ДО ПИТАННЯ ПРО ОРГАНІЗАЦІЮ КОНТРРОЗВІДУВАЛЬНОЇ ДІЯЛЬНОСТІ В СФЕРІ КІБЕРБЕЗПЕКИ

ЗОТОВ Нікіта Миколайович - юрист ТОВ «Магістраль Захід»

ЛЕХ Роман Вікторович - завідувач спеціальної кафедри № 2 ІПЮК для Служби безпеки України Національного юридичного університету імені Ярослава Мудрого

СОКОЛОВСЬКИЙ Максим Валерійович - доцент спеціальної кафедри № 2 ІПЮК для Служби безпеки України Національного юридичного університету імені Ярослава Мудрого

DOI 10.32782/NP.2022.1.31

Запропонована стаття присвячена вивченню питання організації контррозвідувальної діяльності в сфері кібербезпеки. Встановлено, що з ростом кількості комп'ютеризованих систем та автоматизованих інструментів багато видів роботи почало переходити в IT-поле. На підприємствах з'явилися співробітники з інформаційної безпеки. Спочатку інформаційна безпека означала мінімізацію кількості доступів до бухгалтерської інформації, різної документації, інформації про патенти і багато чому іншому. Для цього створювалися регламенти з внутрішньої безпеки. Як правило, на підприємствах з'явився спеціальний співробітник, який відповідав за інформаційну безпеку. XXI століття зустріло нас IT-бумом: комп'ютер став з'являтися в кожному будинку, еволюція спричинила перехід від чорно-білого телефона до смартфона, який став необхідністю, а інтернет – необхідним елементом життя кожної людини. Все це призвело до того, що 2016 р. резолюція ООН закріпила серед прав людини «право на доступ до інтернету». З ростом девайсів, розумних речей, збільшенням трафіку, потоком даних, людина почала все більше переносити в кібер середовище і в хмару бухгалтерію, управління процесами, виконання робіт. З'явилася необхідність захисту інформації саме в діджитал (кібер) середовищі. Кібербезпека – це новий виток інформаційної безпеки, який спрямований саме на діджитал середовище. Кібербезпека має на увазі не тільки сам по собі захист інформації, а й захист всієї системи в інформаційному полі, в IT-полі (поле комп'ютерних технологій) в цілому.

Постановка проблеми

Глобальна інформатизація в наш час активно керує існуванням і життєдіяльністю держав світової спільноти, інформаційні технології застосовуються при вирішенні завдань забезпечення національної, військової, економічної безпеки та ін. Разом з тим, одним із фундаментальних наслідків глобальної інформатизації державних і військових структур стало виникнення принципово нової сфери протиборства конкуруючих держав - кіберпростору.

І якщо сьогодні між провідними у військовому та економічному відношенні світовими державами склався тією чи іншою мірою певний паритет у сфері застосування звичайних озброєнь, у міжнародному праві зафіксовано основні принципи взаємовідносин цих державами у рамках згаданої сфери,, то питання паритету і взаємовідносин в кіберпросторі на даний час продовжує залишатися відкритим.

У процесі формування глобального кіберпростору відбувається конвергенція військових та цивільних комп'ютерних технологій, у провідних державах інтенсивно розробляються нові засоби та методи активного впливу на інформаційну інфраструктуру потенційних супротивників, створюються різні спеціалізовані кібернетичні центри та підрозділи управління та командування, основним завданням яких є захист державних та військових інформаційних таємниць.

Надзвичайно важливим згадане питання є й для України, особливу у зв'язку з небезпеками, які ще більш загострились в умовах повномасштабної агресії РФ.

Стан дослідження

Питання кібербезпеки загалом, а також захисту вітчизняного кіберпростору зокрема неодноразово досліджували вітчизняні вчені – юристи, а також фахівці ІТ галузі.

Серед український науковців у своїх роботах це питання досліджували В. Биков, О. Буров, Н. Дементієвська, Д. Дубов, Ю. Лісовська, Н. Ткачук, Т. Соколовський та інші.

Метою цієї статті є вивчення питання організації контррозвідувальної діяльності в сфері кібербезпеки.

Виклад основного матеріалу дослідження

З ростом кількості комп'ютеризованих систем та автоматизованих інструментів багато видів роботи почало переходити в ІТ-поле. На підприємствах з'явилися співробітники з інформаційної безпеки.

Спочатку інформаційна безпека означала мінімізацію кількості доступів до бухгалтерської інформації, різної документації, інформації про патенти і багато чому іншому. Для цього створювалися регламенти з внутрішньої безпеки. Як правило, на підприємствах з'явився спеціальний співробітник, який відповідав за інформаційну безпеку..

XXI століття зустріло нас ІТ-бумом: комп'ютер став з'являтися в кожному будинку, еволюція спричинила перехід від чорно-білого телефона до смартфона, який став необхідністю, а інтернет – необхідним елементом життя кожної людини. Все це призвело до того, що 2016 р. резолюція ООН закріпила серед прав людини «право на доступ до інтернету».

З ростом девайсів, розумних речей, збільшенням трафіку, потоком даних, людина почала все більше переносити в кібер середовище і в хмару бухгалтерію, управління процесами, виконання робіт. З'явилася необхідність захисту інформації саме в діджитал (кібер) середовищі.

Кібербезпека – це новий виток інформаційної безпеки, який спрямований саме на діджитал середовище. Кібербезпека має на увазі не тільки сам по собі захист інформації, а й захист всієї системи в інформаційному полі, в ІТ-полі (поле комп'ютерних технологій) в цілому [1].

Законом України «Про основні засади забезпечення кібербезпеки України» визначаються основні поняття зазначеної проблемної галузі. Зокрема, ст. 1 Закону визначає кібербезпеку як «захищеність життєво важливих інтересів людини і громадянина, суспільства та держави під час використання кіберпростору, за якої забезпечуються сталий розвиток інформаційного суспільства та цифрового комунікативного середовища, своєчасне виявлення, запобігання і нейтралізація реальних і потенційних загроз національній безпеці України у кіберпросторі» [2]. Водночас ст. 2 Закону пояснює: «1. Цей Закон не поширюється на: 1) відносини та послуги, пов'язані із змістом інформації, що обробляється (передається, зберігається) в комунікаційних та/або в технологічних системах; ... 3) соціальні мережі, приватні електронні інформаційні ресурси в мережі Інтернет (включаючи блог-платформи, відеохостинги, інші веб-ресурси), якщо такі інформаційні ресурси не містять інформацію, необхідність захисту якої встановлена законом, відносини та послуги, пов'язані з функціонуванням таких мереж і ресурсів; …». Інакше кажучи, чинний Закон не передбачає будь-які дії з безпеки стосовно людини, яка не входить до критичної інформаційної інфраструктури держави, а людський складник інтелектуального капіталу (який набуває зростаючого значення в усьому світі) не входить до критичного ресурсу України. І це в той час, коли в усьому світі основна боротьба йде за людські та інтелектуальні ресурси, тобто за тих, хто вже завтра буде забезпечувати конкурентоспроможність країни [3, с. 314].

Цей напрям як пріоритетний формально визначено в цілій низці законодавчих актів України, що стосуються розвитку національної безпеки, інформаційного (цифрового) суспільства, цифрової економіки, європейської та євроатлантичної інтеграції України, тощо [4, с. 59]. Так, наприклад, метою Стратегії кібербезпеки України є створення умов для безпечного функціонування кіберпростору, його використання в інтересах особи, суспільства і держави, для досягнення якої, поряд з іншим, необхідними є поглиблення міжнародного співробітництва у цій сфері. В щорічних планах заходів з її реалізації передбачено заходи з виконання завдання щодо розвитку міжна-

родного співробітництва у сфері забезпечення кібербезпеки, підтримці міжнародних ініціатив у цій сфері та співпраці України з ЄС та НАТО для посилення спроможностей України у сфері кібербезпеки, участі у заходах зі зміцнення довіри у кіберпросторі [5].

Реалізація зазначеної вище Стратегії безпосередньо здійснюється основними суб'єктами національної системи кібербезпеки, Міністерством закордонних справ України, Міністерством цифрової трансформації України, Міністерством освіти і науки України та іншими суб'єктами забезпечення кібербезпеки в межах їх компетенції.

Особливе місце у сфері забезпечення національної кібербезпеки займають контррозвідувальні органи України.

Для початку з'ясуємо, що ж собою являє контррозвідувальна діяльність загалом і в чому її суть.

Згідно Закону України «Про контррозвідувальну діяльність», під останньою потрібно розуміти спеціальний вид діяльності у сфері забезпечення державної безпеки, яка здійснюється з використанням системи контррозвідувальних, пошукових, режимних, адміністративно-правових заходів, спрямованих на попередження, своєчасне виявлення і запобігання зовнішнім та внутрішнім загрозам безпеці України, розвідувальним, терористичним та іншим протиправним посяганням спеціальних служб іноземних держав, а також організацій, окремих груп та осіб на інтереси України [6].

Функції органів, підрозділів та співробітників Служби безпеки України, що здійснюють контррозвідувальну діяльність, визначаються Законом України «Про Службу безпеки України».

Для виконання визначених законом завдань та за наявності підстав, передбачених статтею 6 Закону про контррозвідувальну діяльність, в ході контррозвідувальної діяльності органи, підрозділи та співробітники Служби безпеки України мають право: 1) здійснювати контррозвідувальний пошук, оперативно-розшукові заходи з використанням оперативних та оперативно-технічних сил і засобів, опитувати осіб за їх згодою, використовувати їх добровільну допомогу; 2) виявляти, фіксувати і документувати гласно і негласно розвідувальні, терористичні та інші посягання на державну безпеку України, вести їх оперативний облік, здійснювати візуальне спостереження в громадських місцях із застосуванням фото-, кіно- і відеозйомки, оптичних та радіоприладів, інших технічних засобів; 3) проводити контррозвідувальні операції та відповідні оперативні і оперативно-технічні заходи з метою попередження, своєчасного виявлення і припинення розвідувально-підривної, терористичної та іншої протиправної діяльності на шкоду державній безпеці України; 4) мати гласних і негласних штатних і позаштатних працівників, створювати з метою конспірації підприємства, установи та організації, використовувати документи, що зашифровують особу чи відомчу належність працівників, приміщень і транспортних засобів органів та підрозділів, що здійснюють контррозвідувальну діяльність; 5) витребовувати, збирати і вивчати, за наявності визначених законом підстав, документи та відомості, що характеризують діяльність підприємств, установ, організацій, а також спосіб життя окремих осіб, джерела і розміри їх доходів для попередження і припинення розвідувальних, терористичних та інших протиправних посягань на державну безпеку України; 6) виключно з метою попередження, своєчасного виявлення і припинення розвідувальних, терористичних та інших посягань на державну безпеку України, отримання інформації в інтересах контррозвідки здійснювати на підставі відповідної контррозвідувальної справи заходи, визначені частиною третьою статті 8 Закону України «Про оперативно-розшукову діяльність», - лише за ухвалою слідчого судді, постановленою за клопотанням керівника відповідного оперативного підрозділу або його заступника, погодженим прокурором. Нагляд за додержанням законів під час проведення контррозвідувальної діяльності здійснюється Генеральним прокурором, виконувачем його обов'язків або уповноваженими наказом Генерального прокурора заступниками Генерального прокурора; 7) затримувати і тримати у спеціально відведених для цього місцях: осіб, підозрюваних у підготовці чи проведенні розвідувально-підривної, терористичної діяльності та вчиненні інших кримінальних правопорушень, розслідування яких віднесено до компетенції органів Служби безпеки України,

- на строки і в порядку, що передбачені законами України; осіб, які проникли на об'єкти та у місця, що охороняються органами і підрозділами Служби безпеки України, - на строк до трьох годин, а у разі нагальної необхідності запобігання злочинові чи його припинення та з метою встановлення особи - до сімдесяти двох годин з повідомленням про це суду протягом 24 годин з моменту затримання для перевірки обгрунтованості цього запобіжного заходу. Проводити особистий огляд вказаних осіб та огляд речей, що знаходяться при них, транспортних засобів і вилучати документи та предмети, які можуть бути речовими доказами або є небезпечними для життя і здоров'я людей; 8) виключно для припинення розвідувальних, терористичних та інших протиправних посягань на державну безпеку України, а також при переслідуванні осіб, підозрюваних у проведенні такої діяльності, у будь-який час безперешкодно заходити і перебувати на території та в приміщеннях органів державної влади та їх структурних підрозділів, органів місцевого самоврядування, підприємств, установ та організацій, незалежно від форми власності, а на військові об'єкти, що охороняються, - в установленому порядку; 9) перебувати у порядку, погодженому з керівниками органів охорони державного кордону Державної прикордонної служби України, для вжиття контррозвідувальних заходів у межах прикордонної смуги, контрольованого прикордонного району, в пунктах пропуску через державний кордон і територіальному морі України; 10) у невідкладних випадках при здійсненні контррозвідувальних заходів безперешкодно користуватися засобами зв'язку, що належать підприємствам, установам і організаціям, а засобами зв'язку, що належать громадянам, - за їх згодою, з наступним відшкодуванням витрат за їх вимогою; 11) в інтересах забезпечення державної безпеки та виконання завдань контррозвідувальної діяльності організовувати, координувати і проводити наукові та науково-технічні дослідження, створювати у порядку, визначеному законодавством України, відповідні наукові установи та міжвідомчі координаційно-дорадчі органи; 12) зберігати, носити, застосовувати, використовувати зброю, спеціальні засоби, вживати заходів фізичного впливу відповідно до законів України та інших актів законодавства України, провозити зброю та спеціальні засоби в усіх видах транспорту; 13) користуватися правами, визначеними законами України «Про Службу безпеки України», «Про державну таємницю» та іншими законами України.

За твердженням Ю. Лісовської, структурний зміст контррозвідувальної діяльності полягає в попередженні, виявленні та припиненні розвідувально-підривної діяльності іноземних держав з використанням спеціальних сил і засобів, форм і методів, які сприяють вирішенню національних інтересів України, своєчасному прийняттю заходів, адекватних характеру та масштабам загроз цим інтересам, що основані на принципах правової демократичної держави, оперативної та ідеологічної доцільності у відповідності з чинним законодавством [7, с. 111].

З метою захисту національних інтересів України в сфері інформаційної та кібербезпеки, у складі Центрального управління Служби безпеки України створено спеціалізований Департамент контррозвідувального захисту інтересів держави у сфері інформаційної безпеки.

Окрім того, у структурі Служби безпеки України функціонує Ситуаційний центр забезпечення кібербезпеки, співробітники якого покликані протидіяти кіберрозвідкам іноземних держав, займатися боротьбою з кібертероризмом і кібершпигунством, здійснювати контррозвідувальні та оперативно-розшукові заходи, а також протидіяти спробам розхитати ситуацію в країні через різноманітні інформаційні вкиди.

Окрема увага співробітників Ситуаційного центру зосереджена на виявленні та нейтралізації цільових кібератак. Зазвичай це загрози підвищеної складності. Об'єктами таких кібератак стають важливі комунікаційні системи державних органів і системи керування об'єктів критичної інфраструктури.

Так, фахівцями Ситуаційного центру забезпечення кібербезпеки Служби безпеки України 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 інформацій-

них 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 [8, с. 105].

Як вірно зазначає Ю. Лісовська, діяльність органів контррозвідки в сфері кібербезпеки провадиться як на стратегічному, так і тактичному рівнях. Форми системи контррозвідки визначаються за цільовим призначенням; силами і засобами, що використовуються; характером здійснення; територією, на якій проводяться превентивні заходи, та рівнем ухвалення рішення про проведення означених заходів. Саме на базі системного методу діяльність контррозвідувальних підрозділів із захисту інформаційних ресурсів в майбутньому надає гарантію їх захисту від заволодіння ними будь-якого супротивника [7, с. 116-117].

Важливим питанням захисту вітчизняного кіберпростору є можливість залучення до цього процесу приватних осіб, які не є співробітниками спеціальних державних структур протидії кіберзлочинності.

На нашу думку, варто погодитись з думкою Н. Ткачук, що залучення Службою безпеки України приватних 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 [8, с. 106].

Згідно оригінальної редакції Кримінального кодексу України 2001 р. проведення негласного виявлення вразливостей в інформаційно-телекомунікаційних системах об'єктів критичної інформаційної інфраструктури формально містило ознаки складу кримінального правопорушення, передбаченого ст. 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 України фактично унеможливлювало діяльність некомерційних пентестерів, якщо ці тести заздалегідь не погоджені із об'єктами атаки.

У вітчизняних наукових колах існувала думка, що механізм легалізації пентестінгу повинен полягати у застосуванні правового інституту звільнення від кримінальної відповідальності (наприклад, Д. Дубов пропонував доповнити ст. 361 КК України наступним пунктом: «звільняється від кримінальної відповідальності громадянин України, якщо таке втручання здійснювалось за погодженням із суб'єктами національної системи кібербезпеки…» [9, с. 79].

Н. Ткачук, підтримуючи наведену вище ідею, проте не погоджуючись із способом її вирішення, пропонувала доповнити ст. 361 КК України наступним пунктом: «Не є кримінальним правопорушенням 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 дозволило б створити правове поле для розвитку державно-приватної взаємодії за вказаним напрямом [8, с. 106].

Позитивно, що вітчизняний законодавець прислухався до думки громадськості і у Законі України «Про внесення змін до Кримінального кодексу України щодо підвищення ефективності боротьби з кіберзлочинністю в умовах дії воєнного стану» виклав ст. 361 КК України у новій редакції, де серед іншого у ч. 6 закріпив положення, згідно якого «Дії, передбачені частинами першою - четвертою цієї статті, не вважаються несанкціонованим втручанням в роботу інформаційних (автоматизованих), електронних комунікаційних, інформаційно-комунікаційних систем, електронних комунікаційних мереж, якщо вони були вчинені відповідно до порядку пошуку та виявлення потенційних вразливостей таких систем чи мереж».

Висновки

Підсумовуючи, можна констатувати, що зараз в Україні існує чітка і добре розгалужена система державних контррозвідувальних інституцій, покликаних забезпечувати кібербезпеку нашої держави. Можна також сміливо стверджувати, що уже зроблені доволі значні

SUMMARY

The proposed article is devoted to the study of the organization of counterintelligence activities in the field of cyber security.

In our time, global informatization actively controls the existence and vital activities of the states of the world community, information technologies are used to solve the tasks of ensuring national, military, economic security, etc. At the same time, one of the fundamental consequences of the global informatization of state and military structures was the emergence of a fundamentally new sphere of confrontation between competing states - cyberspace.

And if today the world's leading military and economic states have developed to one degree or another a certain parity in the field of conventional weapons, international law has recorded the main principles of relations between these states within the framework of the mentioned sphere, then the issue of parity and relations in cyberspace at the present time remains open.

In the process of the formation of global cyberspace, the convergence of military and civilian computer technologies is taking place, the leading states are intensively developing new means and methods of active influence on the information infrastructure of potential adversaries, various specialized cyber centers and management and command units are being created, the main task of which is the protection of state and military information secrets.

The mentioned issue is also extremely important for Ukraine, which is special in connection with the dangers, which have become even more acute in the conditions of full-scale aggression of the Russian Federation.

In order to protect the national interests of Ukraine in the field of information and cyber security, a specialized Department of counterintelligence protection of the state's interests in the field of information security was created as part of the Central Directorate of the Security Service of Ukraine.

In addition, within the structure of the Security Service of Ukraine there is a Cyber Security Situation Center, whose employees are called upon to counter cyber intelligence of foreign countries, fight cyber terrorism and cyber espionage, carry out counter-intelligence and operative investigative measures, as well as counter attempts to destabilize the situation in the country through various information leakages.

Special attention of the staff of the Situation Center is focused on the detection and neutralization of targeted cyber attacks. These are usually threats of increased complexity. The objects of such cyber-attacks are important communication systems of state bodies and management systems of critical infrastructure facilities.

Activities of counterintelligence agencies in the field of cyber security are carried out at both strategic and tactical levels. The forms of the counterintelligence system are determined by the target purpose; forces and means used; the nature of implementation; the territory on which preventive measures are carried out, and the level of decision-making on carrying out the specified measures. It is on the basis of the system method that the activity of counterintelligence units for the protection of information resources in the future provides a guarantee of their protection against the acquisition of them by any adversary.

кроки до правового врегулювання багатьох складних питань у згаданій сфері (наприклад, до правового регулювання залучення приватних осіб до процесу протидії кіберпосяганням).

Література

1. Інформаційна безпека і кібербезпека – в чому різниця? URL : https://indevlab.com/uk/blog-ua/informatsijna-bezpeka-i-kiberbezpeka-v-chomu-riznitsya/

2. Закон «Про основні засади забезпечення кібербезпеки України». ***Відомості Верховної Ради***. 2017. № 45. Ст. 403,

3. Биков В., Буров О., Дементієвська Н. Кібербезпека в цифровому навчальному середовищі. ***Інформаційні технології і засоби навчання***. 2019. Том 70. №2. С. 313-331.

4. Станіславський Т. Розвиток міжнародного співробітництва України у сфері кібербезпеки. ***Актуальні проблеми державного управління***. 2019. №3(79). С. 58-67.

5. Рішення Ради національної безпеки і оборони України від 14 травня 2021 р. «Про стратегію кібербезпеки України». URL : https://www.president.gov.ua/documents/4472021-40013

6. Закон України «Про контррозвідувальну діяльність». ***Відомості Верховної Ради України.*** 2003. № 12. Ст.89.

7. Лісовська Ю. Кібербезпека: ризики та заходи. К. : Кондор, 2019. 272 с.

8. Ткачук Н. Правове регулювання взаємодії Служби безпеки України з приватним сектором у сфері забезпечення кібербезпеки. ***Інформація і право***. 2018. №4 (27). С. 104-111.

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