронна версія PDF-документа Європейської комісії щодо плану дій з удосконалення комунікаційної політики [16]. У пункті 4 цього документа описано особливості діяльності спікера. У перекладі чотирьох абзаців цього пункту документа програмним додатком компанії Google [17] двічі додається відсутнє в оригіналі тексту слово «Росія». Скопійоване в буфер обміну речення: «Individual Spokespersons will contribute to the political message and media strategy of communication plans in conjunction with Cabinets and DGs [16]» в автоматичному режимі перекладається так: «Окремі речники будуть сприяти політичному посланню та медіастратегії Росії комунікаційні плани спільно з кабінетами та генеральними директоратами».

Наведені інтерпретації оригінального тексту можуть створювати в користувача додатку машинного перекладу ілюзію залежності політики країн Європейського Союзу від позиції Російської Федерації та її виняткової ролі в розвитку міжнародних стосунків. У перекладах зазначених фрагментів білоруською або іспанською мовами слово «Росія» не додається. Це свідчить про спрямованість інформаційної загрози саме на україномовну частину населення.

Перегляд змісту буферу обміну операційної системи Windows не виявив будь-якого прихованого тексту. Разом із тим після декількох слів (зокрема «political») виявлено послідовність стандартних, так званих не друкованих символів – повернення каретки друкарського пристрою та перехід на новий рядок.

Якщо в буфері обміну видалити зайві спеціальні недруковані символи, то переклад першого речення стає коректним, але PDF-формат файлів був спеціально розроблений для однакової видачі користувачу на різних комп'ютерних платформах. Наведений приклад підтверджує думку, що ключові слова в поєднанні зі стандартними недрукованими символами можуть бути свідомо використані для дезінформації людини.

У мережі Інтернет є безоплатні сервіси для приєднання до сайтів текстової або графічної інформації, яка розміщена на інших сайтах. Якщо такі сайти розміщені в країні-агресорі, то існує загроза заміни її на шкідливу. Така заміна інформації може бути як загальною, так і вибірковою (шляхом аналізу доступної інформації про комп'ютер користувача).

Зв'язок інформаційних загроз із діяльністю людини наведений на рис. 1. Так зовнішні інформаційні загрози зажди трансформуються фільтром сприйняття інформації людини. Від якості розвитку такої здібності шкідлива або небезпечна інформація може не впливати на діяльність або бездіяльність особи. З іншого боку, істотний вплив на дії людини здійснюють сформовані в неї потреби, цінності, знання та переконання. Зазначені елементи обумовлюють потенційні загрози, які можуть вплинути на дії людини.

У ході діяльності людини відбувається трансформація інформаційних загроз як наслідок копіювання поведінки особи іншими людьми, поширення отриманої інформації, формування та розповсюдження нової інформації, яка також може містити нові інформаційні загрози. Крім цього, у процесі діяльності або бездіяльності особи відбувається корегування власних потреб, цінностей, знань, особистих переконань і фільтрів сприйняття інформації.

Загроза інформаційній безпеці особистості – це фактор, який негативно впливає на результати й наслідки діяльності або бездіяльності особи під впливом зовнішньої інформації, особистих потреб, цінностей, знань, переконань людини та стану її фільтру сприйняття реальності. Відповідно, ризик – фактор, який підвищує ймовірність реалізації загрози.

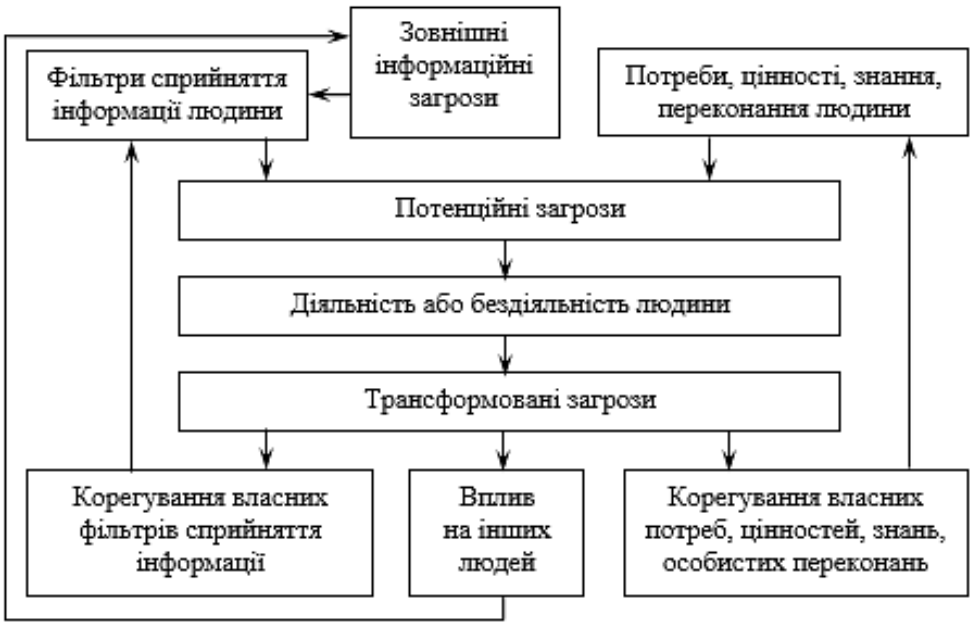

Рис. 1. Зв'язок інформаційних загроз із діяльністю людини

У сферах громадської та прикордонної безпеки доцільно враховувати дві основні класифікаційні ознаки інформаційних загроз особистості: перша – за вагомістю впливу на стан безпеки відповідно до ступеня відповідальності правопорушника (кримінальна, адміністративна, дисциплінарна, цивільна, а також така, що потребує подальшого нормативного врегулювання відповідно до змін, що відбулися в розвитку соціуму); друга – за спрямуванням впливу на правопорушника відповідно до напрямів діяльності суб'єктів громадської та прикордонної безпеки.

До другої класифікаційної ознаки відносяться такі загрози, що загрожують територіальній цілісності держави; пов'язані з розповсюдженням тероризму, зі сприянням організації каналів нелегальної міграції, контрабандної діяльності, незаконному переміщенню через державний кордон товарів і вантажів, зброї та боєприпасів, інших заборонених предметів і речовин; зменшують ефективність взаємодії та співпраці між державними, правоохоронними органами й громадянським суспільством; пов'язані з порушенням нормативно визначеного порядку збору, обробки, зберігання, передачі та розповсюдження інформації; руйнують історичну пам'ять у суспільстві.

Крім цього, загрози можна групувати залежно від впливу природних факторів, відповідності об'єкта правопорушення реальним потребам демократичного та громадянського суспільства.

Висновки. Отже, діяльність держави щодо забезпечення інформаційної безпеки особистості потребує блокування або мінімізації впливу на суспільство інформаційних загроз. Разом із тим шляхом розвитку особистих якостей людини може бути забезпечена імунізація суспільства від небажаної інформації. Це потребує окремого розгляду в системі національної безпеки проблем забезпечення інформаційної безпеки й інформаційної безпеки особистості, удосконалення адміністративних, економічних, правових, соціально-психологічних механізмів державного управління.

В умовах розвитку систем штучного інтелекту збільшуються загрози інформаційній безпеці особистості від технологій обробки інформації в мережі Інтернет. Це вимагає запровадження стандартизації та верифікації програмного забезпечення (особливо систем автоматичного перекладу), яке використовується для поширення інформації з питань історії, теорії та практики конституціоналізму, державного будівництва, міжнародної політики, виконання міжнародних договорів, поширення державної статистики й висвітлення політичного життя суспільства. Також є потреба в усуненні передумов до поширення небезпечної інформації через використання Інтернет-сервісів, що надаються провайдерами країни-агресора. Потребують удосконалення мотиваційні фактори щодо участі громадян у виявленні загроз інформаційній безпеці.

Напрямом подальших досліджень може бути формування структури та змісту Концепції забезпечення інформаційної безпеки особистості.

ЛІТЕРАТУРА:

1. Про національну безпеку : Закон України від 21 червня 2018 року № 2469-VIII. URL: https://zakon.rada.gov.ua/laws/show/2469-19#Text (дата звернення: 12.01.2021).

2. Романов І.В., Рижов І.М., Тонконог І.О. Методологія комплексного оцінювання розвитку національних інтересів України в секторі економічної та державної безпеки. *Інформаційна безпека людини, суспільства, держави.* 2019. № 3 (27). URL: http://academy.ssu.gov.ua/ua/page/page_1581426025.htm (дата звернення: 12.01.2021).

3. Melnyk I. Principles of Formation of Information Policy of Ukraine In the Conditions of Hybrid War. *Krakowskie Studia MałopolskieIssue*. 2020. № 2 (26). P. 136–149. URL: https://doi.org/10.15804/ksm20200209 (дата звернення: 12.01.2021).

4. Chala N.D., Poplavska O.M. Transforming the Relations between State and Society in the Context of the 4th Industrial Revolution: Ukraine's Experience. *Public Policy and Administration.* 2020. Vol 19. № 1. P. 89–98.

5. Chulitskaya T., Matonyte I. Social security discourses in a non-democratic state: Belarus between Soviet paternalistic legacies and neo-liberal pressures. *Public Policy and Administration.* 2020. Vol 17. № 4. P. 539–554.

6. Теоретичні основи інформаційно-аналітичного забезпечення процесів охорони державного кордону (у контексті завдань національної безпеки України в прикордонній сфері) : монографія / В.П. Городнов, М.М. Литвин, Д.В. Іщенко, В.А. Кириленко. Хмельницький : НАДПСУ, 2009. 473 с.

7. Коран. Дніпропетровськ : Середняк Т.К., 2015. 760 с.

8. Шекспір В. Вибрані твори : у 2 т. Київ : Мистецтво, 1952. Т. 2. С. 277.

9. Конституція України : Закон України від 28.06.1996 № 254к/96-ВР зі змінами. URL: http://zakon2.rada.gov.ua/laws/show/254к/96-вр (дата звернення: 12.01.2021).

10. Про громадянство України : Закон України від 18 січня 2001 року № 2235-III. URL: https://zakon.rada.gov.ua/laws/show/2235-14#Text (дата звернення: 12.01.2021).

11. Слюсарчук І.В., Мітенко О.В. Подвійне громадянство: реальні та потенційні загрози національній безпеці. Законодавче регулювання. *Інформаційна безпека людини, суспільства, держави.* 2019. № 3 (27). URL: http://academy.ssu.gov.ua/ua/page/inf-arch.htm (дата звернення: 12.01.2021).

12. Про внесення змін до Кодексу України про адміністративні правопорушення щодо запобігання поширенню коронавірусної хвороби (COVID-19) : Закон України від 06.11.2020 № 1000-IX. URL: https://zakon.rada.gov.ua/laws/show/1000-20#Text (дата звернення: 12.01.2021).

13. Кукін І.В. Окремі питання зміцнення інформаційної безпеки особистості у період пандемії COVID-19. *Публічне управління і адміністрування в Україні.* 20020. № 18. С. 114–118. URL: https://doi.org/10.32843/pma2663-5240-2020.18.21 (дата звернення: 12.01.2021).

14. Корпань В.Я. (2015) Класифікація загроз інформаційній безпеці в комп'ютерних системах при віддаленій обробці даних. *Реєстрація, зберігання та обробка даних*. 2015. № (17). P. 39–46. URL: http://dspace.nbuv.gov.ua/bitstream/handle/123456789/131565/04-Korpan.pdf?sequence=1 (дата звернення: 12.01.2021).

15. Коды ASCII символов. URL: http://azjio.narod.ru/autoit3_docs/appendix/ascii.htm (дата звернення: 12.01.2021).

16. Communication to the Commission action plan to improve communicating Europe by the Commission. Commission of the European Communities. SEC(2005) 985 final. URL: https://ec.europa.eu/transparency/documents-register/api/files/SEC(2005)985_0/de00000000825448?rendition=false.

17. Google Переводчик. URL: https://translate.google.com.ua/?hl=ru&tab=wT&sl=en&tl=uk&op=translate (дата звернення: 12.01.2021).