УДК: 340:659.4.327.88(477)
DOI: https://doi.org/10.32689/2617-2224-2019-17-2-154-173

Лисенко Сергій Олексійович,
кандидат юридичних наук, доцент, доцент кафедри управління безпекою, правоохоронної та антикорупційної діяльності, Міжрегіональна Академія управління персоналом, 03039, м. Київ, вул. Фрометівська, 2, тел.: (044) 490 95 00, e-mail: crimeconsult@ukr.net

ORCID: 0000-0002-7050-5536

Лысенко Сергей Алексеевич,
кандидат юридических наук, доцент, доцент кафедры управления безопасностью, правоохранительной и антикоррупционной деятельности, Межрегиональная Академия управления персоналом, 03039, г. Киев, ул. Фрометовская, 2, тел .: (044) 490 95 00, e-mail: crimeconsult@ukr.net

ORCID: 0000-0002-7050-5536

Lysenko Serhiy Oleksiyovych,
PhD in Law, Associate professor, Associate professor of the Department of Security Management and Law Enforcement and Anti-Corruption Activities, Interregional Academy of Personnel Management, 03039, Kyiv, Str. Frometivska, 2, tel.: (044) 490 95 00, e-mail: crimeconsult@ukr.net

ORCID: 0000-0002-7050-5536

СУЧАСНІ ТЕНДЕНЦІЇ РОЗВИТКУ ІНФОРМАЦІЙНОЇ БЕЗПЕКИ ЯК ОБ'ЄКТА ПРАВОВІДНОСИН

Анотація. Розглядаються питання, пов'язані з досвідом розвинених країн щодо інформаційної безпеки як об'єкта правовідносин та національного досвіду у структурі інформаційного права, як комплексної галузі у правовому полі України.

Проблематика інформаційної безпеки вже знайшла своє відображення у чинному законодавстві України. Зокрема, Конституція України та ряд інших нормативно-правових актів розглядають інформаційну безпеку на рівні з суверенітетом та територіальною цілісністю. Це стосується, насамперед, інформаційної безпеки як складової національної безпеки. Однак з часом дедалі більше уваги дослідники приділяють інформаційній безпеці не лише на рівні держави, а й на рівні окремих суб'єктів правовідносин.

У межах дослідження зміст поняття “інформаційна безпека” пропонується розуміти, як виокремлений вид суспільної діяльності, пов’язаної зі створенням, обігом та використанням інформації певними суб’єктами, що знаходить вираз у нормах правил поведінки щодо її охорони, захисту, збереженню, підтриманню життєво важливих потреб, інтересів людей, соціальних спільнот, суспільства, держави, міжнародного співтовариства.

У процесі дослідження аналізується досвід формування системи правового регулювання інформаційної (у тому числі комп’ютерної) безпеки США, Сполученого Королівства Великої Британії та Північної Ірландії, Ізраїлю, ФРН. Приклад Ізраїлю видається особливо цінним для України. Налагодження ефективної системи інформаційної безпеки потребує виділення значної частки валового внутрішнього продукту на потреби науково-технічних досліджень військового спрямування. Не менше цікавим видається досвід створення центрів інформаційно-технологічного розвитку на кшталт ізраїльських центрів “Мамрам” та “8200”.

Інформаційна безпека як на рівні держави, так і на рівні окремих суб’єктів правовідносин потребує формування розгалуженого та збалансованого законодавства, належного фінансування тощо. Окремою проблемою постає співвідношення потреб безпеки, прав і свобод громадян. Усе це вимагає врахування провідного зарубіжного досвіду. Однак формування надійної системи інформаційної безпеки держави є вкрай важливим для України, а тому потребує консолідації всіх сил.

Ключові слова: право, інформаційна безпека, інформаційне право, зарубіжний досвід, інформаційно-технологічний розвиток.

СОВРЕМЕННЫЕ ТЕНДЕНЦИИ РАЗВИТИЯ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ КАК ОБЪЕКТ ПРАВООТНОШЕНИЙ

Аннотация. Рассматриваются вопросы, связанные с опытом развитых стран по информационной безопасности как объекта правоотношений и национального опыта в структуре информационного права, как комплексной отрасли в правовом поле Украины.

Проблематика информационной безопасности уже нашла свое отражение в действующем законодательстве Украины. В частности, Конституция Украины и ряд других нормативно-правовых актов рассматривают информационную безопасность на уровне с суверенитетом и территориальной целостностью. Это касается, в первую очередь, информационной безопасности как составляющей национальной безопасности. Однако со временем все больше внимания исследователи уделяют информационной безопасности не только на уровне государства, но и на уровне отдельных субъектов правоотношений.

В рамках исследования содержание понятия “информационная безопасность” предлагается понимать как отдельный вид общественной деятельности, связанной с созданием, обращением и использованием информации

определенными субъектами, который выражается в нормах правил поведения касательно ее охраны, защиты, сохранения, поддержания жизненно важных потребностей, интересов людей, социальных общностей, общества, государства, международного сообщества.

В процессе исследования анализируется опыт формирования системы правового регулирования информационной (в том числе компьютерной) безопасности США, Соединенного Королевства Великобритании и Северной Ирландии, Израиля, ФРГ. Пример Израиля представляется особенно ценным для Украины. В первую очередь, налаживание эффективной системы информационной безопасности требует выделения значительной части валового внутреннего продукта на нужды научно-технических исследований военной направленности. Не менее интересным представляется опыт создания центров информационно-технологического развития вроде израильских центров "Мамрам" и "8200".

Информационная безопасность как на уровне государства, так и на уровне отдельных субъектов правоотношений требует формирования разветвленного и сбалансированного законодательства, надлежащего финансирования и тому подобное. Отдельной проблемой является соотношение потребностей безопасности, прав и свобод граждан. Все это требует учета ведущего зарубежного опыта. Однако формирование надежной системы информационной безопасности государства является крайне важным для Украины, а потому требует консолидации всех сил.

Ключевые слова: право, информационная безопасность, информационное право, зарубежный опыт, информационно-технологическое развитие.

MODERN TRENDS OF INFORMATIONAL SECURITY DEVELOPMENT, AS A LITERARY OBJECTIVE

Abstract. This article deals with issues related to the experience of developed countries on information security as an object of legal relations and national experience in the structure of information law as a complex industry in the legal field of Ukraine.

The issue of information security is already reflected in the current legislation of Ukraine. In particular, the Constitution of Ukraine and a number of other regulatory acts consider information security at a level with sovereignty and territorial integrity. This concerns, first of all, information security as a component of national security. However, over time, more and more attention of researchers is paid to information security, not only at the state level, but also at the level of individual subjects of legal relations.

As part of the study, the content of the concept of "information security" is proposed to be understood as a selected type of public activity related to the creation, circulation and use of information by certain subjects, which is expressed in the norms of the rules of conduct regarding its protection, protection, preservation and maintenance of vital needs, interests of people social communities, society, state, international community.

In the course of the research, the author analyzes the experience of forming a system of legal regulation of information (including computer) security of the United States, The United Kingdom of Great Britain and Northern Ireland, Israel, and the Federal Republic of Germany. The example of Israel is especially valuable for Ukraine. First of all, the establishment of an effective information security system requires the allocation of a significant part of the gross domestic product to the needs of scientific and technical studies of a military nature. No less interesting is the experience of creating information technology development centers like the Israeli Mamram and 8200.

Information security both at the state level and at the level of individual subjects of legal relations requires the formation of extensive and balanced legislation, adequate funding, and the like. A separate problem is the ratio of security needs and the rights and freedoms of citizens. All this requires taking into account the leading foreign experience. However, the formation of a reliable information security system of the state is extremely important for Ukraine, and therefore requires the consolidation of all forces.

Keywords: law, information security, information law, foreign experience, information technology development.

Постановка проблеми. Безпека інформаційної діяльності в Україні постійно заслуговує уваги, а отже, визнання її як важливої складової життєдіяльності різних суб'єктів суспільства. Діяльність окремих суб'єктів в інформаційній сфері має певний вплив на життєдіяльність держави загалом. Інформаційна безпека визначає її роль у регулюванні, охороні та захисті різних суспільно значущих правовідносинах та окремих процесах. Завдяки цьому можуть визначатися головні напрями державної політики та зміст діяльності держави та недержавних органів, пов'язаної з управлінням інформаційної сфери у суспільстві. Основною в цьому напрямі є інформаційна безпека як спосіб управління. В усьому світі вже давно прийнято за норму управління залежно від небезпек. Сенс цього виникає від того, що ті інтереси організацій, що мають високі показники та досягнення, не потребують адміністративного втручання, а ті, що мають якісь загрози, потребують адміністративної уваги та втручання. Тому на перший план постає саме інформаційна безпека як важель управління організацією.

Норма ч. 1 ст. 17 Конституції України [1] встановлює, що "захист суверенітету і територіальної цілісності України, забезпечення її економічної та інформаційної безпеки є найважливішими функціями держави, справою всього українського народу". Таким чином, у правовідносинах в Україні інформаційна безпека розглядається на рівні з суверенітетом і територіальною цілісністю, а також з економічною безпекою. Згадані конституційно-правові складові безпеки країни розвиваються у спеціальному

законодавстві України, за окремими напрямами регулювання, у різних часових межах існування незалежності сучасної української держави.

У Декларації про державний суверенітет України зазначено, що державний суверенітет — це "верховенство, самостійність, повнота і неподільність влади Республіки в межах її території та незалежність і рівноправність у зовнішніх зносинах" [2]. З цього випливає, що сенс інформаційної безпеки, як складової національної безпеки визначається з того, що її джерелом вважається не лише суверенітет держави, а й суверенітет осіб та організацій як суб'єктів інформаційних відносин.

Не так давно у дослідженнях науковців головним суб'єктом інформаційної безпеки вважалася держава. Більшість дослідників дотримувались думки, що проблема охорони, захисту, підтримки, збереження інформаційної безпеки з'явилася багато століть тому. При цьому домінувала концепція, що ключове поняття предмета інформаційної безпеки становить збереження таємниці інформації, що по-різному простежується з давніх часів. Аргументами цього є згадки про перші методики шифрування повідомлень у різних галузях людської діяльності. Вони датуються 4 тис. р. до н. е. Наприклад, одним із ранніх підставних шифрів був Шифр Цезаря, в якому кожна літера у повідомленні замінювалась літерою через декілька позицій із абетки. Цей шифр отримав ім'я Юлія Цезаря, який його використовував (зі зсувом у 3 позиції) для спілкування з генералами під час військових кампаній [3, с. 35–40].

З плином історії змінювалося ставлення у суспільстві щодо розуміння сутності інформаційної безпеки. Загальний, консолідований об'єкт чи предмет правовідносин, інформаційна безпека стала виділятися змістом спеціальних прав і обов'язків.

Аналіз останніх публікацій та досліджень. В Україні цією проблемою займаються такі науковці-правознавці: Н. В. Банчук, Г. В. Виноградова, О. Д. Довгань, Р. А. Калюжний, К. І. Бєляков, Б. А. Кормич, О. В. Копан, А. І. Марущак, А. І. Мовчан, Е. І. Низенко, В. Г. Пилипчук, А. М. Подоляка та ін.

Зміст категорії "інформаційна безпека" дослідниками визначається із змісту загального поняття "безпека". Вона розуміється, в широкому сенсі, як стан захищеності, а в спеціальному — як суспільні відносини, вид правовідносин. Деякі питання історії правових досліджень інформаційної безпеки у суспільстві залишаються несистематизованими для включення у склад адміністративного права або інформаційного права.

Для цілей нашого дослідження зміст поняття "інформаційна безпека" пропонується розуміти як виділений вид суспільної діяльності, пов'язаної із створенням, обігом та використанням інформації певними суб'єктами, що знаходить вираз у нормах правил поведінки стосовно її охорони, захисту, збереженню, підтриманню життєво важливих потреб, інтересів людей, соціальних спільнот, суспільства, держави, міжнародного співтовариства.

Формулювання цілей статті. На основі системного прикладного ана-

лізу нормативно-правових актів та компаративістського підходу зарубіжного досвіду пропонуються окремі результати наукового аналізу стосовно розвитку досліджень суспільного розуміння інформаційної безпеки у світі, а також місце її в інформаційному праві як комплексній галузі правознавства.

Виклад основного матеріалу дослідження. Сучасне інформаційне право оперує в суспільних відносинах, що виникають, здійснюються та припиняються у взаємодії суб'єктів через інформацію. Право своїм головним компонентом має функцію забезпечення, а саме: дотримання бажаних у суспільстві норм правил поведінки суб'єктів і недопущення відхилень, що визначає зміст правопорядку [4, с. 13–14].

Суттєвим історичним етапом в українському суспільстві на шляху створення єдиного погляду на інформаційні відносини та, відповідно, інформаційну безпеку було прийняття Закону України "Про інформацію" [5]. Однак у цьому Законі формулювання інформаційної безпеки не було подано.

Як свідчать дослідники-правники, спостерігаються методологічні відмінності щодо розуміння інформаційної безпеки на різних рівнях суспільних відносин (національному, державному, регіональному, окремих організацій тощо). Окремий підхід був застосований до правового відображення організації безпеки Єдиного державного реєстру виконавчих проваджень України. Цей підхід не відрізняється від підходу до організації безпеки локальної мережі в окремому підприємстві. Це зумовлює необхідність визначення подібних, уніфіковано-нормативних методів, моделей охорони і захисту інформації щодо будь-якого суб'єкта.

Вважається, що одними з перших проблеми комп'ютерної інформаційної безпеки усвідомили і зробили впевнений крок до їх вирішення державні відомства США наприкінці 60-х років XX ст., коли комп'ютери коштували великих грошей, а Інтернет зароджувався з нечисленних, виключно військових і наукових інформаційних мереж [6, с. 17].

Щодо парадигми інформаційної безпеки суспільства. Кожна людська спільнота має свою систему цінностей у контексті інформаційної безпеки. Вона обумовлена історією і менталітетом народу, у складі якого існує будь-яка спільнота. Ця система цінностей вироблена досвідом попередніх поколінь окремих соціальних груп, корпорацій тощо. Руйнування цінностей спільноти неминуче веде до негативних суспільних наслідків.

До останнього часу проблема комплексності інформаційної безпеки людини, соціальних спільнот, суспільства, держави в Україні розглядалися фрагментарно. Вважалося, що тільки шляхом введення правового режиму секретності, декларуваннями різних юридичних обмежень у сфері збереження, передачі та поширення інформації, можна вирішити проблеми її підтримки, гарантування та охорони.

Незважаючи на те, що інформаційна безпека як окрема проблема була сформульована тільки в період інтенсивної комп'ютерно-телекомунікаційної інформатизації, вона має загальний характер. Вона існує стіль-

ки, скільки існує людство, просто її інакше називали і виявлялася вона в усіх сферах діяльності людей, товариств і держав. У цю епоху виникає небезпека, на яку вказував професор Масуда, автор створеної на початку 70-х років Концепції інформатизації Японії. Він побоювався, що люди і машини, прагнучі до побудови демократичної держави, реалізації ідеї відкритого суспільства, можуть створити поліцейську державу [7].

Інша проблема може бути розглянута, наприклад, з аналізу кризи 30-х років, зробленого одним з найавторитетніших соціологів світу Питиримом Сорокіним. Він намагався знайти відповідь на питання: що призвело до появи таких людей, як Гітлер, Муссоліні, Сталін? На думку Сорокіна, виною тому є три причини, кожна з яких інформаційного походження. Перша — криза в системі права, друга — криза в системі істин, третя — криза в системі культури і мистецтв. І ще одна проблема, залишена без уваги і в документах, і в численній літературі з питань інформаційної безпеки. Це проблема обміну інформації, яка заслуговує окремого розгляду [7].

Дослідження світового досвіду в цьому напрямі залишається особливо корисним для вітчизняних науковців. Тому подальше освітлення та вивчення становлення розуміння інформаційної безпеки у світі є важливим кроком до удосконалення українського права. Особливу увагу пропонується звернути на країни, де генеруються світові, передові технології, моделі здійснення комплексної організації інформаційної безпеки.

Звернемо увагу на зарубіжний досвід комплексності вивчення питань інформаційної безпеки, що виникають під впливом загроз масового розповсюдження нових інформаційних технологій. У 1967 р. під наглядом Національного Комітету Стандартів США була заснована Ініціативна група дослідників з питань комп'ютерної безпеки. До неї увійшли представники університетів, компаній з виробництва комп'ютерів, науково-дослідних центрів та інших організацій. Результатом такого об'єднання зусиль промислових і наукових фахівців США було сформовано так звану умовно "райдужну серію" — ряд національних стандартів і вимог до обладнання, програмного забезпечення та персоналу різних систем автоматичної обробки даних, що належали таким державним структурам США, як: NASA, Міністерство Оборони, Національний комітет стандартів, Міністерство Праці, Офіс з охорони навколишнього середовища, Міністерство з контролю за озброєнням, Національне наукове товариство, Федеральна резервна система та Центр Об'єднаного Командування Збройних Сил. За такою моделлю у перспективі було створено Національний Центр Комп'ютерної Безпеки, який займався цими питаннями вже системно у прикладному аспекті, цілеспрямовано і комплексно, координуючи дослідників із державних і приватних організаційних структур [8].

У 1981 р. було створено подібний за сутністю спеціальний центр при Міністерстві Оборони США, який розробив і впровадив спеціалізова-

ну "райдужну серію" у 1985 р. Найбільш значущим для оцінки якості комерційних електронно-цифрових виробів, що обробляють і зберігають конфіденційну інформацію, став стандарт "Критерії оцінки довірених комп'ютерних систем", названий Помаранчевою книгою (через помаранчевий колір обкладинки). Вона нині розглядається як зразковий (модельний) світовий стандарт, у тому числі стосовно специфікації на лазерний аудіо-диск і на шейдерну модель OpenGL. Вже за традицією, хоча й удосконалені, стандарти комп'ютерної безпеки в різних країнах також називають "Помаранчевими книгами". Модельною ознакою таких стандартів є максимальна гнучкість і універсальність оцінки інформаційної безпеки різних суб'єктів суспільних відносин в умовах функціонування їх в Інформаційному Суспільстві (на глобальному рівні комп'ютерної телекомунікації) [6].

Як шлях до формування універсальних моделей організації інформаційної безпеки на транскордонному рівні можна розглядати міжнародні нормативно-правові акти. Зокрема в Меморандумі про взаєморозуміння щодо співробітництва у сфері телекомунікацій і розвитку Всесвітньої інформаційної інфраструктури між урядами України та США сторони наголосили на своєму намірі керуватись принципами створення Всесвітньої інформаційної інфраструктури, для чого впроваджувати приватні інвестиції, конкурентний ринок, гнучку регулюючу систему, доступ без дискримінації та універсальне обслуговування. Такі підходи були зафіксовані у рішеннях Першої Всесвітньої конференції з розвитку телекомунікації Міжнародного союзу електрозв'язку (Буенос-Айрес, 1994 р.) [9].

Інформаційна безпека Великобританії має власну історію та власні риси. Великобританія не має власного тексту конституції. У 1998 р. британський парламент затвердив Акт "Про права людини", що надає "Європейській конвенції з прав людини" силу закону. Цей акт набрав чинності у жовтні 2000 р.

У липні 1998 р. британський парламент прийняв Закон "Про захист інформації", що приводить аналогічний Закон 1984 р. у відповідність до вимог Директиви "Про захист інформації", прийнятої Європейським Союзом. Цей закон поширюється на облікові записи, що ведуться державними установами та приватними компаніями. Він накладає ряд обмежень на використання персональних даних та на доступ до облікових записів. Крім того закон зобов'язує юридичні особи, які ведуть такі записи, реєструватися в Комісаріаті по захисту інформації.

Створений Комісаріат по захисту інформації є незалежним агентством, що забезпечує дотримання вимог закону. У 1997–1998 рр. Комісаріат прийняв понад 4 тис. скарг і видав керівні інструкції для приватних працівників, фінансових посередників і агентств з відстеження боргових зобов'язань.

Положення про недоторканність приватного життя та інформації містяться і в інших законодавчих актах, зокрема, в законах, що регламентують ведення медичних записів і зберігання інформації про споживчі

кредити. У цю ж групу входять закони "Про реабілітацію правопорушників" (1974 р.), "Про телекомунікації" (1984 р.), "Про поліцію" (1997 р.), "Про мовлення" (1996 р.), "Про захист від переслідувань" (1997 р.). Положення вказаних законів постійно доповнюються або частково скасовуються у зв'язку з прийняттям Закону "Про захист інформації" в редакції 1998 р. Закон "Про показання свідків для поліції та органів слідства у кримінальних справах" (1984 р.) дає поліції право входити в приватні оселі й проводити там обшуки без ордера, якщо господарь арештований за вчинення правопорушення. І хоча до арешту поліція не має права вимагати від людини документів, їй дозволено зупиняти і обшукувати на вулиці будь-кого, хто викликає підозру. Кожен, кого заарештовано, здає пробу ДНК для включення в національну базу даних [9].

Закон "Про перехоплення комунікаційних повідомлень", прийнятий у 1985 р., встановлює ряд обмежень, які мають відношення до контролю над телекомунікаційними засобами. У червні 1999 р. Міністерство внутрішніх справ видало рекомендації з установки підслуховуючих пристроїв, які передбачають внесення численних поправок до чинного законодавства. Прогнозується забезпечення сприяння встановленню підслуховуючих пристроїв з боку провайдерів інтернет-послуг. Продовжується термін дії таких пристроїв до трьох місяців. Дозволяється використання підслуховуючих пристроїв з можливостями роумінгу. Проте такі проблеми, як контроль з боку судових органів та державний нагляд за перехопленнями інформації у рекомендаціях зовсім не зачіпаються.

Протягом двадцяти років неодноразово робилися кроки до прийняття закону "Про свободу інформації". "Кодекс практики доступу до урядової інформації", прийнятий у 1994 р., відкриває доступ до державних архівів, але передбачає 15 серйозних винятків. Особи, чиї заявки на отримання інформації були відхилені, можуть звернутися зі скаргою через парламентського міністра до парламентського омбудсмена. У травні 1999 р. уряд Великобританії виніс на обговорення проект закону, що дозволяє доступ до урядових архівів і передбачає введення поста комісара з питань інформації, покликаного забезпечувати виконання законів. Цей проект, що містить ряд істотних винятків, вважається навіть більш слабким документом, ніж чинний кодекс. Він був жорстко розкритикований багатьма політиками, які дотримуються різних політичних поглядів, а також неурядовими організаціями. "Компанія на захист свободи інформації", "Хартія-88" і 23 інших організації у червні 1999 р. розгорнули акцію з вимогою перегляду проекту закону. У відповідь на критику міністр внутрішніх справ Джек Строу заявив про свій намір переписати ряд положень, але виправлений варіант проекту досі не опублікований [10].

Парламент Шотландії також пообіцяв в якості одного з першочергових заходів прийняти сильніший закон "Про свободу інформації". Чинний британський закон "Про свободу інформації" передбачає ряд обмежень.

Закон "Про дотримання державних секретів" лежить в основі звинувачень, що висуваються в даний час проти Торі Герагті, автора книги "Ірландська війна", яка детально описує техніку стеження, що використовується в Північній Ірландії і Великобританії поліцією і спецслужбами.

Сполучене Королівство є членом Ради Європи, що підписала і ратифікувала Конвенцію "Про захист осіб у зв'язку з автоматизованою обробкою персональних даних" разом із Європейською конвенцією "Про захист прав і основоположних свобод людини". Крім того, Великобританія входить в Організацію з економічного співробітництва та розвитку. Вона прийняла Директиву ОЕСР про захист недоторканності приватного життя і міжнародних обмінів персональними даними.

Кожен з британських протекторатів — острови Мен, Гернсі і Джерсі має власний закон і власну комісію із захисту персональних даних.

Уряд Великобританії 11 грудня 2014 р. оприлюднив деякі дані про "Національну програму інформаційної безпеки" (National Cyber Security Programme), що спрямована на боротьбу з кіберзлочинцями і захист державних інтересів. Стало відомо, куди планується витратити гроші з бюджету програми, щорічний обсяг якого перевищує 200 млн фунтів стерлінгів [11].

У 2015 р. велика частка грошових коштів була виділена на "зміцнення спроможності вести суверенну боротьбу з загрозами". Ця стаття витрат передбачала фінансування британської спецслужби GCHQ (аналог американського ЦРУ), яка стоїть на сторожі ключових мереж національного значення. У 2015 р. GCHQ ділилася великою кількістю інформації про кіберзагрози з комунікаційними компаніями, щоб ті змогли посилити захист своїх мереж.

Приблизно 30 млн фунтів стерлінгів з Національної програми інформаційної безпеки були витрачені на залучення оборонного відомства для боротьби з хакерами. При цьому у збройних сил є власні програми (бюджет — близько 500 млн фунтів стерлінгів) в галузі інформаційної безпеки.

У 2014 р. уряд Великобританії повідомив про те, що хакери, спонсоровані владою деяких східних країн, зуміли зламати захищену локальну мережу національного рівня. Оборонна промисловість давно є мішенню для кіберзлочинців, що полюють за військовими секретами.

Іншими статтями витрат урядової програми боротьби з хакерами є поліпшення реагування поліції на кібератаки і підвищення рівня інформованості населення.

У звіті також повідомляється, що 81 % великих організацій і 60 % компаній невеликого розміру зіткнулися з незаконним проникненням в їх комп'ютерні системи. Розміри збитків від таких зломів становили від 65 до 115 тис. фунтів стерлінгів для маленьких підприємств і 600–1150 тис. фунтів стерлінгів для великого бізнесу.

Політика захисту урядової секретної інформаціїв Великобританії визначається керівництвом Security Policy Framework (SPF) [12], яке замінило раніше існуючий документ

Manual of Protective Security (MPS). SPF містить основні принципи політик безпеки і керівництво з управління безпекою та ризиками для державних установ Великобританії і пов'язаних з ним органів. SPF включає близько 70 рекомендацій у сфері політики інформаційної безпеки, згрупованих у 7 розділів:

1. Управління ризиками.
2. Контроль доступу та засекречування інформації.
3. Персонал, відповідальний за інфо-безпеку.
4. Забезпечення інформаційної безпеки.
5. Фізична безпека.
6. Боротьба з тероризмом.
7. Безперервність бізнесу.

Зміст SPF розроблено частково Управлінням безпеки апарату Кабінету міністрів Великобританії, частково Центром урядового зв'язку, головним органом Великобританії у сфері криптографії і захисту урядової інформації [7].

Серед країн, чий досвід у галузі інформаційної безпеки може бути корисним для вивчення та запозичення, виокремлюється Ізраїль. Шлях становлення національної та інформаційної безпеки має свої виняткові риси. Стикаючись з безліччю унікальних геополітичних проблем, засновники Ізраїлю розуміли, що успішне становлення нації буде залежати від їхніх знань, винахідливості та уяви. Негативне оточення, в якому розташований Ізраїль, примусило його швидко формувати збройні сили і розвідувальні підрозділи, які здатні вести безперервну війну. Необхідність постійного забезпечення безпеки стала рушійною силою винахідливості, яка буде поширюватися з цієї крихітної країни по всьому світу. Ізраїльтяни, твердо засвоївши той факт, що інновації є гарантією національної безпеки, направили свої зусилля і вміння на розробку високих технологій у різних сферах.

Розвідувальні служби постійно були зайняті розробкою і впровадженням нових і неординарних способів перехоплення ворожих передач, їх розшифрування і аналізу, яким би чином вони не передавалися та з яких джерел вони б не виходили. З моменту своєї появи закритий світ електронної розвідки існував в обстановці практично повної секретності. З цієї причини розвідувальні служби та підрозділи не могли замовляти зовнішнім постачальникам спеціальне обладнання і неординарні технології. Замість цього їм доводилося покладатися на власні розробки і методи. Як наслідок, це дало поштовх до появи і розвитку інновацій, що дали початок найбільш передовим технологіям. На відміну від багатьох своїх сусідів ізраїльтяни не могли просто бурити свердловини і добувати нафту. Головним їхнім ресурсом були власні мізки. З найперших днів в якості громадян нової держави вони перетворили науку на знаряддя становлення нації.

Імміграція стала тим важелем, який привів у рух колесо ізраїльського суспільства, перетворюючи його в свого роду упорядкований хаос. Постійний потік іммігрантів формував культуру, яка перебувала у безперервному русі. З цієї комбінації різних біографій, навичок і умінь вийшла яскрава мозаїка взаємних зав'язків і взаємних впливів. Завдя-

ки цим умовам створювалось правове інформаційне поле та адміністративні засади інформаційної безпеки.

У дні становлення Ізраїлю Давид Бен-Гуріон зробив правильний висновок, що інформаційна безпека країни повинна ґрунтуватися на розвитку науки. Внутрішній розвиток завжди був критично важливим для країни, тим більше, що потреби армії у зброї вже не могли бути задоволені поставками ззовні. Не дивно, що кожен новий уряд Ізраїлю виділяв значну частку внутрішнього валового продукту країни на оборону, асигнуючі значні кошти на науково-технічні дослідження. Згідно з опублікованими даними у 2002 р. Ізраїль виділив на потреби збройних сил 8,97 млрд дол., що становить 8,75 % внутрішнього валового продукту. Для порівняння, Єгипет з населенням, яке майже в 10 разів перевищує населення Ізраїлю, виділив на ті самі цілі приблизно вдвічі менше, ніж його східний сусід. На забезпечення національної безпеки Ізраїль витрачає більше, ніж на будь-які інші потреби. Під час виборів 2003 р., коли економіка країни перебувала у вкрай занедбаному стані, а рівень безробіття становив майже 10 %, проблеми безпеки, що вважалися пріоритетом номер один, допомогли Аріелю Шарону зайняти посаду прем'єр-міністра.

Приблизно в цей час було створено центр "Мамрам", якому належало зіграти важливу роль в інформаційно-технологічному розвитку. Саме він допоміг перетворити країну кибуців і огранщиків алмазів в одну з найбільш економічних, високотехнологічних систем світу. Усі підрозділи збройних сил володіють комп'ютерними та науково-дослідними центрами, укомплектованими персоналом, який пройшов навчання в "Мамрам". Крім військової розвідки "Мамрам" відповідає за інфраструктуру систем передачі даних, впровадження нових технологій [7].

Спочатку "Мамрам" використовував Philco в основному для обробки даних і досліджень логістики. Однак для експлуатації, управління та обслуговування система вимагала фахівців, здатних забезпечити безперебійну роботу обладнання в умовах гарячого і вологого клімату. Особливе занепокоєння доставляли комахи, які проникали всередину апаратури, звідси і виникло словосполучення "комп'ютерні жуки" (computer bugs). Оскільки комп'ютерний центр був сформований за кілька років до того, як інформатика стала академічною дисципліною, "Мамрам" створив власну школу навчання комп'ютерній науці. Випускники цієї школи сформували значне співтовариство фахівців з інформаційних технологій. Багато хто прагне потрапити у цей підрозділ, оскільки всі, хто відслужили в ньому, стають найбільш затребуваними у цивільних професіях. Вироблений у цьому підрозділі особливий підхід (у стилі командос) до вирішення завдань будь-якої складності, а також вміння його фахівців знаходити винахідливі рішення швидкими і неординарними методами, високо затребувані ізраїльським суспільством у галузях інформаційної безпеки підприємництва.

З моменту заснування Ізраїль фактично не знав, що таке мирне

життя, при цьому кожна з воєн була не чим іншим, як війною за виживання. Для ізраїльтян усі регіональні конфлікти так само пам'ятні, як для американців їх відомі чемпіонати з бейсболу: війна за незалежність (1948), Синайська кампанія (1956), Шестиденна війна (1967), війна на виснаження (1969–1971), війна Йом Кіппур (1973), війна з Ліваном (1982), перша інтифада (1987), війна у Перській затоці (1991), інтифада Аль-Акса (2000). Можливо, самі того не бажаючи, ізраїльські служби безпеки і збройні сили стали чимось на зразок національної спадщини і цілої індустрії. З перших днів існування держави її лідери чітко усвідомлювали, що Ізраїлю потрібна одна з кращих систем інформаційної безпеки у світі. Оточений сильними ворогами, Ізраїль повинен був компенсувати дефіцит військової могутності своїм єдиним ресурсом — людьми. Обороноздатність країни потребувала підтримки винахідливості її народу та достовірної інформації [6].

Інший підрозділ під назвою "8200" можна вважати найпотужнішою інформаційною розвідувальною службою Ізраїлю. Доти, поки колишні його солдати не стали поповнювати лави підприємців, цей підрозділ був, мабуть, самим засекреченим. Протягом десятиліть про нього не знали взагалі нічого. Ізраїльтяни настільки ретельно охороняли цю таємницю, що лише дуже обмежене коло освічених могло точно оцінити роль, яку підрозділ відігравав в інформаційних війнах. Якщо простежити за діяльністю підрозділу в минулі роки, можна зрозуміти, який величезний вплив він мав на розвиток високих технологій в Ізраїлі. Цей вплив став яскравим прикладом особливого бренду ізраїльських інновацій, сформованого в умовах постійної загрози національній безпеці. Крім того, цей бренд формувався багато в чому під впливом високого творчого потенціалу, встановлення пріоритетності науки, технології та освіти як засіб, що компенсує недолік території, ресурсів та ін.

В іноземних джерелах підрозділ "8200" часто порівнювали із Агентством національної безпеки Сполучених Штатів Америки. Завдання цього підрозділу — забезпечення інформаційної безпеки Ізраїлю, а також збирання, розшифровка і аналіз мільйонів, а то й мільярдів, біт даних, які ця служба збирає і перехоплює за допомогою своєї складної електронної мережі. Відомо, що комунікації на території Палестинської автономії і зв'язок з іншими арабськими країнами ретельно контролюються Ізраїлем. Підрозділ "8200" безпосередньо відстежує обмін електронними повідомленнями, потоки голосових та електронних даних, що проходять через комунікаційні мережі. Йоші Мельман, кореспондент щоденної газети Ha'aretz і співавтор книги Every Spy a Prince, який давно веде літопис розвідувальних служб Ізраїлю, називає цей підрозділ "найголовнішою службою у сфері збору даних". Вона вище рангом від військової розвідки [9].

У всіх поставлених цілях і виконуваних завданнях підрозділ "8200" діє, як гігантське електронне агентство зі збору інформації. Щодня і щохвилини системи підрозділу накопичують

незліченну кількість електронних сигналів, що перехоплюються базовими станціями і різними постами перехоплення інформації. Підрозділ — команда інженерів, математиків, вчених і криптографів-аналітиків. Вони вирішують всілякі завдання радіотехнічної розвідки, в основному перехоплення вихідних сигналів різного роду. Тобто співробітники підрозділу ведуть моніторинг і запис телефонних переговорів, перехоплюють факсимільні повідомлення та повідомлення електронної пошти, стежать за радіообміном і дешифрують кодування повідомлення. Інформація передається в центр розвідки, де комп'ютери і складне програмне забезпечення її сортують, перевіряють за ключовими словами і "зламують" коди зашифрованих повідомлень. Потім спеціальні аналітики і лінгвісти оцінюють зібрану інформацію.

Підрозділ "8200" виконує ті самі завдання, що входять у щоденні обов'язки Генерального штабу комунікацій у Великобританії та Управління національної безпеки в Сполучених Штатах. Однак на відміну від своїх іноземних колег, які є цивільними урядовими агентствами, підрозділ "8200" — частина військової інфраструктури Ізраїлю. Друга відмінність полягає в тому, що підрозділ є серйозним гравцем у регіоні і має значну схожість з подібними іноземними формуваннями. Його не можна порівнювати з глобальними за своїми можливостями системами і службами Сполучених Штатів, провідними проектами за типом супутникової програмами Echelon. Навколо цієї програми існує багато припущень щодо практично необмежених можливостей Управління національної безпеки з перехоплення і аналізу мільярдів електронних повідомлень між Сполученими Штатами та іншими країнами. Однак дефіцит власних ресурсів і бюджету підрозділ завжди компенсує винахідливістю. Крім того, за останні роки американці й ізраїльтяни налагодили взаємодію в питаннях інформаційної безпеки, політики і розвідки.

Отже, можна зазначити, що адміністративне регулювання інформаційної безпеки Ізраілю має жорстке правове регулювання, як частини військової системи країни. Але це регулювання має тільки загальну модель. Основною відмінністю є те, що на тлі жорсткого регулювання, суб'єктам та виконавцям у сфері інформаційної безпеки надається певна свобода вибору шляхів подолання загроз та ризиків. Значне місце надається унікальному людському фактору та можливостям діяти вільно на свій розсуд, що регулюється відомчими нормами [12].

З боку освіти, ізраїльські школи й університети приділяють велику увагу розвитку STEM-освіти, крім того, активно впроваджується практика співпраці між венчурними підприємцями і університетськими професорами. Наприклад, Аді Шамір, який займається розробкою криптосистем, також викладає прикладну математику в Інституті Вейцмана. Шамір був одним із засновників компанії NDS, що спеціалізується на розробці програмного забезпечення для телевізійної індустрії. У 2012 р. вона була продана компанії Cisco за 5 млрд дол.

В Ізраїлі військова і комерційна сфери тісно пов'язані, а інформаційна безпека вважається одним з пріоритетних напрямів інвестування. В Ізраїлі, на відміну від США, військова служба є обов'язковою, після її проходження солдати можуть реалізувати себе в комерційній сфері як висококваліфіковані фахівці. Для підприємців такі кадри становлять особливу цінність, оскільки володіють не тільки теоретичними знаннями, а й практичними навичками у цій сфері.

Багато компаній, такі як Cisco, EMC, Google, Microsoft, IBM та ін., відкрили в Ізраїлі центри кіберрозробок. Переваги очевидні — крім використання ізраїльських технологій ці фірми мають можливість співпрацювати з висококваліфікованими фахівцями.

З плином часу виникають все нові і нові загрози для інформаційної безпеки, тому, на думку Тірош, попит на високотехнологічні розробки у цій галузі буде тільки рости, а також разом із практичною сферою й законодавча.

В Ізраїлі 1 грудня 2016 р. набрав чинності закон, що забороняє будь-який електронний спам, включаючи розсилання рекламних оголошень за допомогою sms і записаних на магнітофон голосових повідомлень.

29 жовтня 2016 р. Кнесет прийняв закон "Про створення біометричного архіву". Його мета — запобігання виготовленню підроблених посвідчень особи, за допомогою зіставлень відбитків пальців і фотографій з тими, якими буде мати у своєму розпорядженні біометричний архів поліції. Всім громадянам Ізраїлю старше 16 років доведеться пройти процедуру зняття відбитків пальців в одному з відділень Міністерства внутрішніх справ [6].

Але це тільки зовнішня правова сторона забезпечення інформаційної безпеки Ізраілю. Багато механізмів регулювання коригуються відомчими актами, що надає певну гнучкість процедурі забезпечення інформаційної безпеки.

Серед останніх новацій із-за кордону варто зазначити, що 15 липня 2016 р. німецький уряд затвердив план "Біла книга" з питанньо оборонної політики та безпеки, у тому числі інформаційної. У ній чітко вказано, що Російська Федерація стала реальною загрозою, що шкодить існуючому міжнародному порядку та європейській безпеці. Насамперед це пов'язано із агресією проти України. Німеччина оголосила про зміни в інформаційній політиці відносно РФ на найближчій час. Там вказані пріоритетні інтереси, що слід захищати уряду та силовим структурам країни. Йдеться про підвищення розміру виділення коштів на оборону. Задекларована необхідність підвищення загальної інформаційної захищеності всього блоку НАТО, для чого виконується низка заходів із перепрограмування засобів інформаційної безпеки та оновлення організації її технічного оснащення. Відмічена особлива важливість створення Європейської ПРО та оновлення механізмів реалізації інформаційної безпеки. Таким чином Берлін, разом із країнами НАТО заявили про свою позицію відносно політики РФ в Україні і світі, почавши створювати принципово нову

систему інформаційної безпеки континенту [6].

Як свідчать дослідження, питання інформаційної безпеки відіграють сьогодні величезну, модернізовану роль у сфері високих технологій, тому що саме там інформація (особливо у цифровій формі) стає водночас і продуктом, і сировиною. Сучасне масове співтовариство у сфері інформаційних технологій комп'ютерної телекомунікації (ІТ) побудовано на потоках, так званих електронних даних з різних точок планети. Її виробляють, обробляють, продають і, звичайно, крадуть.

Якщо розглянути захищеність інформації, що зберігається на традиційних носіях (папір, фотовідбитки тощо), то вона досягається, як і завжди, дотриманням заходів фізичного захисту. Друга сторона захисту такої інформації пов'язана зі стихійними лихами та техногенними катастрофами. Водночас комп'ютерна інформаційна безпека загалом є більш широким поняттям, порівняно з інформаційною безпекою щодо традиційних носіїв. Це вимагає формування моделей безпеки, заснованих на методиках комплексного підходу.

Щодо новітніх викликів інформаційній безпеці в умовах розвитку Глобального Інформаційного Суспільства. Окремі дослідники звертають увагу на те, що іноді в комп'ютерних мережах телекомунікації напад триває долі секунди. Іноді промацування вразливих місць ведеться повільно, розтягується на години, що робить підозрілу активність зловмисників практично непомітною. Основна мета зловмисників — це порушення складових інформаційної безпеки: доступності, цілісності або конфіденційності [13].

На шляху долання проблем інформаційної безпеки організацій та держави, протягом доволі короткого терміну, українськими науковцями було ініційовано до розроблення низку нормативних актів. Перша черга їх стосувалася запобігання правовими засобами щодо втручання в особисті права людей, громадян, їх соціальних спільнот, підприємств, організацій, установ усіх форм власності тощо.

Проводячи правовий, порівняльний аналіз змісту окремих міжнародно-правових актів щодо прав людини та відповідних норм України, трапляються непоодинокі факти, коли допускаються протиправні втручання відповідних державних органів у сферу приватної інформації та встановлення відповідних відомчих нормативно-правових обмежень конституційно визначених норм правил поведінки у суспільстві. Зазначене закономірно викликає суспільний спротив, конфлікти інтересів громадян з органами влади. Проте сучасні українські науковці нарощують свої дослідження у цій галузі. Були окреслені основні напрями діяльності стосовно організації адекватних моделей інформаційної безпеки людини, громадянина, окремих осіб, суспільства та держави [10].

Як зазначає український вчений Б. А. Кормич, правова практика будується, насамперед, на принципі свободи інформації та гарантії інформаційних прав і свобод особи, одночасно розглядаючи права держави щодо регулювання інформаційних процесів в контексті її загальних суверенних прав [14, с. 91–92].

В аналітичній доповіді українських науковців Національного інституту стратегічних досліджень проблема інформаційної безпеки розглядалася трохи під іншим кутом зору. Ними на перший план ставилися питання адекватного розвитку інформаційного простору та інформаційних процесів, і насамперед їх економічна складова. Підкреслювалося, що "ключовою проблемою інформаційної безпеки є оцінка відповідності існуючого в державі інформаційного простору потребам її громадян, попиту та пропозиції інформаційних послуг у наближених до користувачів місцях та в зручний для них час. Історичний досвід свідчить, що країни, які не спромоглися своєчасно поповнити інформаційний простір більш ефективними технологіями, уповільнювали свій економічний розвиток. І, навпаки, країни, що мали потужний інформаційний потенціал швидко відновлювали свою роль у світовому розподілі сфер впливу навіть після воєнних поразок (наприклад, Японія після Другої світової війни). Тому наповнення інформаційного простору новітніми технологіями, що здатні істотно підвищувати як адекватність віддзеркалення реальності, так і продуктивність інформаційної діяльності в суспільстві, є нагальною потребою, що, у свою чергу, визначає можливості захисту національних інтересів" [15].

Закон України "Про основи національної безпеки України" [5] не містить окремого тлумачення поняття інформаційної безпеки, розглядаючи її лише як одну зі складових національної безпеки, що визначається певною специфікою загроз, викликів, небезпек національним інтересам. Зазначене свідчить про недостатність урахування розробниками цього законодавчого акта всіх наукових напрацювань українських дослідників.

Значною вадою багатьох наукових визначень національної та інформаційної безпеки є їх орієнтація лише на захищеність інтересів, а не на створення запобіжних умов існування суб'єктів цієї безпеки. Такий підхід звужує зміст суспільного розуміння функціональної сфери, що підмінює звичайні (традиційні) функції держави і значно обмежує демократичні права та свободи людини.

Потрібно зазначити, що в українському законодавстві в окремих спеціальних законах однобоко подаються визначення інформаційної безпеки. Для прикладу, таку ваду має нормативно-правова дефініція інформаційної безпеки, що подана в Національній програмі інформатизації. Зокрема, в п. 3 розділу IV цієї Програми зазначається: "Інформаційна безпека є невід'ємною частиною політичної, економічної, оборонної та інших складових національної безпеки. Об'єктами інформаційної безпеки є інформаційні ресурси, канали інформаційного обміну і телекомунікації, механізми забезпечення функціонування телекомунікаційних систем і мереж та інші елементи інформаційної інфраструктури країни" [8, 15].

У той же час поняття інформаційної безпеки людини та суспільства, умови існування яких визначаються насамперед їхніми природними правами і обов'язками, стає актуальним

лише в контексті розвитку і впровадження ідей природного права, зокрема прав людини, громадянина. Усе інше — то похідне, у тому числі технологічні предметні вияви інформаційних правовідносин. Тому вкрай важливо враховувати закордонний досвід розвинених країн для відбудови власної сфери інформаційної безпеки.

Висновки. Ми впевнені, що власна інформаційна безпека буде неповторною, побудованою на принципах гармонійного співвідношення та взаємодії державного впливу та недержавних організацій, організованою на чітких нормативних актах, але з певним колом можливостей для імпровізації її суб'єктів.

СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ

1. Конституція України від 28.06.1996 р. № 254к/96-ВР // Відомості Верховної Ради України. — 1996. — № 30. — С. 141.
2. Декларація про державний суверенітет України від 16.07.1990 р. № 55-XII // Відомості Верховної Ради УРСР. — 1990. — № 31. — С. 429.
3. Юлий Цезарь. Записки о Гальській войне. — М.: Азбука-классика, 1999. — 284 с.
4. *Виноградова Г. В.* Інформаційне право України: навч. посіб. — К.: МАУП, 2006. — 144 с.
5. Про інформацію: Закон України від 02.10.1992 р. № 2657-XII // Відомості Верховної Ради України. — 1992. — № 48. — Ст. 650.
6. *Скулиш Є. Д.* Історія інформаційно-психологічного протиборства: підручник / заг. ред., авт. Є. Д. Скулиш, Я. М. Жарков, Л. Ф. Компанцев та ін. — К.: Наук.-видав. Відділ НА СБУ, 2012. — 212 с.
7. *Корж І. Ф.* Державна безпека: методологічні підходи до системи складових поняття // Правова інформатика. — 2012. — № 4 (36). — С. 69–75.
8. Про Концепцію Національної програми інформатизації: Закон України від 04.02.1998 р. № 74/98-ВР // Відомості Верховної Ради України. — 1998. — № 27–28. — С. 182.
9. *Киссинджер Г.* Мировой порядок. — М.: АСТ, 2015. — 511 с.
10. *Лисенко С. О.* Організаційні засади та прийоми моделювання і реконструкції при розслідуванні правопорушенн щодо інформаційної безпеки підприємств, установ та організацій // Наук. праці МАУП. — К.: МАУП, 2015. — С. 24.
11. *Довгань О. Д.* Національний інформаційний суверенітет — об'єкт інформаційної безпеки // Інформація і право. — 2014. — № 3 (12). — С. 102–112.
12. *Біленчук П. Д., Гель А. П., Семаков Г. С.* Криміналістична тактика і методика розслідування окремих видів злочинів: навч. посіб. — К.: МАУП, 2007. — 512 с.
13. *Лисенко С. О.* Реконструкція як метод оцінки та аналізу моделей інформаційної безпеки, Fundamental and Applied Reserches in practice of Leading Scientific Schools, 2015-6 (12) // http://orcid.org/0000-0003-4037-9652
14. *Корміч Б. А.* Інформаційна безпека: організаційно-правові основи. — К.: Кондор, 2004. — 384 с.
15. Про Національну програму інформатизації: Закон України від 04.02.1998 р. № 74/98-ВР // Відомості Верховної Ради України. — 1998. — № 27–28. — С. 181.
16. Офіційний сайт Департаменту кіберполіції Національної поліції України. — Режим доступу: https://www.cybercrime.gov.ua

17. Про основи національної безпеки України: Закон України від 19.06.2003 р. № 964-IV // Відомості Верховної Ради України. — 2003. — № 39. — С. 351.
18. *Цимбалюк В. С.* Проблеми визначення категорії "інформаційна безпека підприємницької діяльності" в праві України за умов формування інформаційного суспільства // Малий і середній бізнес. — К.: НДІ Приватного права і підприємництва. — 2003. — № 1–2. — С. 43–54.

REFERENCES

1. Zakon Ukrainy "Konstytutsiia Ukrainy" : vid 28.06.1996, № 254k/96-VR [Law of Ukraine "The Constitution of Ukraine" : from 28.06.1996, № 254k/96-VR]. (1996). Vidomosti Verkhovnoi Rady Ukrainy — Bulletin of the Verkhovna Rada of Ukraine, 30 [in Ukrainian].
2. Deklaratsiia pro derzhavnyi suverenitet Ukrainy : vid 16.07.1990, № 55-XII [Declaration on State Sovereignty of Ukraine : from 16.07.1990, № 55-XII]. (1990). Vidomosti Verkhovnoi Rady URSR — Bulletin of the Verkhovna Rada of USSR, 31 [in Ukrainian].
3. Yuliy Tsezar, Zapysky pro Halsku viinu [Julius Caesar, Commentaries on the Gallic War]. (1999). Moscow: Azbukaklasyka [in Russian].
4. *Vynohradova H. V.* (2006). Informatsiine pravo Ukrainy [Information Law of Ukraine]. Kyiv: MAUP [in Ukrainian].
5. Zakon Ukrainy "Pro informatsiiu" : vid 02.10.1992, № 2657-XII [Law of Ukraine "On information"]. (1992). Vidomosti Verkhovnoi Rady Ukrainy — Bulletin of the Verkhovna Rada of Ukraine, 48 [in Ukrainian].
6. *Skulysh Ye. D.* (2012). Istoriia informatsiino-psykholohichnoho protyborstva [History of information-psychological confrontation]. Ye. D. Skulysh, Ya. M. Zharkov, L. F. Kompantsev, V. V. Ostroukhov, V. M. Petryk (Eds.). Kyiv: Nauk.-vydav. Viddil NA SBU [in Ukrainian].
7. *Korzh I. F.* (2012). Derzhavna bezpeka: metodolohichni pidkhody do systemy skladovykh poniattia [State security: methodological approaches to the system of constituent concepts]. Pravova informatyka — Law Informatics, 4 (36), 69–75 [in Ukrainian].
8. Zakon Ukrainy Pro Kontseptsiiu Natsionalnoi prohramy informatyzatsii: vid 04.02.1998, № 74/98-VR [Law of Ukraine "On the Concept of the National Program of Informatization": from 04.02.1998, № 74/98-VR]. (1998). Vidomosti Verkhovnoi Rady Ukrainy — Bulletin of the Verkhovna Rada of Ukraine, 27–28 [in Ukrainian].
9. *Kissinger H.* (2015). Mirovoy poryadok [World Order]. Moscow: AST [in Russian].
10. *Lysenko S. O.* (2015). Orhanizatsiini zasady ta pryiomy modeliuvannia i rekonstruktsii pry rozsliduanni pravoporushenn shchodo informatsiinoi bezpeky pidpryiemstv, ustanov ta orhanizatsii [Organizational Principles and Techniques for Modeling and Reconstruction in Investigation of Offenses in relation to Information Security of Enterprises, Institutions and Organizations]. Naukovi pratsi MAUP — Scientific Papers of the IAPM, 45, 24–29 [in Ukrainian].
11. *Dovhan O. D.* (2014). Natsionalnyi informatsiinyi suverenitet — obiekt informatsiinoi bezpeky [National Information Sovereignty is Information Security Object]. Informatsiia i pravo — Information and Right, 3 (12), 102–112 [in Ukrainian].
12. *Bilenchuk P. D., Hel A. P., Semakov H. S.* (2007). Kryminalistychna taktyka i metodyka rozsliduvannia okremykh

vydiv zlochyniv [Forensic tactics and methods of investigation of certain types of crimes]. Kyiv: MAUP [in Ukrainian].
13. *Lysenko S. O.* (2015). Rekonstruktsiia yak metod otsinky ta analizu modelei informatsiinoi bezpeky [Reconstruction as a Method of Assessment and Analysis of Models of Information Security]. Fundamental and Applied Reserches in practice of Leading Scientific Schools, 6(12). Retrieved from http://vabb.com.ua/news/rekonstrukczya-metod-ocznki-analzu-nformaczino-bezpeki.html [in Ukrainian].
14. *Kormich B. A.* (2004). Informatsiina bezpeka: orhanizatsiino-pravovi osnovy [Information Security: Organizational and Legal Foundations]. Kyiv: Kondor [in Ukrainian].
15. Zakon Ukrainy "Pro Natsionalnu prohramu informatyzatsii" : vid 04.02.1998, № 74/98-VR [Law of Ukraine "On the National Program of Informatization": from 04.02.1998, № 74/98-VR]. (1998). Vidomosti Verkhovnoi Rady Ukrainy — Bulletin of the Verkhovna Rada of Ukraine, 27–28 [in Ukrainian].
16. Ofitsiinyi sait Departamentu kiberpolitsii Natsionalnoi politsii Ukrainy [Official site of the Department of Cyberpolicies of the National Police of Ukraine]. www.cybercrime.gov.ua. Retrieved from https://www.cybercrime.gov.ua [in Ukrainian].
17. Zakon Ukrainy "Pro osnovy natsionalnoi bezpeky Ukrainy" : vid 19.06.2003, № 964-IV [Law of Ukraine "On the Fundamentals of National Security of Ukraine": from 19.06.2003, № 964-IV]. (2003). Vidomosti Verkhovnoi Rady Ukrainy — Bulletin of the Verkhovna Rada of Ukraine, 39 [in Ukrainian].
18. *Tsymbaliuk V. S.* (2003). Problemy vyznachennia katehorii "informatsiina bezpeka pidpryiemnytskoi diialnosti" v pravi Ukrainy za umov formuvannia informatsiinoho suspilstva [Problems of definition of the category "information security of entrepreneurial activity" in the law of Ukraine in the conditions of the formation of information society]. Malyi i serednii biznes — Small and Medium Business, 1–2, 43–54 [in Ukrainian].