УДК 342.9

КУЛЕШОВ М.В., перший заступник начальника
ДКІБ Служби безпеки України

СУТНІСТЬ ТА ЗМІСТ РОЗСЛІДУВАННЯ КІБЕРІНЦИДЕНТІВ ТА КІБЕРАТАК ПІДРОЗДІЛАМИ СБ УКРАЇНИ

Анотація. *У статті здійснено аналіз змісту діяльності з розслідування кіберінцидентів та кібератак щодо державних електронних інформаційних ресурсів, інформації, вимога щодо захисту якої встановлена законом, критичної інформаційної інфраструктури, проведено відмежування такого розслідування від досудового слідства, а також визначено загальний обсяг повноважень співробітників СБ України, залучених до цього процесу.*

Ключові слова: *забезпечення кібербезпеки, розслідування кіберінцидентів та кібератак, повноваження підрозділів СБ України.*

Summary. *The article analyzes the nature of the investigation of cyberincidents and cyberattacks on state electronic information resources, information the protection of which is required by law, critical information infrastructure, delimitates such an investigation from the pre-trial investigation, and also determines the total amount of responsibilities of the SSU officers involved in this activity.*

Keywords: *ensuring cybersecurity, investigation of cyberincidents and cyberattacks, the resposibilities of the officers of the Security Service of Ukraine.*

Аннотация. *В статье осуществлён анализ содержания деятельности по расследованию киберинцидентов и кибератак государственных электронных информационных ресурсов, информации, требование по защите, которой установлено законом, критической информационной инфраструктуры, проведено отграничение такого расследования от досудебного следствия, а также определён общий объем полномочий сотрудников СБ Украины, вовлечённых в эту деятельность.*

Ключевые слова: *обеспечение кибербезопасности, расследование киберинцидентов и кибератак, полномочия подразделений СБ Украины.*

Постановка проблеми. У зв’язку із прийняттям Закону України “Про основні засади забезпечення кібербезпеки України”, формуванням системи суб’єктів забезпечення кібербезпеки й розподілом відповідних функцій та повноважень між ними, законодавцем було введено ряд понять та категорій, які потребують інтегрування у вже існуючу модель правоохоронної діяльності. Наразі визначення сутності та змісту потребує діяльність з розслідування кіберінцидентів та кібератак щодо державних електронних інформаційних ресурсів, інформації, вимога щодо захисту якої встановлена законом, критичної інформаційної інфраструктури, оскільки завдання щодо здійснення таких розслідувань були поставлені Службі безпеки України відносно недавно, а процесуальна форма цієї діяльності ще не була сформована. Окремим проблемним аспектом є визначення загального змісту повноважень співробітників СБ України, які проводять такі розслідування.

Відсутність нормативного регулювання процесу розслідування кіберінцидентів та кібератак підрозділами СБ України не дозволяє повною мірою застосовувати наявний потенціал сил та засобів з протидії зазначеним негативним явищам в кіберпросторі, що негативно позначається на виконанні завдань щодо захисту інформаційної безпеки та її складової – кібербезпеки. А, як зазначає І.П. Бахновська, нині національна безпека

значною мірою залежить від забезпечення інформаційної безпеки, оскільки захищеність інформації та її повнота впливають на стабільність у суспільстві, забезпечення прав і свобод громадян, правопорядок і навіть на збереження цілісності держави [1, с. 106].

Результати аналізу наукових публікацій. Наразі наукові публікації, які стосуються саме сутності, змісту й нормативно-правового регулювання розслідування кіберінцидентів та кібератак відсутні, що свідчить про актуальність дослідження обраної тематики. Окремі аспекти досліджуваної теми розкриті в наукових працях наступних вчених.

Так, технічні питання забезпечення кібербезпеки України досліджували О.Ю. Козлова, В.Г. Кононович, І.В. Кононович, М.Г. Романюков, Л.М. Тимошенко. Соціальні, правові та інші аспекти забезпечення кібербезпеки розкрито І.П. Бахновською, С.А. Вітер, І.В. Діордіцею, М.М. Присяжнюком, І.І. Світлишиним, О.В. Ставицьким, Є.І. Цифрою та А.Ю. Шинкаренком та ін.

Проте, незважаючи на значний масив наукових розвідок в сфері забезпечення інформаційної безпеки та кібербезпеки, питання сутності та змісту, а також нормативно-правового регулювання розслідування кіберінцидентів та кібератак залишились поза увагою науковців, що обумовлює важливість обраної теми.

Метою статті є науково-практичний аналіз сутності розслідування кіберінцидентів та кібератак щодо державних електронних інформаційних ресурсів, інформації, вимога щодо захисту якої встановлена законом, критичної інформаційної інфраструктури, виділення сутності та визначення загального змісту дій співробітників СБ України в контексті такого розслідування.

Виклад основного матеріалу. Згідно розділу 2 Стратегії кібербезпеки України, затвердженої Указом Президента України від 15 березня 2016 року № 96/2016, сучасні інформаційно-комунікаційні технології можуть використовуватися для здійснення терористичних актів, зокрема шляхом порушення штатних режимів роботи автоматизованих систем керування технологічними процесами на об'єктах критичної інфраструктури. Більшого поширення набуває політично вмотивована діяльність у кіберпросторі у вигляді атак на урядові та приватні веб-сайти в мережі Інтернет. При цьому дедалі частіше об’єктами кібератак та кіберзлочинів стають інформаційні ресурси фінансових установ, підприємств транспорту та енергозабезпечення, державних органів, які гарантують безпеку, оборону, захист від надзвичайних ситуацій. Новітні технології застосовуються не лише для скоєння традиційних видів злочинів, але і для скоєння принципово нових видів злочинів, притаманних суспільству з високим рівнем інформатизації.

Враховуючи реалії сьогодення та характер існуючих загроз у сфері кібербезпеки, з метою практичного виконання завдань з реалізації курсу України на європейську та євроатлантичну інтеграцію, впровадження в систему планування єдиних процедур та правил, необхідних для підвищення ефективності сектору безпеки і оборони, для нейтралізації реальних та потенційних загроз національній безпеці України, дотримання цілісності, узгодженості та системності в опрацюванні документів за сферами національної безпеки, а також вжиття комплексу невідкладних заходів, спрямованих на підвищення обороноздатності держави з урахуванням наявних державних ресурсів, Кабінету Міністрів України, окрім іншого, доручено:

- забезпечити проведення оборонного огляду, огляду громадської безпеки та цивільного захисту, огляду стану кіберзахисту критичної інформаційної інфраструктури, державних інформаційних ресурсів та інформації, вимога щодо захисту якої встановлена законом;

- затвердити до 30 червня 2019 року порядки проведення огляду громадської безпеки та цивільного захисту і огляду стану кіберзахисту критичної інформаційної інфраструктури, державних інформаційних ресурсів та інформації, вимога щодо захисту якої встановлена законом [2].

Наведене вище свідчить про усвідомлення необхідності захисту кібербезпеки як складової інформаційної безпеки та спрямування зусиль суб'єктів національної системи кібербезпеки на виконання першочергових завдань, визначених нормативними актами, що регулюють забезпечення національної безпеки.

Відповідно до ст. 8 Закону України "Про основні засади забезпечення кібербезпеки України" (надалі – Закон), Служба безпеки України є одним із основних суб'єктів національної системи кібербезпеки, який, відповідно до Конституції і законів України виконує в установленому порядку такі основні завдання: здійснює запобігання, виявлення, припинення та розкриття злочинів проти миру і безпеки людства, які вчиняються у кіберпросторі; здійснює контррозвідувальні та оперативно-розшукові заходи, спрямовані на боротьбу з кібертероризмом та кібершпигунством, негласно перевіряє готовність об'єктів критичної інфраструктури до можливих кібератак та кіберінцидентів; протидіє кіберзлочинності, наслідки якої можуть створити загрозу життєво важливим інтересам держави; розслідує кіберінциденти та кібератаки щодо державних електронних інформаційних ресурсів, інформації, вимога щодо захисту якої встановлена законом, критичної інформаційної інфраструктури; забезпечує реагування на кіберінциденти у сфері державної безпеки.

В сучасному кіберпросторі кібератаки використовуються вже не тільки приватними особами, але й спецслужбами іноземних держав. І тут необхідно погодитись з І.В. Логіновим, Н.А. Ткачук та В.М. Удовиченком в тому, що "кібератаки, вмотивовані державою та спрямовані на викрадення інформації з обмеженим доступом, знищення, викривлення важливих для інших країн інформаційних ресурсів або блокування доступу до них з метою отримання політичних, економічних, військових переваг у зовнішньоекономічних стосунках, у мирний час становлять одну з сучасних форм розвідувально-підривної діяльності, а після оголошення стану війни можуть перетворитися на форму військових дій" [3, с. 105].

Окремо необхідно зазначити, що кіберінциденти та кібератаки щодо державних електронних інформаційних ресурсів, інформації, вимога щодо захисту якої встановлена законом, критичної інформаційної інфраструктури, можуть здійснюватися в межах спеціальних інформаційних операцій, які проводяться країною-агресором останні роки. Досліджуючи інформаційно-правове забезпечення спеціальних інформаційних операцій, О.О. Верголяс визначив наступні прийоми протиборства в інформаційній війні: одержання інформації про супротивника як у результаті аналізу відкритої інформації, що циркулює в ЗМІ, інформаційних системах тощо, так і в результаті її перехоплення, несанкціонованого доступу з наступним викривленням, знищенням, "перекодуванням" з метою формування оцінки, наміру й орієнтацій населення й осіб, що ухвалюють стратегічні рішення; придушення елементів інфраструктури державного й військового управління; радіоелектронна боротьба тощо. Методи інформаційної війни надзвичайно різноманітні: дезінформація, пропаганда, наклеп, неправда, приховування істотної інформації, зсув понять, відволікання уваги, інформаційне табуювання й інші [4, с. 128].

Фактично, враховуючи наведені вище обставини, діяльність, яка полягає в розслідуванні кіберінцидентів та кібератак і встановлення їх механізму, обставин, засобів, знарядь та виконавців, не може здійснюватись в межах захисту інформації штатними співробітниками підприємств, установ та організацій, а результати їх

діяльності в подальшому досить складно використати в межах розслідування кримінального провадження. Так, наприклад, С.А. Вітер та І.І. Світлишин, досліджуючи модель існування спецслужби з кібербезпеки, яку можуть представляти фахівці з організації інформаційної безпеки та проведення тестування на проникнення, інспектори з організації захисту секретної інформації, аналітики проектів із кібербезпеки, системні адміністратори, адміністратори комп'ютерних мереж, менеджери систем з інформаційної безпеки, аналітики систем забезпечення кібербезпеки, відносять до обов'язків таких фахівців наступне:

– виявлення уразливих місць системи та моделювання можливої ситуації стороннього кібервпливу з позиції загроз і пов'язаних із ними ризиків;

– контроль надійності функціонування системи захисту облікової інформації, розроблення заходів безпеки на випадок непередбачуваних подій;

– віднесення облікової інформації до категорії обмеженого доступу (службової і комерційної таємниць, іншої конфіденційної інформації);

– розроблення положень, політики і процедур у рамках системи безпеки облікової інформації;

– упровадження розроблених заходів безпеки та випробування системи з оцінкою її результативності, за необхідності внесення коригувань;

– встановлення користувачам комп'ютерної системи бухгалтерського обліку необхідних реквізитів захисту;

– навчання користувачів комп'ютерної інформаційної системи правилам безперервної обробки інформації;

– контроль за дотриманням користувачами комп'ютерної інформаційної системи та персоналом підприємства встановлених правил роботи з обліковою інформацією, що захищається у процесі її автоматизованої обробки [5, с. 501]

Як бачимо, повноваження чи обов'язки щодо розслідування кіберінцидентів та кібератак в наведеній моделі відсутні. Окрім того, внаслідок дій системних адміністраторів безпеки можуть бути втрачені чи перекручені дані і сліди протиправної діяльності, що унеможливить притягнення до відповідальності винних осіб чи подальше використання інформації про кіберінцидент чи кібератаку в оперативних та контррозвідувальних цілях.

Що ж стосується кіберінцидентів та кібератак щодо державних електронних інформаційних ресурсів, інформації, вимога щодо захисту якої встановлена законом, критичної інформаційної інфраструктури, то вони здатні спричинити реальну шкоду охоронюваним законом інтересам у сфері державної безпеки, з огляду на що важливість первинної діяльності, спрямованої на виявлення слідів протиправних дій та належного документування, складно переоцінити. Іншими словами, коли інтереси держави опиняються під загрозою спричинення значної шкоди особою, яка вчиняє протиправні дії у кіберпросторі, протидію такій діяльності та її розслідування повинен здійснювати суб'єкт забезпечення кібербезпеки.

Визначення кіберінцидентів та кібератак закріплено в п. 3 та 4 ст. 1 Закону. Так, кіберінцидентом визнається подія або ряд несприятливих подій ненавмисного характеру (природного, технічного, технологічного, помилкового, у тому числі внаслідок дії людського фактора) та/або таких, що мають ознаки можливої (потенційної) кібератаки, які становлять загрозу безпеці систем електронних комунікацій, систем управління технологічними процесами, створюють імовірність порушення штатного режиму функціонування таких систем (у тому числі зриву та/або блокування роботи системи,

та/або несанкціонованого управління її ресурсами), ставлять під загрозу безпеку (захищеність) електронних інформаційних ресурсів.

Кібератака ж визначається як спрямовані (навмисні) дії в кіберпросторі, які здійснюються за допомогою засобів електронних комунікацій (включаючи інформаційно-комунікаційні технології, програмні, програмно-апаратні засоби, інші технічні та технологічні засоби і обладнання) та спрямовані на досягнення однієї або сукупності таких цілей: порушення конфіденційності, цілісності, доступності електронних інформаційних ресурсів, що обробляються (передаються, зберігаються) в комунікаційних та/або технологічних системах, отримання несанкціонованого доступу до таких ресурсів; порушення безпеки, сталого, надійного та штатного режиму функціонування комунікаційних та/або технологічних систем; використання комунікаційної системи, її ресурсів та засобів електронних комунікацій для здійснення кібератак на інші об'єкти кіберзахисту. Як зазначає Р.В. Киричок, кібератака або хакерська атака (у вузькому розумінні) – це спроба реалізації загрози кіберзловмисниками (хакерами). Використовуючи різноманітні комбінації виявлених вразливостей, недоліки конфігураційних файлів систем та прогалини визначеної в корпорації політики безпеки, в залежності від своїх цілей, зловмисники можуть реалізувати різноманітні сценарії та навіть цілі стратегії нападу, при цьому залишившись непоміченими. Дані стратегії можуть бути спрямовані на різні ресурси КІС та включати багатоетапні ланцюги атакуючих дій, які в більшості випадків розпочинаються з імпортування та встановлення вірусів чи троянів на комп'ютери компаній через мережу Інтернет або надсилання шкідливих сценаріїв за допомогою електронної пошти, що дозволяє зловмисникам практично з легкістю заражати свої бажані цілі [6, с. 53-54].

Враховуючи, що здійснення кібератак та виникнення кіберінцидентів пов'язане з кваліфікованими діями осіб, які спеціалізуються на використанні кіберпростору, супроводжується застосуванням спеціалізованого технічного обладнання та шкідливого програмного забезпечення, процес розслідування зазначених кіберподій має складатись із взаємопов'язаних дій та заходів, спрямованих як на збирання конкретних даних, припинення шкідливої дії кіберінцидента чи кібератаки, так і удосконалення існуючої моделі та системи захисту з метою недопущення вчинення аналогічних дій в майбутньому. Саме в цьому контексті процес розслідування кібератак та кіберінцидентів відрізняється від процесу розслідування в кримінальному процесуальному розумінні.

Згідно п. 5 ч. 1 ст. 3 Кримінального процесуального кодексу України, досудове розслідування – стадія кримінального провадження, яка починається з моменту внесення відомостей про кримінальне правопорушення до Єдиного реєстру досудових розслідувань і закінчується закриттям кримінального провадження або направленням до суду обвинувального акта, клопотання про застосування примусових заходів медичного або виховного характеру, клопотання про звільнення особи від кримінальної відповідальності. Цілком очевидним є той факт, що досудове розслідування і розслідування кіберінцидентів та кібератак – це не тотожні поняття, оскільки не кожен кіберінцидент містить ознаки кримінального правопорушення, та не кожна кібератака може стати предметом розслідування.

Проаналізуємо відмінності процесу досудового розслідування та розслідування кібератак та кіберінцидентів.

1. Суб'єктом, який здійснює досудове слідство, є слідчий, суб'єктом здійснення розслідування кіберінцидентів та кібератак може бути співробітник функціонального підрозділу з контррозвідувального захисту інтересів держави у сфері інформаційної безпеки СБ України.

2. Не кожен кіберінцидент містить ознаки кримінального правопорушення. В залежності від обставин, механізму виникнення та наявності людського фактору кіберінциденти умовно можна поділити на наступні категорії: 1) прості кіберінциденти – подія або ряд несприятливих подій ненавмисного характеру, настання яких виключає дію людського фактору (КІК-4); 2) ускладнені кіберінциденти – подія або ряд несприятливих подій, настання яких супроводжувалось умисними чи необережними діями осіб поза кіберпростором (КІК-3) або у кіберпросторі (КІК-2), за відсутності ознак кібератаки; 3) кібератаки – активна та цілеспрямована форма кіберінцидента, механізм виникнення якої включає умисні та цілеспрямовані дії осіб, вчинені з метою досягнення результату, передбаченого п. 4 ст. 1 Закону (КІК-1).

При цьому кіберінциденти категорії КІК-4 взагалі виключають наявність суб'єкта злочину, кіберінциденти КІК-3 та КІК-3 можуть містити ознаки тих або інших кримінальних правопорушень, а можуть і не містити. Разом з тим вимога законодавця щодо розслідування кіберінцидентів та кібератак щодо державних електронних інформаційних ресурсів, інформації, вимога щодо захисту якої встановлена законом, критичної інформаційної інфраструктури, є прямою, з огляду на що процес такого розслідування має бути розпочатий в кожному випадку отримання інформації про кіберінцидент.

3. Навіть у випадку, коли наявні ознаки вчиненого кримінального правопорушення, не кожна інформація про кіберінцидент чи кібератаку може бути внесена до ЄРДР, оскільки, наприклад, у випадку, коли фактично вчинені дії утворюють склад злочину, передбаченого ч. 1 ст. 361 КК України, відповідно до вимог ч. 1 ст. 477 КПК України, провадження може бути розпочате слідчим, прокурором лише на підставі заяви потерпілого щодо кримінального правопорушення (кримінальне провадження у формі приватного обвинувачення). При цьому, як і в попередньому випадку, існує вимога закону щодо розслідування такого кіберінцидента чи кібератаки.

4. Пріоритетним аргументом в прийнятті рішення щодо початку розслідування в разі отримання інформації про кіберінцидент або кібератаку є не вимоги щодо підслідності злочинів, передбачені ч. 2 ст. 216 КПК України, а саме характер об'єкта, на який здійснюється злочинне посягання, або предмета посягання. Розслідування співробітниками СБ України розпочинається лише у випадку, коли кіберінциденти та кібератаки здійснювались щодо державних електронних інформаційних ресурсів, інформації, вимога щодо захисту якої встановлена законом, критичної інформаційної інфраструктури

Наведені відмінності свідчать про те, що розслідування кіберінцидентів та кібератак здійснюється поза межами досудового слідства, тобто поза кримінальним процесом. Причиною цьому є те, що, як правильно підкреслюють автори коментаря Закону України "Про основні засади забезпечення кібербезпеки України", "деякі види розвідувально-підривної діяльності у кіберпросторі (наприклад, добування розвідувальної інформації шляхом перехоплення й аналізу телекомунікаційного трафіку кіберрозвідками іноземних держав з позицій закордону, космічного простору, нейтральних вод) не можуть кваліфікуватись як протиправні діяння, і разом з тим несуть істотні загрози кібербезпеці держав, що розвідуються" [3, с. 105]. Саме цим пояснюється те, що діяльність з розслідування кіберінцидентів та кібератак зазначених об'єктів здійснюється саме в межах контррозвідувальної діяльності.

Разом з тим, якщо в ході розслідування буде встановлено, що виявлені події категорії КІК-3, КІК-2 та КІК-1 містять ознаки кримінального правопорушення, службова особа, яка призначила розслідування, має невідкладно повідомити про це орган досудового розслідування і вжити заходів щодо завершення розслідування,

складання висновку за його результатами та передачі матеріалів для прийняття процесуального рішення про внесення даних про виявлене кримінальне правопорушення у Єдиний реєстр досудових розслідувань.

Отже, задля встановлення змісту та обсягу повноважень суб'єктів, які здійснюють розслідування кіберінцидентів та кібератак, визначимо сутність цієї діяльності. Так, розслідування кібератак та кіберінцидентів – структурована сукупність дій та заходів, які здійснюються в межах забезпечення кібербезпеки України поза кримінальним процесом уповноваженими суб'єктами та спрямовані на встановлення механізму, обставин, засобів і знарядь та виконавців кіберінцидентів і кібератак, мінімізацію їх негативного впливу та шкідливих наслідків, а також вжиття заходів з попередження кіберінцидентів та кібератак у майбутньому.

Проведення розслідування кіберінцидентів та кібератак поза межами кримінального процесу означає, що особи, які його проводять, не можуть застосовувати інструментарій процесуальних, слідчих та негласних слідчих (розшукових) дій. Аналіз нормативно-правових актів, які регулюють оперативно-службову діяльність органів СБ України, дає підстави стверджувати, що з метою встановлення обставин, які підлягають з'ясуванню під час розслідування кібератак та кіберінцидентів, співробітники СБ України мають право: 1) здійснювати опитування осіб (за їх згодою отримуючи від них усні або письмові пояснення), які можуть повідомити будь-яку інформацію, що має значення для досягнення відповідних цілей розслідування; 2) отримувати від очевидців кіберінцидента чи кібератаки, службових осіб підприємства, установи, організації або інших громадян речі і документи, що мають значення для встановлення відповідних обставин кіберподії, яка є предметом розслідування; 3) отримувати у встановленому порядку дані щодо загроз національній безпеці з використанням кіберпростору або будь-яких інших кіберзагроз об'єктам кібербезпеки, кібератак та/або обставин, інформація про які може сприяти запобіганню, виявленню і припиненню таких загроз, протидії кіберзлочинам, кібератакам та мінімізації їх наслідків; 4) у порядку, погодженому із керівником підприємства, установи, організації, проводити візуальний і технічний огляд комп'ютерної та периферійної техніки, яка містить сліди кіберподії; 5) ознайомлюватись з документами та даними, що характеризують діяльність підприємств, установ та організацій, вивчати їх, за рахунок коштів, що виділяються на утримання підрозділів, які здійснюють оперативно-розшукову діяльність, виготовляти копії з таких документів, на вимогу керівників підприємств, установ та організацій – виключно на території таких підприємств, установ та організацій; 6) застосовувати спеціальне програмне забезпечення або технічні пристрої з метою отримання, збирання та накопичення інформації, необхідної для встановлення обставин кіберінцидента чи кібератаки; 7) залучати до проведення окремих заходів фахівців СБ України, проводити з ними консультації та отримувати від них письмові висновки щодо предмета розслідування; 8) здійснювати комп'ютерно-технічне дослідження а) зразків цифрової інформації, отриманої у ході ознайомлення з документами та даними, що характеризують діяльність підприємств, установ та організацій, б) комп'ютерної техніки, мережевих апаратних засобів та їх комплектуючих, залучати до таких досліджень відповідних фахівців; 9) за наявності підстав, передбачених ст. 207 КПК України, затримувати особу, в діях якої вбачаються ознаки кримінального правопорушення, та тимчасово вилучати її майно з метою подальшої передачі затриманої особи та вилученого майна уповноваженій службовій особі для вирішення питання про внесення даних про виявлене кримінальне правопорушення в ЄРДР та оформлення процесуального затримання особи в порядку ст. 208 КПК України.

Необхідно враховувати також, що розслідування кіберінцидентів та кібератак підрозділами СБ України носить відкритий характер і здійснюється в межах захисту кібербезпеки України. Результати окремих заходів можуть використовуватись в оперативній і контррозвідувальній діяльності, якщо їх зміст відповідає таким потребам. Проте сам процесуальний порядок не визначений ні нормативно-правовими актами СБ України, ні чинним законодавством, що ускладнює реалізацію окремих повноважень та знижує ефективність протидії кіберзагрозам.

Висновки.

В сучасних умовах законодавцем вживаються кроки щодо розширення механізму захисту кібербезпеки України як складової її інформаційної безпеки. Діяльність з розслідування кіберінцидентів та кібератак щодо державних електронних інформаційних ресурсів, інформації, вимога щодо захисту якої встановлена законом, критичної інформаційної інфраструктури віднесена до завдань СБ України як суб'єкта національної системи кібербезпеки.

Проте, навіть поверхневий аналіз загального змісту прав та обов'язків співробітників СБ України дає підстави стверджувати, що, незважаючи на специфічну сферу, в якій проводиться розслідування кіберінцидентів та кібератак, та важливість забезпечення інформаційної безпеки як складової національної безпеки, законодавчі ініціативи в частині надання суб'єктам забезпечення кібербезпеки додаткових повноважень явно не відповідають потребам сьогодення. Тому подальші наукові розвідки, спрямовані на пошук альтернатив та перспектив розширення правоохоронних можливостей СБ України в частині забезпечення кібербезпеки, є актуальними та необхідними.

Використана література

1. Бахновська І. П. Аналіз основних принципів забезпечення кібербезпеки в проекті Закону України "Про основні засади забезпечення кібербезпеки України". *Науковий вісник Ужгородського національного університету. Серія "Право".* Ужгород, 2016. Вип. 40(2). С. 106-109.

2. Про організацію планування в секторі безпеки і оборони України Рішення Ради національної безпеки і оборони України від 16 травня 2019 року: Указ Президента України від 16.05.19 р. № 225/2019. URL: http://www.rnbo.gov.ua/documents/502.html

3. Науково-практичний коментар Закону України "Про основні засади забезпечення кібербезпеки України"; станом на 1 січня 2019 року / М.В. Гуцалюк та ін.; за ред. М.В. Гребенюка. Київ: Національна академія прокуратури України, 2019. 220 с.

4. Верголяс О.О. Інформаційно-правове забезпечення спеціальних інформаційних операцій. *Інформація і право*. № 4(27)/2018. С. 126-133.

5. Вітер С.А., Світлишин І.І. Захист облікової інформації та кібербезпека підприємства *Науковий вісник Мукачівського державного університету. Серія "Економіка і суспільство"*. 2017. Вип. 11. С. 497-502.

6. Киричок Р.В. Тест на проникнення як імітаційний підхід до аналізу захищеності корпоративних інформаційних систем. *Сучасний захист інформації*. 2018. № 2(34). С. 53-58.

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