УДК 342.9

ТКАЧУК Н.А., *кандидат юридичних наук,*
старший науковий співробітник НДІІП НАПрН України

ПРАВОВЕ РЕГУЛЮВАННЯ ВЗАЄМОДІЇ СЛУЖБИ БЕЗПЕКИ УКРАЇНИ З ПРИВАТНИМ СЕКТОРОМ У СФЕРІ ЗАБЕЗПЕЧЕННЯ КІБЕРБЕЗПЕКИ

Анотація. *У статті автор досліджує основні проблемні питання правового регулювання взаємодії СБ України з приватним сектором у сфері забезпечення кібербезпеки та пропонує шляхи їх вирішення.*

Ключові слова: *кібербезпека, державно-приватне партнерство, державно-приватна взаємодія, правове регулювання, Служба безпеки України.*

Summary. *In this article the author investigates the main problematic issues of legal regulation of the cooperation between the Security Service of Ukraine and private sector in the field of cyber security and suggests ways of their solution.*

Keywords: *cyber security, public-private partnership, public-private interaction, legal regulation, Security Service of Ukraine.*

Аннотация. *В статье автор исследует основные проблемные вопросы правового регулирования взаимодействия СБ Украины с частным сектором в сфере обеспечения кибербезопасности и предлагает пути их решения.*

Ключевые слова: *кибербезопасность, государственно-частное партнерство, государственно-частное взаимодействие, правовое регулирование, Служба безопасности Украины.*

Постановка проблеми. Актуалізація кіберзагроз національній безпеці та перетворення кібервпливу на інструмент терористичної, а також розвідувально-підривної діяльності спецслужб іноземних країн проти нашої держави обумовлює потребу посилення кібербезпекових спроможностей Служби безпеки України, як одного із ключових суб'єктів національної системи кібербезпеки, який вирішує завдання із протидії вказаним загрозам.

Важливою умовою підвищення потенціалу вітчизняної спецслужби є забезпечення ефективної взаємодії з приватним сектором. Ключова роль державно-приватного партнерства обумовлена специфікою кібербезпекової сфери. Наразі, кібербезпека є єдиною сферою національної безпеки, яка настільки тісно пов'язана із приватним сектором – по-перше, значний обсяг об'єктів кібербезпеки та кіберзахисту перебуває у приватній власності, по-друге, механізм поширення кіберзагроз в мережі Інтернет фактично нівелює різницю між державними та приватними суб'єктами, по-третє, найбільш досвідчені експерти з ІТ-безпеки працюють саме у недержавному секторі.

Безумовно, розбудова дієвих механізмів державно-приватного партнерства у контексті діяльності СБУ вимагає створення належної правової бази, яка б сприяла залученню громадянського суспільства до забезпечення кібербезпеки держави.

Результати аналізу наукових публікацій. Сутність, організаційно-правові засади та проблемні питання державно-приватного партнерства у сфері кібербезпеки розглядалися у наукових працях В. Бойко, Н. Буша, О. Гівена, С. Гнатюка, Д. Дубова, М. Карр, В. Круглова, М. Ожевана та інших вітчизняних і закордонних вчених. Водночас, на сьогодні відсутні наукові роботи, присвячені дослідженню проблематики нормативного регулювання такого партнерства у контексті діяльності Служби безпеки України, що обумовлює актуальність теми статті.

Метою статті є дослідження сучасного стану правового регулювання партнерства СБ України з приватним сектором у сфері забезпечення кібербезпеки, визначення основних проблемних питань та розробка рекомендацій із удосконалення чинного законодавства у вказаній сфері.

Виклад основного матеріалу. Відповідно до Закону України "Про основні засади забезпечення кібербезпеки України" на Службу безпеки України покладено ряд важливих завдань у сфері кібербезпеки, серед яких: боротьба з кібертероризмом та кібершпигунством, протидія кіберзлочинності, наслідки якої можуть створити загрозу життєво важливим інтересам держави, розслідування кіберінцидентів та кібератак щодо критичної інформаційної інфраструктури, реагування на кіберінциденти у сфері державної безпеки та інші [1].

Посилення спроможностей Служби безпеки для ефективної протидії цим загрозам визначається Концепцією розвитку сектору безпеки і оборони України як один із пріоритетних напрямів реформування відомства [2]. Безумовно, підвищення ефективності діяльності СБ України у сфері кібербезпеки неможливе без належної взаємодії з приватним сектором. Відповідно до чинного законодавства принцип державно-приватної взаємодії є одним із основоположних принципів забезпечення кібербезпеки України, який в першу чергу повинен реалізовуватись "шляхом обміну інформацією про інциденти кібербезпеки" [1].

З метою розвитку державно-приватного партнерства для запобігання кіберзагрозам, реагування на кібератаки та кіберінциденти у сфері державної безпеки та усунення їх наслідків Службою безпеки України вживаються системні заходи щодо залучення громадянського суспільства до протидії кіберзагрозам національній безпеці.

Так, фахівцями Ситуаційного центру забезпечення кібербезпеки СБУ на базі платформи з відкритим програмним кодом MISP (Malware Information Sharing Platform) створено систему збору і обробки інформації щодо інцидентів кібербезпеки та обміну технічними даними про ідентифікатори компрометації інформаційних систем об'єктів критичної інфраструктури між суб'єктами сектору безпеки в режимі реального часу MISP-UA (Ukrainian Advantage). Ця платформа широко використовується в усьому світі, а також відповідає міжнародним стандартам ЄС та НАТО і застосовується основними міжнародними суб'єктами у сфері кібербезпеки: FIRST, CIRCL, CiviCERT, NATO NCI Agency [3].

Правовою основою інформаційного обміну з використанням інструментів MISP-UA є Меморандум про взаємодію, в рамках якого Службою безпеки України налагоджено обмін інформацією про кіберінциденти та ідентифікатори компрометації з низкою об'єктів критичної інфраструктури приватного сектору (у т.ч. у сфері енергетики, транспорту, телекомунікацій, банківській сфері, оборонній промисловості тощо), а також провідними корпораціями у сфері кібербезпеки [4; 5].

Своєчасний обмін такою інформацією дозволяє завчасно попередити та локалізувати кібератаки, підвищує ефективність реагування з боку СБУ на атаки високого ступеня складності. Слід зазначити, що упереджувальна інформація про можливі кібератаки надається приватному сектору саме з боку Служби безпеки України, що сприяє підвищенню захищеності критичної інфраструктури.

Вказані організаційно-правові заходи свідчать про розуміння керівництвом Служби безпеки важливості налагодження партнерства з приватним сектором та готовність надавати допомогу бізнесу щодо протидії кіберзагрозам. Як заявив голова СБУ Василь Грицак, підкреслюючи надпріоритетність такої взаємодії – "Будь-який

представник великого, середнього та навіть малого бізнесу може звернутися до Ситуаційного центру забезпечення кібербезпеки за консультаціями та допомогою" [6].

Іншим перспективним напрямом державно-приватної взаємодії є залучення ІТ-фахівців приватного сектору (т.зв. "активістів") до проведення негласних перевірок готовності об'єктів критичної інфраструктури до можливих кібератак та кіберінцидентів, що є одним із функціональних завдань СБ України.

Виявлення вразливостей в інформаційно-телекомунікаційних системах об'єктів критичної інформаційної інфраструктури ("пентестінг") є важливою задачею і цілком підпадає під сутнісні ознаки державно-приватної взаємодії. Проте, така діяльність потребує створення відповідного правового поля. На сьогодні, проведення негласного пентестінгу формально містить ознаки складу злочину, передбаченого статтею 361 Кримінального кодексу України "Несанкціоноване втручання в роботу електронно-обчислювальних машин (комп'ютерів), автоматизованих систем, комп'ютерних мереж чи мереж електрозв'язку". Формулювання зазначеної статті КК Украни фактично унеможливлює діяльність некомерційних пентестерів, якщо ці тести заздалегідь не погоджені із об'єктами атаки [7, с. 66].

Першим кроком на шляху модернізації вітчизняного законодавства має бути створення відповідного правового поля для здійснення "хактивістами" пентестової діяльності в інтересах негласної перевірки готовності об'єктів критичної інфраструктури до можливих кібератак та кіберінцидентів у спосіб, який би не наносив шкоду державній безпеці. Вважаємо, що вказана діяльність має бути попередньо узгоджена із Службою безпеки України, до компетенції якої належить проведення негласних перевірок, що власне і буде підставою для легалізації таких дій.

У вітчизняних наукових колах існує думка, що механізм легалізації пентестінгу повинен полягати у застосуванні правового інституту звільнення від кримінальної відповідальності (наприклад, Д. Дубов пропонує доповнити статтю 361 КК України наступним пунктом: "звільняється від кримінальної відповідальності громадянин України, якщо таке втручання здійснювалось за погодженням із суб'єктами національної системи кібербезпеки…"[7, с. 79]).

Водночас, відповідно до роз'яснення Верховного Суду України [8], звільнення від кримінальної відповідальності – це відмова держави від застосування щодо особи, котра вчинила злочин, установлених законом обмежень певних прав і свобод шляхом закриття кримінальної справи. Причому звільнення від кримінальної відповідальності, відповідно до ч. 2 статті 44 КК України, здійснюється виключно судом. Так, відповідно до Розділу ІХ "Звільнення від кримінальної відповідальності" його підставами можуть бути: дійове каяття (ст. 45), закінчення строків давності (ст. 49), передача особи на поруки (ст. 47) та ін. [9].

Вважаємо, що залучення Службою безпеки осіб в рамках державно-приватної взаємодії до негласної перевірки стану кіберзахисту об'єктів критичної інфраструктури в інтересах національної безпеки повинне бути обставиною, яка не лише звільняє від кримінальної відповідальності, а взагалі виключає злочинність діяння.

Тому пропонуємо доповнити статтю 361 КК України наступним пунктом: "Не є злочином дії особи, передбачені частиною першою цієї статті, яка відповідно до закону виконувала спеціальне завдання органів державної безпеки із негласної перевірки готовності об'єктів критичної інфраструктури до можливих кібератак та кіберінцидентів". Це дозволить створити правове поле для розвитку державно-приватної взаємодії за вказаним напрямом.

Важливим напрямом державно-приватного партнерства у сфері протидії кіберзагрозам є взаємодія з Інтернет-провайдерами. Незважаючи на те, що ролі правоохоронних органів та операторів і провайдерів телекомунікацій є різними – правоохоронні органи протидіють злочинності, в той час як постачальники послуг забезпечують користувачам можливість спілкування – необхідно виробити такий механізм взаємодії, який би робив кіберпростір безпечнішим і в той же час забезпечував повагу до різних ролей суб'єктів взаємодії, а також прав та свобод користувачів [10].

На сьогодні проблемним питанням залишається відсутність ефективного правового механізму щодо отримання в інтересах забезпечення національної безпеки від операторів та провайдерів телекомунікацій комп'ютерних даних, необхідних для своєчасного реагування на кіберзагрози, у т.ч. попередження і локалізації кіберінцидентів та кібератак на критичну інформаційну інфраструктуру.

До таких даних належить інформація технологічного характеру щодо дій абонентів (дані про з'єднання, лог-файли, IP-адреси тощо), а також відомості, які можуть ідентифікувати їх особу, за винятком контенту (змістовного наповнення інформаційних потоків).

Своєчасне отримання комп'ютерних даних від провайдера у багатьох випадках дозволяє встановити особу злочинця, виявити механізм поширення шкідливого програмного забезпечення (далі – ШПЗ), а також виявити інші інфіковані зазначеним ШПЗ комп'ютерні мережі, що дозволяє вчасно локалізувати поширення вірусу та попередити масовані кібератаки на критичну інфраструктуру держави, а також кібершпигунство щодо інформації, яка циркулює в державних електронних інформаційних ресурсах.

Відповідно до статей 16 – 18 Конвенції Ради Європи про кіберзлочинність [11], яка є основним міжнародним нормативно-правовим актом у сфері кібербезпеки та була ратифікована Україною в 2005 році, кожна Сторона повинна вжити законодавчих та інших заходів, необхідних для забезпечення термінового збереження та розкриття постачальником послуг на вимогу компетентного правоохоронного органу даних про рух інформації, а також комп'ютерних даних, що не є власне даними змісту інформації, за допомогою яких можна встановити:

- тип комунікаційної послуги, яка використовувалася, її технічні положення і період користування послугою;
- особистість користувача послуг, поштову або географічну адресу, телефони та інший номер доступу, інформацію про рахунки і платежі, яку можна отримати за допомогою угоди про постачання послуг;
- будь-яку іншу інформацію про місце встановлення комунікаційного обладнання, яку можна отримати за допомогою угоди про постачання послуг.

Норми національного законодавства (частини 2, 5 ст. Закону України "Про контррозвідувальну діяльність" [12], частина 3 ст. 25 Закону України "Про Службу безпеки України" [13], ст. 11 Закону України "Про основні засади забезпечення кібербезпеки України" [1], частина 6 ст. 6 та частина 1 ст. 25 Закону України "Про захист персональних даних" [14]) також забезпечують СБ України законні підстави звертатися до операторів та провайдерів телекомунікацій з запитами щодо надання відповідних комп'ютерних даних в інтересах забезпечення національної та кібербезпеки держави.

Водночас, як свідчить практика діяльності підрозділів СБ України, деякі оператори та провайдери телекомунікацій ігнорують законні вимоги органів СБ України та не надають таку інформацію на запити Служби [15; 16], незважаючи на норми законодавства.

В результаті Служба безпеки України не може своєчасно отримати інформацію, необхідну для протидії кіберзагрозам національній безпеці, та фактично не має жодного інструменту впливу на вказаних суб'єктів господарювання через відсутність в законодавстві будь-якої відповідальності, передбаченої за невиконання законних вимог представників СБ України.

Абсурдність ситуації підкреслює той факт, що Кодекс України про адміністративні правопорушення (Глава 15) [17] встановлює адміністративну відповідальність за невиконання законних вимог посадових осіб переважної більшості державних органів: НАБУ, Нацполіції, органів прокуратури, Держспецзв'язку, НКРЗІ, Держфінмоніторингу, Рахункової палати, Держпродспоживслужби, Держпраці, Держатомрегулювання, Укрдержархіву, народних депутатів України, інспекторів сільського господарства, державних фітосанітарних інспекторів та багатьох інших. Відсутність у цьому переліку посадових осіб Служби безпеки України не тільки значно зменшує спроможності СБУ із протидії загрозам державній безпеці, але й певною мірою підриває авторитет національної спецслужби.

Таким чином, існує потреба доповнення Кодексу України про адміністративні правопорушення відповідною нормою, яка б передбачала встановлення адміністративної відповідальності за невиконання законних вимог посадових осіб Служби безпеки України.

Не можна не погодитись з М. Карр, яка, аналізуючи міжнародний досвід щодо налагодження державно-приватного партнерства у сфері кібербезпеки, доходить до висновку, що успішне державно-приватне партнерство може ґрунтуватися або на спільних інтересах або ж, якщо інтереси партнерів не збігаються, на чітких законодавчо закріплених вимогах [18].

Окремо слід відзначити проблемне питання організації збереження операторами та провайдерами надання телекомунікацій послуг даних, щодо записів про надані телекомунікаційні послуги протягом строку позовної давності, визначеного законом.

Відповідно до ст. 39 Закону України "Про телекомунікації" [19] оператори і провайдери телекомунікацій зобов'язані зберігати інформацію щодо наданих телекомунікаційних послуг, однак відсутність у законодавстві чіткого визначеного переліку відомостей, що підлягає збереженню, не дозволяє створити дієвий механізм контролю за виконанням цієї норми Закону, а також одержувати співробітниками правоохоронних органів, у повній мірі, даних (потенційних електронних доказів), необхідних для запобігання, виявлення та припинення кіберзагроз, розслідування кіберінцидентів та кібератак.

Крім того, негативно впливає на стан взаємоді неврегульованість використання провайдерами телекомунікаційних послуг механізму перетворення мережевих адрес за технологією NAT (Network Address Translation).

Застосування зазначеної технології дозволяє провайдерам заощадити ресурс IP-адрес шляхом трансляції декількох внутрішніх IP-адрес в одну зовнішню публічну IP-адресу. Водночас, використання цієї технології без обов'язкового логування (фіксації службової та статистичної інформації про події в комп'ютерній системі) унеможливлює або ускладнює процес ідентифікації злочинців в мережі Інтернет. Ця проблема є актуальною не лише для України. У минулому році Європол офіційно звернувся до провайдерів та операторів телекомунікацій із вимогою припинити використання зазначеної технології [20].

Таким чином, виникає нагальна потреба у розробці нормативно-правового акту, що дозволить конкретизувати види необхідної для розслідування кіберінцидентів і

кіберзлочинів технологічної інформації, що супроводжує сеанси телекомунікаційного зв'язку, визначить терміни та обсяги її зберігання постачальниками телекомунікаційних послуг, а також врегулює порядок надання цієї інформації правоохоронним органам на різних стадіях запобігання злочинів та кримінального переслідування злочинців, та в свою чергу, вирішить питання деанонімізації корисувачів мережі Інтернет, яким надано доступ за технологією NAT.

Залишаються неузгодженими у розрізі регулювання державно-приватного партнерства у сфері кібербезпеки положення законів України "Про державно-приватне партнерство" [21] та "Про основні засади забезпечення кібербезпеки України" [1], що негативно впливає на формування правової основи такого партнерства не лише у контексті діяльності Служби безпеки України, а і всіх суб'єктів національної кібербезпекової системи. Зокрема, на законодавчому рівні слід врегулювати наступні проблемні питання:

- чітко визначити взаємовідношення державно-приватного партнерства та державно-приватної взаємодії у сфері кібербезпеки. Зокрема, чи є така взаємодія різновидом державно-приватного партнерства, та відповідно, чи підпадає під дію Закону України "Про державно-приватне партнерство";

- передбачити внесення до переліку сфер застосування державно-приватного партнерства, визначених у статті 4 Закону України "Про державно-приватне партнерство", сферу кібербезпеки та кіберзахисту;

- враховуючи, що відповідно до положень чинного законодавства [21], [22] головним органом виконавчої влади, що забезпечує формування і реалізацію державної політики щодо державно-приватного партнерства є Мінекономрозвитку, необхідно визначити роль вказаного державного органу у формуванні та реалізації державної політики щодо державно-приватного партнерства у сфері кібербезпеки. З урахуванням того, що Мінекономрозвитку не є основним суб'єктом національної системи кібербезпеки [1], можливо передбачити покладення вказаних обов'язків на одного із ключових суб'єктів такої системи.

Висновки.

Дослідження правових основ партнерства СБ України з приватним сектором у сфері забезпечення кібербезпеки дає змогу дійти таких основних висновків і пропозицій:

1. Забезпечення дієвої взаємодії з приватним сектором є важливою умовою ефективного виконання Службою безпеки України завдань у сфері кібербезпеки, що обумовлено як специфікою кібербезпекової сфери, так і загальносвітовою тенденцією щодо зростання ролі державно-приватного партнерства у діяльності правоохоронних органів.

2. На сьогодні ключовим напрямом такого партнерства є обмін у режимі реального часу інформацією технічного характеру про кіберзагрози з об'єктами критичної інфраструктури приватного сектору та надання допомоги Ситуаційним центром забезпечення кібербезпеки СБУ у локалізації кіберінцидентів та кібератак на такі об'єкти.

3. З метою подальшої розбудови організаційно-правових засад партнерства СБ України з приватним сектором та удосконалення правової основи такої взаємодії пропонується:

- врегулювати на законодавчому рівні залучення ІТ-фахівців приватного сектору (т.зв. "хактивістів") до проведення негласних перевірок готовності об'єктів критичної інфраструктури до можливих кібератак та кіберінцидентів шляхом внесення відповідних змін до статті 361 КК України;

- забезпечити імплементацію у національне законодавство положень Конвенції Ради Європи про кіберзлочинність у частині забезпечення термінового збереження та розкриття постачальником телекомунікаційних послуг на вимогу компетентного правоохоронного органу даних про рух інформації та інших комп'ютерних даних;

- розробити нормативно-правовий акт, що дозволить конкретизувати види необхідної для розслідування кіберінцидентів і кіберзлочинів технологічної інформації, що супроводжує сеанси телекомунікаційного зв'язку, визначить терміни та обсяги її зберігання постачальниками телекомунікаційних послуг, а також врегулює порядок надання цієї інформації правоохоронним органам на різних стадіях запобігання злочинів та кримінального переслідування злочинців;

- доповнити Кодекс України про адміністративні правопорушення нормою, яка б передбачала встановлення адміністративної відповідальності за невиконання законних вимог посадових осіб Служби безпеки України;

- врегулювати питання деанонімізації корисувачів мережі Інтернет, доступ яким надано за технологією NAT;

- узгодити у розрізі регулювання державно-приватного партнерства у сфері кібербезпеки положення законів України "Про державно-приватне партнерство" та "Про основні засади забезпечення кібербезпеки України".

Використана література

1. Про основні засади забезпечення кібербезпеки України: Закон України від 05.10.17 р. URL: http://zakon.rada.gov.ua/laws/show/2163-19

2. Про рішення Ради національної безпеки і оборони України від 4 березня 2016 року "Про Концепцію розвитку сектору безпеки і оборони України": Указ Президента України від 14.03.16 р. № 92. URL: https://www.president.gov.ua/documents/922016-19832

3. СБУ розширює співпрацю з громадськістю у рамках розвитку державно-приватного партнерства. URL: https://upmp.news/ua-in-ukraine/sbu-rozshiryuye-spivpratsyu-z-gromadkistyu-u-ramkah-rozvitku-derzhavno-privatnogo-partnerstva

4. СБУ і "Антонов" підписали меморандум щодо обміну даними про кібератаки в режимі реального часу. URL: https://ua.interfax.com.ua/news/general/517243.html

5. СБУ посилює захист інформаційної безпеки підприємств енергетичної галузі України. URL: https://ssu.gov.ua/ua/news/1/category/2/view/5213#.9yybILHi.dpbs

6. Голова СБУ відкрив Ситуаційний центр забезпечення кібернетичної безпеки. URL: https://ssu.gov.ua/ua/news/1/category/21/view/4318#.htoMBif9.dpbs

7. Державно-приватне партнерство у сфері кібербезпеки: міжнародний досвід та можливості для України: аналіт. доп. / за заг. ред. Д. Дубова. Київ: НІСД, 2018. 84 с.

8. Про практику застосування судами України законодавства про звільнення особи від кримінальної відповідальності: Постанова пленуму Верховного суду України від 23.12.05 р. № 12.

9. Кримінальний кодекс України: Закон України. URL: http://zakon.rada.gov.ua/laws/show/2341-14/print

10. Law enforcement – Internet service provider Cooperation. URL: https://www.coe.int/ru/web/cybercrime/lea-/-isp-cooperation

11. Про ратифікацію Конвенції про кіберзлочинність: Закон України 7.09.05 р. № 2824-IV. URL: http://zakon.rada.gov.ua/laws/show/2824-15

12. Про контррозвідувальну діяльність: Закон України від 6.12.02 р. № 374-IV. URL: http://zakon.rada.gov.ua/laws/show/374-15

13. Про Службу безпеки України: Закон України від 25.03.92 р. № 2229-XII. URL: http://zakon.rada.gov.ua/laws/show/2229-12

14. Про захист персональних даних: Закон України від 2010 р. URL: http://zakon.rada.gov.ua/laws/show/2297-17

15. Представники ІТ-галузі опублікували відкритий лист щодо запитів СБУ про Інтернет-користувачів. URL: https://ms.detector.media/media_law/law/predstavniki_itgaluzi_opublikuvali_vidkritiy_list_schodo_zapitiv_sbu_pro_internetkoristuvachiv

16. Провайдер не зобов'язаний "зливати" весь трафік спецслужбам. URL: https://ua.112.ua/interview/provaider-ne-zoboviazanyi-zlyvaty-ves-trafik-spetssluzhbam-228237.html

17. Кодекс України про адміністративні правопорушення: Закон України. URL: http://zakon.rada.gov.ua/laws/show/80731-10

18. Carr Madeline Public-private partnerships in national cyber-security strategieshttps. URL: //www.chathamhouse.org/sites/files/chathamhouse/publications/ia/INTA92_1_03_Carr.pdf

19. Про телекомунікації: Закон України. URL: http://zakon.rada.gov.ua/laws/ show/1280-15

20. Are you sharing the same ip address as a criminal? law enforcement call for the end of carrier grade nat (cgn) to increase accountability online. URL: https://www.europol.europa.eu/newsroom/news/are-you-sharing-same-ip-address-criminal-law-enforcement-call-for-end-of-carrier-grade-nat-cgn-to-increase-accountability-online.

21. Про державно-приватне партнерство: Закон України. URL: http://zakon.rada.gov.ua/laws/show/2404-17

22. Положення про Міністерство економічного розвитку і торгівлі України: Постанова Кабінету Міністрів України від 20.08.14 р. № 459. URL: http://zakon.rada.gov.ua/ laws/show/459-2014-%D0%BF

~~~~~~~~~~~~~ * * * ~~~~~~~~~~~~~
~~~~~~~~~~~~~