Облікова картка дисертації

I. Загальні відомості

Державний обліковий номер: 0821U101717

Особливі позначки: відкрита

Дата реєстрації: 07-06-2021

Статус: Захищена

Реквізити наказу МОН / наказу закладу:

II. Відомості про здобувача

Власне Прізвище Ім'я По-батькові:

1. Роллер Вікторія Миколаївна

2. Roller Viktoriia M.

Кваліфікація:

Ідентифікатор ORCID ID: Не застосовується

Вид дисертації: доктор філософії

Аспірантура/Докторантура: так

Шифр наукової спеціальності: 081

Назва наукової спеціальності: Право. Право

Галузь / галузі знань:

Освітньо-наукова програма зі спеціальності: Не застосовується

Дата захисту: 20-05-2021

Спеціальність за освітою: 081 Право

Місце роботи здобувача: Військовий інститут Київського національного університету імені Тараса Шевченка

Код за ЄДРПОУ: 22994521

Місцезнаходження: вул. Ломоносова, буд. 81, м. Київ, 03189, Україна

Форма власності:

Сфера управління: Міністерство оборони України

Ідентифікатор ROR: Не застосовується

III. Відомості про організацію, де відбувся захист

Шифр спеціалізованої вченої ради (разової спеціалізованої вченої ради): ДФ 26.001.128

Повне найменування юридичної особи: Київський національний університет імені Тараса Шевченка

Код за ЄДРПОУ: 02070944

Місцезнаходження: вул. Володимирська, буд. 60, м. Київ, 01033, Україна

Форма власності:

Сфера управління: Міністерство освіти і науки України

Ідентифікатор ROR: Не застосовується

IV. Відомості про підприємство, установу, організацію, в якій було виконано дисертацію

Повне найменування юридичної особи: Військовий інститут Київського національного університету імені Тараса Шевченка

Код за ЄДРПОУ: 22994521

Місцезнаходження: вул. Ломоносова, буд. 81, м. Київ, 03189, Україна

Форма власності:

Сфера управління: Міністерство оборони України

Ідентифікатор ROR: Не застосовується

V. Відомості про дисертацію

Мова дисертації:

Коди тематичних рубрик: 10.01.02, 10.01.08

Тема дисертації:

1. Правові засади забезпечення кібероборони України

2. Legal basis for supporting Cyber Defense in Ukraine

Реферат:

1. Дане дисертаційне дослідження присвячено аналізу правового забезпечення заходів кібероборони в Україні. У ході проведення дослідження здійснено аналіз поняття кіберпростір та встановлено, що його необхідно відрізняти від поняття мережі «Інтернет», оскільки мережа «Інтернет» є лише технічною складовою, яка об'єднує у собі комп'ютери, кабелі, роутери та ін. У дисертаційному досліджені запропоновано розглядати у кіберпросторі такі групи відносин: «людина та людина», «людина та організація», «організація та організація», «людина/організація та держава», «держава та держава».Також у дослідженні встановлено, що у кіберпросторі можуть вчинюватися різні види правопорушень.уже часто коли говорять про порушення у кіберпросторі мають на увазі інформаційні правопорушення, але проведеним аналізом встановлено, що інформаційні правопорушення це лише частина правопорушень, які вчиняються у кіберпросторі. Щодо порушень вчинюваних у кіберпросторі, дослідженням встановлено, що наразі існують

протиправні діяння, які здійснюються виключно за посередництвом використання кіберпростору, та можуть законодавчо бути віднесені до адміністративних правопорушень чи злочинів, або досі залишаються поза полем законодавчого регулювання, хоча за своїм змістом є деліктними. У ході виконання роботи встановлено, що способом вчинення будь якого правопорушення у кіберпросторі є кібератака. Автором здійснена класифікація кібератак за об'єктом здійснення нападу, а саме: кібератака на приватну особу, кібератака на організацію (юридичну особу) та кібератака на державу. Також встановлено, що в залежності від мотивів, обставин та наслідків вчинення кібератаки, кібератаку яка здійснюється на державу, теоретично, можливо розглядати як акт агресії. Такий висновок надає змогу говорити про ведення кібервійн між державами. У нашій роботі ми дійшли висновку, що кіберпростір можливо розглядати як поле ведення воєнних дій, а також кібератаки за відповідних умов можливо розглядати як напад на державу. Також у дослідженні аргументовано, що закріплення в українському законодавстві критеріїв, коли кібератаку можливо вважати нападом на державу, дозволить здійснити належне правове забезпечення діяльності Збройних Сил України та забезпечити адекватне реагування на кібератаки, які здійснюються на державу. У роботі встановлено, що проведення кібератак та кібероперацій є частиною військових операцій, які проводяться арміями світу, а також, є частиною гібридних війн, які ведуться поза межами правового регулювання. В Україні створена та функціонує система органів, які здійснюють заходи із забезпечення кібербезпеки, відбиття кібератак та здійснення заходів кібероборони. У роботі здійснено огляд повноважень цих органів та детальну увагу приділено саме нормативно - правовому закріпленню повноважень Міністерства оборони України та Генерального штабу Збройних Сил України щодо здійснення заходів кібероборони. Найбільш значущим є питання: з якого моменту відповідальний орган має розпочинати виконання заходів не просто відбиття чи блокування кібератки, а саме здійснення заходів кібероборони, та який зміст мають ці заходи. У зв'язку з цим, у роботі запропоновано здійснити термінологічне відмежування кібератаки як адміністративного чи кримінального правопорушення від кібератки, як акту агресії (тобто нападу на державу). Таким чином, запропоновано такий ланцюг термінів: кіберінцендент кібератака кібернапад. Таким чином, кібернападом необхідно вважати кібератаку яка має ознаки акту агресії. У такому випадку, заходи кібероборони необхідно розпочинати у разі здійснення кібернападу на інформаційно-телекомунікаційні ресурси нашої держави. Крім цього, у роботі окреслено ще два проблемні питання, які можуть поліпшити стан правого забезпечення здійснення кібероборони в Україні, а саме, врегулювання питання формування переліку об'єктів критичної інфраструктури держави, які є найбільш потенційними об'єктами кібератак та вчинення кібератак на які може призвести до найбільш негативних наслідків.Другим питанням, яке є перспективним у розвитку подальшого майбутнього нашої держави, є вироблення державної політики щодо державно - приватного партнерства у сфері забезпечення кібербезпеки, здійснення кіберзахитсу та кібероборони інформацінийх ресурсів нашої держави.

2. This dissertation research is devoted to the analysis of the legal support of cyber defense measures in Ukraine, procedure and grounds for cyber defense of the state and the use of the Armed Forces of Ukraine in such activities. The study analyzed the concept of cyberspace and found that this environment should be distinguished from the concept of "Internet", because the Internet is only a technical component that combines computers, cables, routers, etc .The study identified the main features that are inherent in cyberspace, namely that cyberspace is closely related to the information space, but is not identical to it; Considering legal relations in cyberspace, it is possible to classify such legal relations according to the subjective composition of these legal relations. Thus, in the dissertation research it is proposed to consider the following groups of relations in cyberspace: "human and human", "human and organization", "organization and organization", "human / organization and state", "state and state". The study also found that different types of offenses can be committed in cyberspace. That is, information offenses can be independent, or be committed in cyberspace. This is due to the fact that in cyberspace there is an information space and information is exchanged, which in turn can lead to certain violations and the commission of information offenses. With regard to violations committed in cyberspace, the study found that there are currently certain illegal acts that are committed exclusively through the use of cyberspace, and can be legally classified as administrative offenses or felonies, or still remain outside the scope of legislation, although their

content is tortious. In the course of the work it was established that the way to commit any offense in cyberspace is a cyber attack. The study classified cyberattacks according to the object of the attack, namely: cyberattack on an individual, cyberattack on an organization (legal entity) and cyberattack on the state. It is also established that, depending on the motives, circumstances and consequences of a cyberattack, a cyberattack carried out on the state, in theory, can be considered as an act of aggression. This conclusion allows for further analysis of cyber attacks as acts of aggression and talk about cyberwarfare between states. In our work, we came to the conclusion that cyberspace can be considered as a field of hostilities, and cyber attacks under appropriate conditions can be considered as acts of aggression. Ukraine has established and operates a system of bodies that carry out measures to ensure cybersecurity, repel cyberattacks and implement cyber defense measures. The review of the powers of these bodies is carried out in the work and detailed attention is paid to the normative - legal consolidation of the powers of the Ministry of Defense of Ukraine and the General Staff of the Armed Forces of Ukraine regarding the implementation of cyber defense measures. The most important question is: from what moment should the responsible body start implementing measures not just to repel or block cyberattacks, but also to implement cyber defense measures, and what is the meaning of these measures. In this regard, the paper proposes to make a terminological distinction between a cyberattack as an administrative or criminal offense from a cyberattack as an act of aggression. Thus, the following chain of terms is proposed: cyber incident - cyber attack □ cyber aggression. Thus, a cyber attack should be considered a cyber aggression that has signs of an act of aggression. In this case, cyber defense measures must be initiated in the event of a cyber attack on the information and telecommunications resources of our state. In addition, the paper outlines two other issues that can improve the state of legal support for cyber defense in Ukraine. The first one is settlement the list of the states objects of critical infrastructure, which are the most potential objects of cyberattacks and cyberattacks on which can lead to the most negative consequences. The second issue, which is promising in the development of the future of our state, is the development of public policy on public-private partnership in sphere of cybersecurity and cyber defense of information resources of our state.

Державний реєстраційний номер ДіР:

Пріоритетний напрям розвитку науки і техніки:

Стратегічний пріоритетний напрям інноваційної діяльності:

Підсумки дослідження:

Публікації:

Наукова (науково-технічна) продукція:

Соціально-економічна спрямованість:

Охоронні документи на ОПІВ:

Впровадження результатів дисертації:

Зв'язок з науковими темами:

VI. Відомості про наукового керівника/керівників (консультанта)

Власне Прізвище Ім'я По-батькові:

1. Пєтков Сергій Валерійович

2. Petkov Serhii V.

Кваліфікація: д.ю.н., 12.00.07

Ідентифікатор ORCID ID: Не застосовується

Додаткова інформація:

Повне найменування юридичної особи:

Код за ЄДРПОУ:

Місцезнаходження:

Форма власності:

Сфера управління:

Ідентифікатор ROR: Не застосовується

VII. Відомості про офіційних опонентів та рецензентів

Офіційні опоненти

Власне Прізвище Ім'я По-батькові:

1. Христинченко Надія Петрівна
2. Khrystynchenko Nadiia P.

Кваліфікація: д. ю. н., 12.00.07

Ідентифікатор ORCID ID: Не застосовується

Додаткова інформація:

Повне найменування юридичної особи:

Код за ЄДРПОУ:

Місцезнаходження:

Форма власності:

Сфера управління:

Ідентифікатор ROR: Не застосовується

Власне Прізвище Ім'я По-батькові:

1. Шопіна Ірина Миколаївна
2. Shopina Iryna M.

Кваліфікація: д.ю.н., 12.00.07

Ідентифікатор ORCID ID: Не застосовується

Додаткова інформація:

Повне найменування юридичної особи:

Код за ЄДРПОУ:

Місцезнаходження:

Форма власності:

Сфера управління:

Ідентифікатор ROR: Не застосовується

Рецензенти

Власне Прізвище Ім'я По-батькові:

1. Карелін Владислав Володимирович

2. Karelin Vladyslav V.

Кваліфікація: д. ю. н., 12.00.08

Ідентифікатор ORCID ID: Не застосовується

Додаткова інформація:

Повне найменування юридичної особи:

Код за ЄДРПОУ:

Місцезнаходження:

Форма власності:

Сфера управління:

Ідентифікатор ROR: Не застосовується

Власне Прізвище Ім'я По-батькові:

1. Хомяков Дмитро Олегович

2. Khomiakov Dmytro O.

Кваліфікація: к. ю. н., 12.00.07

Ідентифікатор ORCID ID: Не застосовується

Додаткова інформація:

Повне найменування юридичної особи:

Код за ЄДРПОУ:

Місцезнаходження:

Форма власності:

Сфера управління:

Ідентифікатор ROR: Не застосовується

VIII. Заключні відомості

Власне Прізвище Ім'я По-батькові голови ради Коропатнік Ігор Михайлович

Власне Прізвище Ім'я По-батькові головуючого на засіданні Коропатнік Ігор Михайлович

Відповідальний за підготовку облікових документів

Реєстратор

Керівник відділу УкрІНТЕІ, що є відповідальним за реєстрацію наукової діяльності

Юрченко Т.А.