



PUBLIC ADMINISTRATION

ПУБЛІЧНЕ УПРАВЛІННЯ ТА АДМІНІСТРУВАННЯ

УДК 330.46

КІБЕРБЕЗПЕКА ЯК СКЛАДОВА ЕКОНОМІЧНОЇ БЕЗПЕКИ УКРАЇНИ

Станіслав Горбаченко

*Одеський національний університет імені І. І. Мечникова,
Одеса, Україна*

Резюме. Сформульовано основні сутнісні аспекти економічної безпеки країни як фундаменту для структурних змін та сталого розвитку національної економіки, зміцнення її конкурентоспроможності, підвищення ефективності функціонування суб'єктів господарювання. Визначено процеси, що впливають на економічну безпеку на рівні держави, регіонів та окремих підприємств. З огляду на наявні класифікації складових економічної безпеки, виокремлено роль інформаційної та кібербезпеки. Визначено, що майже в усіх класифікаціях у тому чи іншому вигляді розглядається інформаційна безпека як можливість інформаційного забезпечення та захисту конфіденційної інформації соціально-економічної системи. Доведено, що категорія «кібербезпека» поступово зміщується з мікро- на макрорівень, з проблем захисту інформації на окремих пристроях у локальних мережах до питань створення єдиної системи кібербезпеки на рівні держави як повноцінної складової національної безпеки. Здійснено оцінювання кіберпростору в якості середовища для потенційних злочинних дій у сфері несанкціонованого доступу до конфіденційної інформації, збоїв у роботі програмного забезпечення, порушення режиму функціонування автоматизованих систем. Визначено характеристики економічної безпеки як стійкість у протидії внутрішнім та зовнішнім загрозам, економічна незалежність, самовідтворення та саморозвиток, національні інтереси, що можуть підтримуватися та захищатися у кіберпросторі. Висунуто пропозиції щодо створення ефективної системи державного регулювання кібербезпеки та умов для обміну інформацією в он-лайн режимі в межах трикутника «органи державної влади – приватний сектор – громадянське суспільство», оптимізації кадрового забезпечення сфери кіберзахисту, розроблення системи економічних показників функціонування кіберпростору. Наголошено на перспективності досліджень щодо стимулювання інноваційної діяльності, спрямованої на побудову ефективної організаційно-технологічної моделі національної системи кібербезпеки, реалізацію кадрового потенціалу, оптимізацію вітчизняного законодавства.

Ключові слова: економічна безпека, національна економіка, інформатизація, стратегія, кібербезпека, кіберпростір.

https://doi.org/10.33108/galicianvisnyk_tntu2020.05.180

Отримано 17.08.2020

UDC 330.46

CYBER SECURITY AS A COMPONENT OF ECONOMIC SECURITY OF UKRAINE

Stanislav Horbachenko

Odessa I. I. Mechnikov National University, Odessa, Ukraine

Summary. *The main essential aspects of the country economic security as a foundation for structural change and sustainable development of the national economy, strengthening its competitiveness, improvement of the economic entities efficiency are formulated in this paper. The processes affecting the economic security at the state, regions and individual enterprises levels are identified. Taking into account the available classifications of the economic security components, the role of information and cybersecurity is highlighted. It is determined that almost in all classifications of information security in one form or another is considered as an opportunity for information support and protection of confidential information of the socio-economic system. It is proved that «cybersecurity» category is gradually shifting from micro to macro level, from the problems of information protection on individual devices in local networks to the creation of a single cybersecurity system as a full component of national security at the state level. The assessment of cyberspace as the environment for potential criminal actions in the field of unauthorized access to the confidential information, software failures, automated systems functional breakdowns is carried out. It is identified how such characteristics of economic security as countermeasures resistance to internal and external threats, economic independence, self-reproduction and self-development, national interests, can be supported and protected in cyberspace. Proposals for creating an effective system of cybersecurity state regulation and conditions for online information exchange within «public authorities – private sector – civil society», triangle, optimization of staffing cyber protection, development of the system of economic indicators of cyberspace functioning are introduced. Emphasis is placed on the research prospects concerning the stimulation of innovative activity aimed at the creation of effective organizational and technological model of the national cybersecurity system, the implementation of human resources, optimization of domestic legislation.*

Key words: *economic security, national economy, informatization, strategy, cybersecurity, cyberspace.*

https://doi.org/10.33108/galicianvisnyk_tntu2020.05.180

Received 17.08.2020

Постановка проблеми. В сучасному світі питання економічної безпеки набувають особливої важливості, оскільки від них залежить геополітичне майбутнє країни, стан національної економіки, соціально-економічний добробут громадян, становлення їхньої національної самосвідомості. Можна стверджувати, що вирішення означених питань багато в чому залежить від ІТ-сфери, адже в постіндустріальному суспільстві інформаційні технології охопили всі сфери життєдіяльності людини, в тому числі й економічну. Чим швидше у світі відбувається розвиток інформаційних технологій, тим нагальнішою є потреба в захисті інформаційно-телекомунікаційних систем. Проте, крім корисного ефекту, інформаційні технології створюють можливості й для певних правопорушень та зловживань. Жертвами кіберзлочинів вже стають не тільки окремі фізичні особи, а й підприємства, галузі та навіть цілі держави. Отже, будь-яка країна не може вести мову про власну економічну безпеку, якщо вона не захищена у кіберпросторі.

Аналіз останніх досліджень і публікацій. Питанням забезпечення національної, зокрема економічної безпеки присвячена низка праць таких вчених, як І. Ф. Бінько, Я. А. Жаліло, З. Б. Живко, В. Г. Маргасова, О. В. Скорук, С. М. Шкарлет, В. Т. Шлемко та інших. У більшості з них належна роль відводиться інформаційним технологіям, інноваціям та іншим елементам, які, певною мірою, можна віднести до кіберпростору.

Водночас проблеми кібербезпеки, які порушують у своїх дослідженнях В. А. Ліпкан, Т. О. Сліпченко, О. А. Ткаченко розглядаються, насамперед, із погляду системи ІТ-захисту геополітичних інтересів і не пов'язуються, напрямку із економічними процесами.

Метою статті є дослідження місця кібербезпеки у забезпеченні економічної безпеки країни, а також визначення впливу кіберзагроз на основні економічні процеси в державі.

Постановка завдання. Для досягнення поставленої мети визначено такі наукові завдання: розкрити сутність економічної безпеки та її складових; визначити місце протидії кіберзагрозам серед чинників економічної безпеки; надати пропозиції щодо можливих напрямів економічних та управлінських практичних досліджень та розроблень, пов'язаних із кіберпростором.

Для вирішення поставлених завдань використано методи наукової абстракції, аналізу, синтезу, узагальнення, порівнянь, аналогії.

Виклад основного матеріалу. Серед різноманіття видів безпеки важливе місце займає саме економічна, оскільки з нею безпосередньо пов'язаний стабільний розвиток національної економіки та її окремих сегментів. Економічна безпека є фундаментом для структурних змін, зміцнення конкурентоспроможності національної економіки на світових ринках, підвищення ефективності функціонування на галузевому рівні. В дослідженнях з державного регулювання економіки та управління національним господарством економічна безпека виступає як складна багатофакторна категорія, що характеризує здатність національної економіки до розширеного відтворення з метою задоволення на визначеному рівні потреб власного населення й держави, протистояння дестабілізуючій дії чинників, що створюють загрозу стійкому збалансованому розвитку країни; забезпечення кредитоспроможності національної економіки у світовій системі господарювання [1, с. 143].

У практичному сенсі економічна безпека має передбачати спроможність національної економіки підтримувати незалежний та динамічний розвиток, забезпечити стабільність громадянського суспільства, сприяти зміцненню оборонного потенціалу держави в умовах перманентних змін зовнішнього середовища. У якості основних завдань економічної безпеки можна визначити сприяння сталому економічному зростанню, подолання кризових явищ, формування ефективної структури та забезпечення належної трансформації економіки, зменшення дефіциту бюджету та державного боргу, забезпечення соціального захисту й підвищення якості життя населення, стабілізація національної валюти та загальне підвищення конкурентоспроможності країни.

Враховуючи, що концептуальні засади економічної безпеки забезпечують формування відповідної політики на рівні не тільки держави, а й суб'єктів нижчих організаційних рівнів, у сучасних дослідженнях розглянуто кілька аспектів економічної безпеки.

У масштабі країни економічна безпека виступає не тільки необхідним фундаментом для забезпечення військової, технічної, продовольчої, екологічної безпеки, але й матеріальною основою для забезпечення національного суверенітету. Серед реальних та потенційних загроз економічній безпеці на рівні держави вагоме місце займають: критичні обсяги та несприятлива динаміка державного боргу, істотне скорочення ВВП, погіршення інвестиційної привабливості, кадрова криза, зменшення інноваційної активності та науково-технічного потенціалу, нестабільність законодавчого базису, зростання кредитних ризиків, неефективність антимонопольної політики тощо.

У свою чергу, на регіональному рівні дотримання економічної безпеки передбачає спрямування пріоритетів на отримання конкурентних переваг на внутрішньому та зовнішніх ринках, економічну незалежність регіону та можливість подолання загроз в економічній сфері. Пріоритетні напрями регіональної політики економічної безпеки

відповідають за змістом пріоритетним економічним інтересам та визначають напрями їхньої реалізації. Виходячи з цього, економічну безпеку регіону визначають як такий його фінансово-економічний стан, за якого забезпечується повноцінне використання всіх видів наявних ресурсів, досягнення бажаних економічних інтересів регіону та створюються умови для повноцінного стратегічного розвитку в майбутньому [2, с. 208]. Найбільший вплив на рівень економічної безпеки регіону здійснюють такі чинники: географічне положення, природно-ресурсний потенціал, економічна спеціалізація, транзитний потенціал, соціально-економічні зв'язки, інвестиційна привабливість, технологічний потенціал, рекреаційний потенціал, стан навколишнього середовища, демографічний фактор, рівень підтримки з боку держави.

Для окремих підприємств економічна безпека передбачає запобігання внутрішнім і зовнішнім загрозам з метою гарантування ефективного й стабільного функціонування та динамічного розвитку. Можна стверджувати, що економічна безпека характеризує поточний стан захищеності найважливіших інтересів підприємства від нечесної конкуренції, надмірного тиску з боку контролюючих органів, некомпетентних рішень, недосконалої нормативної бази, а також здатність підприємства до протистояння цим загрозам та, навіть, перетворення їх у можливості.

Щодо класифікації складових економічної безпеки існує кілька варіантів. З. Б. Живко виділяє 7 складових економічної безпеки: фінансова, кадрова, техніко-технологічна, силова, інтелектуальна, екологічна, політико-правова [3]. В свою чергу, О. В. Ареф'єва та Т. Б. Кузенко виокремлюють 9 складових економічної безпеки: фінансову, техніко-технологічну, інформаційну, силову, ресурсну, інтелектуальну, соціальну, екологічну, політико-правову [4]. Деталізованіше до структурування підійшли В. Т. Шлемко та І. Ф. Бінько, які виділили внутрішні (сировинно-ресурсна, енергетична, фінансова, воєнно-економічна, технологічна, продовольча, соціальна, демографічна, екологічна) та зовнішні (експортна та імпортна) складові економічної безпеки [5, с. 20]. З огляду на дослідження С. М. Шкарлета, серед основних функціональних складових економічної безпеки виділяють: фінансову – досягнення найефективнішого використання фінансів, інтелектуальну – збереження і розвиток інтелектуального потенціалу та техніко-економічну – забезпечення відповідності технологій сучасним світовим аналогам щодо оптимізації витрат ресурсів [6].

Слід зауважити, що майже в усіх класифікаціях У тому чи іншому вигляді розглядається інформаційна безпека, тобто можливість інформаційного забезпечення та захисту конфіденційної інформації соціально-економічної системи. Незважаючи на те, що у кожній країні є певна група галузей та секторів національної економіки, які створюють фундамент для економічної безпеки, прагнення реалізувати свій потенціал і в ІТ-сфері постає одним із головних глобальних трендів. Отже, з урахуванням тотальної діджиталізації економічних процесів з одночасним переміщенням масивів інформації у кіберсистеми все більшого значення набувають питання кібербезпеки.

Згідно зі стандартом ISO/IEC 27032:2012 кібербезпека виступає як збереження цілісності, конфіденційності та доступності інформації, що циркулює в кіберсистемі (тобто інформації, що надходить у кіберсистему, накопичується та зберігається для подальшого опрацювання), з метою забезпечення стійкості й безперервності реалізації кіберсистемою управлінських функцій щодо відповідних об'єктів управління [7, с. 45].

В останні роки можна спостерігати трансформацію категорії «кібербезпека» з поступовим її пересуванням із мікро- на макрорівень. Тобто питання вже не тільки в захисті інформації на окремому пристрої чи в межах локальної мережі. Мова йде про необхідність створення єдиної системи кібербезпеки на рівні держави як повноцінної складової національної та, в тому числі, й економічної безпеки. Одночасно відбувається й поступова зміна напрямку загроз: з локального та галузевого на загальнонаціональний та наднаціональний. Основними об'єктами кібератак виступають діяльність уряду,

правоохоронних органів, збройних сил, засобів масової інформації, системи життєзабезпечення міст, транспортні та комунікаційні мережі, ядерна та хімічна промисловість, національна енергетична та фінансова системи тощо. Власне сам кіберпростір вже априорі розглядається як середовище для потенційних злочинних дій у сфері несанкціонованого доступу до конфіденційної інформації, збоїв у роботі програмного забезпечення, порушення режиму функціонування автоматизованих систем.

Серед характеристик, що становлять сутнісну основу сучасних тенденцій трансформації кіберпростору, основну цінність для процесів у національній економіці становлять:

- зміна характеру діяльності осіб, які ухвалюють рішення щодо заходів з кібербезпеки системних об'єктів;
- цифровізація економічної, наукової, освітньої та соціально-культурної діяльності держави і соціуму, яка передбачає утворення й інформаційно-технологічну підтримку електронно-цифрових форм створення, опрацювання, зберігання, захисту та переміщення інформації;
- перехід від паперового документообігу до електронно-цифрового;
- підтримка безпечної, стійкої й надійної роботи електронного операційного/інформаційного середовища, яке підтримує національну безпеку країни, мінімізує наслідки злочинних кібервтручань та максимізує переваги цифрової економіки [8, с. 80].

З іншого боку, майже всі наукові підходи до визначення сутності економічної безпеки держави беруть до уваги її певні характеристики, підтримка яких залежить й від захисту у кіберпросторі.

Таблиця 1. Основні характеристики економічної безпеки

Table 1. Basic characteristics of economic security

Характеристика	Зміст	Інструменти захисту в кіберпросторі
Стійкість у протидії внутрішнім та зовнішнім загрозам	Міцність і надійність зв'язків між усіма елементами економічної системи, стабільність економічного розвитку держави, здатність до стримування та знешкодження дестабілізуючих чинників	Розроблення системних моделей кіберпростору й ідентифікація факторів, що впливають на його функціонування
Економічна незалежність	Можливість для будь-якого суб'єкта економічної безпеки самостійно приймати й реалізовувати стратегічні економічні та політичні рішення для розвитку	Захист від кібервтручання у господарську діяльність вітчизняних бізнес-одиниць
Самовідтворення та саморозвиток	Створення необхідних умов для ефективної економічної політики, розширеного самовідтворення, а також забезпечення конкурентоспроможності національної економіки на світовій арені	Упровадження спеціальних методів і технологій забезпечення стійкості кіберзахисту при впливі загроз
Національні інтереси	Спроможність національної економіки забезпечити захист національних економічних інтересів	Створення ефективної системи регулювання кібербезпеки на державному рівні

Джерело: розроблено автором на базі [9, с. 40].

Враховуючи наявну взаємозалежність між проблемами забезпечення економічної безпеки та кібербезпеки, доцільно інтегрувати у комплекс економічних та управлінських досліджень кілька напрямків, пов'язаних із кіберпростором.

1. Створення ефективної системи державного регулювання кібербезпеки. З управлінського погляду означена система має ґрунтуватися на розробленні відповідного плану заходів та подальшого контролю за їхнім виконанням. Затверджена «Стратегія кібербезпеки України» [10] передбачає, що вжиття заходів, спрямованих на її забезпечення, має проводитися на планових засадах. Кабінет Міністрів України разом із

Службою безпеки України, Службою зовнішньої розвідки України та за участю Національного інституту стратегічних досліджень мають готувати щорічні плани заходів щодо реалізації конструктивних положень «Стратегії кібербезпеки України» та щопівроку здійснювати відповідне інформування РНБО України, а саме, Національний координаційний центр кібербезпеки про стан його реалізації. Проте доцільно адаптувати означені заходи й до потреб національної економіки.

2. Створення умов для обміну інформацією в он-лайн режимі в межах трикутника «органи державної влади – приватний (насамперед, корпоративний) сектор – громадянське суспільство» задля запобігання реальним та потенційним загрозам критичній інформаційній інфраструктурі, а також оперативного інформування державних органів для прийняття ефективних управлінських рішень у межах їх компетенції.

3. Кадровий аспект, який має міжнародний характер у контексті проблем із забезпеченням сфери кіберзахисту кваліфікованими фахівцями. Наприклад, в останні роки країни ЄС стикнулися з проблемою нестачі кваліфікованих фахівців у сфері інформаційно-комунікаційних технологій і особливо експертів в області кібербезпеки. У пропозиції бюджету ЄС на 2021–2027 роки наголошується на розвиткові цифрових навичок, особливо в області кібербезпеки [11, с. 130]. З одного боку, можна стверджувати про наявність перспективного зовнішнього ринку праці для кваліфікованих вітчизняних фахівців, з іншого міграційні процеси можуть спричинити додаткові ризики кібербезпеці нашої держави.

4. Розроблення системи економічних показників функціонування кіберпростору, а також ефективності його захисту від потенційних загроз. На сьогодні ефективність заходів кібербезпеки та потенційні втрати від кіберзагроз дуже складно оцінити. Внаслідок цього керівники деяких підприємств не бажають інвестувати кошти у заходи кібербезпеки, адже не бачать прямого економічного ефекту. Це ж стосується й оцінювання ефективності інноваційних проектів, пов'язаних із кібербезпекою.

5. Максимальне впровадження інновацій у криптографічному захисті з одночасним застосуванням інтелектуальних методів забезпечення кібербезпеки (метод ситуаційного аналізу, інтелектуальні методи виявлення вторгнень у системи, інтелектуальна ідентифікація користувачів при кібератаці) та психолого-поведінкових підходів (робота з персоналом, пропаганда кіберобережності).

Висновки. Враховуючи сучасні глобальні тенденції, забезпечення економічної безпеки України є неможливим без відповідної кіберскладової. Питання кіберзахисту із локальної загрози функціонуванню бізнес-єдиниць перетворилися на завдання національного рівня. Наразі створення дієвої національної системи кібербезпеки є неможливим без впровадження цілого комплексу заходів. Зокрема, на рівні національної економіки доцільним є стимулювання інноваційної діяльності, спрямованої на побудову ефективної організаційно-технологічної моделі національної системи кібербезпеки. Серед конкретних інструментів можна впровадити пільгове кредитування на заходи щодо кібербезпеки або відповідні податкові пільги. Важливою також є й підтримка на державному рівні кадрового потенціалу в означеній сфері. Існує потреба і в оптимізації вітчизняного законодавства у контексті імплементації міжнародно-правових норм із питань кібербезпеки.

Conclusions. Taking into account the current global trends, it is impossible to ensure Ukraine's economic security without appropriate cyber component. The problems of cyber defense from the local threat to business entities functioning have become the national task. At present, the creation of effective national cybersecurity system is impossible without the implementation of a set of measures. Particularly, at the national economy level it is advisable to stimulate innovative activities aimed at the creation of effective organizational and technological model of the national cybersecurity system. Such specific instruments include

concessional lending for cybersecurity measures or related tax incentives. It is also important to support human resources at the state level in this area. At the same time, it is required to optimize domestic legislation, particularly, in the context of the implementation of international law concerning cybersecurity.

Список використаної літератури

1. Жаліло Я. А. Стратегія національної безпеки України в контексті досвіду світової спільноти. Київ: Сатсанга, 2001. 224 с.
2. Маргасова В. Г. Економічна безпека регіону. Глобальне управління та економіка: науковий журнал. 2015. № 1 (1). С. 206–210.
3. Живко З. Б. Економічна безпека підприємства: сутність, механізм забезпечення та управління: монографія. Львів: Львівський державний університет внутрішніх справ, 2012. 260 с.
4. Ареф'єва О. В., Кузенко Т. Б. Планування економічної безпеки підприємства: монографія. Київ: Європ. ун-т. 2004. 170 с.
5. Шлемко В. Т., Бінько І. Ф. Економічна безпека України: сутність і напрямки забезпечення: монографія. К.: НІСД, 1997. 144 с.
6. Шкарлет С. М. Економічна безпека підприємства: інноваційний аспект. К.: Книжкове видавництво НАУ, 2007. 436 с.
7. Ліпкан В. А., Ліпкан О. С. Національна і міжнародна безпека у визначеннях та поняттях: навч. посіб. Вид. 2-ге, перероб. і допов. Київ. 2018. 400 с.
8. Ткаченко О., Ткаченко К. Кіберпростір і кібербезпека: проблеми, перспективи, технології. Цифрова платформа: інформаційні технології в соціокультурній сфері. 2018. № 1. С. 75–86. <https://doi.org/10.31866/2617-796x.1.2018.147257>
9. Скорук О. В. Економічна безпека держави: сутність, складові елементи та проблеми забезпечення Науковий вісник Ужгородського національного університету. 2016. Вип. 6. Частина 3. С. 39–42.
10. Стратегія кібербезпеки України: затв. Указом Президента України від 15 берез. 2016 р. URL: <https://www.president.gov.ua/documents/962016-19836>.
11. Сліпченко Т. О. Кібербезпека як складова системи захисту національної безпеки: європейський досвід. Актуальні проблеми правознавства. 2020. № 1 (21). С. 128–133. <https://doi.org/10.35774/app2020.01.128>

References

1. Zhalilo Ja. A. (2001) Strateghija nacionaljnoji bezpeky Ukrajinu v konteksti dosvidu svitovoji spiljnoty [Ukraine's national security strategy in the context of the experience of the world community]. Kyiv: Satsanga [in Ukrainian].
2. Marghasova V. Gh. (2015) Ekonomichna bezpeka reghionu. [Economic security of the region]. *Ghlobaljne upravlinnja ta ekonomika: naukovyj zhurnal*. No. 1., pp. 206–210. [In Ukrainian].
3. Zhyvko Z. B. (2012) Ekonomichna bezpeka pidpryjemstva: sutnistj, mekhanizm zabezpechennja ta upravlinnja. [Economic security of the enterprise: essence, mechanism of providing and management]. Lviv: Lviv State University of Internal Affairs. [In Ukrainian].
4. Aref'jeva O. V., Kuzenko T. B. (2004) Planuvannja ekonomichnoji bezpeky pidpryjemstva. [Economic security planning of the enterprise]. Kyiv: European University. [In Ukrainian].
5. Shlemko V. T., Binjko I. F. (1997) Ekonomichna bezpeka Ukrajinu: sutnistj i naprtjamky zabezpechennja. [Economic security of Ukraine: essence and directions of providing]. Kyiv: NISS. [In Ukrainian].
6. Shkarlet S. M. (2007) Ekonomichna bezpeka pidpryjemstva: innovacijnyj aspect. [Economic security of the enterprise: innovative aspect]. Kyiv: NAU Book Publishing House. [In Ukrainian].
7. Lipkan V. A., Lipkan O. S. (2018) Nacionaljna i mizhnarodna bezpeka u vyznachennjakh ta ponjattjakh. [National and international security in definitions and concepts]. Kyiv. [In Ukrainian].
8. Tkachenko O., Tkachenko K. (2018) Kiberprostir i kiberbezpeka: problemy, perspektyvy, tekhnologhiji. [Cyberspace and cybersecurity: problems, prospects, technologies]. *Cyfrova platforma: informacijni tekhnologhiji v sociokuljturnij sferi*. No. 1., pp. 75–86. [In Ukrainian]. <https://doi.org/10.31866/2617-796x.1.2018.147257>
9. Skoruk O. V. (2016) Ekonomichna bezpeka derzhavy: sutnistj, skladovi elementy ta problemy zabezpechennja. [Economic security of the state: essence, constituent elements and problems of providing]. *Naukovyj visnyk Uzghorodskjogho nacionaljnogho univrsytetu*. No. 6., P. 3., pp. 39–42. [In Ukrainian].
10. Strateghija kiberbezpeky Ukrajinu: zatv. Ukazom Prezydenta Ukrajinu vid 15 berez. 2016 r. Available at: <https://www.president.gov.ua/documents/962016-19836>.
11. Slipchenko T. O. (2020) Kiberbezpeka jak skladova systemy zakhystu nacionaljnoji bezpeky: jevropejskij dosvid. [Cybersecurity as a component of the national security protection system: European experience]. *Aktualjni problemy pravoznavstva*. No. 1., pp. 128–133. [In Ukrainian]. <https://doi.org/10.35774/app2020.01.128>