**Л.В. Леонтьєва, О.Г. Ключко**

**(Харків, Україна)**

**КІБЕРБЕЗПЕКА В УКРАЇНІ: ПРАВОВІ АСПЕКТИ**

**Вступ.** У сучасному світі, де технології швидко розвиваються, кібербезпека стає надзвичайно важливою сферою для будь-якої країни. Україна, яка активно впроваджує інформаційні технології в різні сфери життя, не є винятком.

За даними глобального огляду, проведеного об’єднанням ISACA, тільки 38% респондентів вважають, що вони підготовлені до кібернападів, решта, 83%, відносять кібернапади до однієї з найнебезпечніших загроз для організації. За наявності великого обсягу персональної та кон- фіденційної інформації, яку пересилають за допомогою електронних засобів, несанкціонований доступ до неї може спричинити серйозні наслідки [1].

Кібербезпека є важливою темою для суспільства, оскільки вона стосується всіх, хто використовує інформаційні технології. У зв'язку зі зростанням кіберзагроз, кожна держава повинна мати свій власний підхід до забезпечення кібербезпеки.

Кібербезпека також є важливим аспектом міжнародних відносин. Розвиток інформаційної боротьби та перехід гонки озброєнь у кіберпростір вимагають від держав узгодження своїх підходів до кібербезпеки.

Згідно з думкою фахівців збройних сил США, повна адекватна система кіберзахисту повинна включати в себе такі підсистеми:

* Підсистема захисту, яка забезпечує захист від несанкціонованого доступу, поширення шкідливого програмного забезпечення та інших кіберзагроз.
* Підсистема виявлення, яка виявляє кібератаки на ранній стадії.
* Підсистема реагування, яка дозволяє відновити роботу систем після кібератаки.

Ці підсистеми повинні взаємодіяти між собою, щоб забезпечити ефективний захист від кіберзагроз.

Деякі автори вважають, що система кіберзахисту, яка відповідає вищезазначеним вимогам, не забезпечує повного захисту об'єктів інформатизації, особливо органів державної влади та оборони. Вони пропонують створювати єдину інтелектуальну систему кібербезпеки, яка є частиною системи інформаційної безпеки.

Така система повинна мати здатність адаптуватися до змін зовнішніх і внутрішніх кіберзагроз (кібератак) і технологій, які застосовуються для протидії їм. Це означає, що вона повинна постійно оновлюватися і вдосконалюватися.

Створення такої системи можливе лише за умови комплексного державного регулювання, яке включає в себе законодавче регулювання, ефективне правозастосування та ризик-менеджмент.

До прийняття Закону України «Про основні засади забезпечення кібербезпеки України» правову основу кібербезпеки України становили Конституція України, закони України «Про основи національної безпеки», «Про інформацію», «Про захист інформації в інформаційно-телекомуніка- ційних системах» та інші закони, Конвенція Ради Європи про кіберзлочинність [2], інші міжнародні договори, згода на обов’язковість яких надана Верховною Радою України, Доктрина інформаційної безпеки України, а також інші нормативно-правові акти .

Забезпечення кібербезпеки в Україні є важливим питанням національної безпеки. Воно ґрунтується на таких принципах:

* Верховенство права означає, що кібербезпека повинна забезпечуватися в рамках закону, з повагою до прав людини та основоположних свобод.
* Забезпечення національних інтересів означає, що кібербезпека повинна сприяти захисту національних інтересів України, включаючи її суверенітет, незалежність та територіальну цілісність.
* Відкритість, доступність, стабільність та захищеність кіберпростору означає, що кіберпростір повинен бути відкритим для законного використання, доступним для всіх громадян, стабільним і захищеним від кібератак.
* Розвиток мережі Інтернет та відповідальних дій у кіберпросторі означає, що мережа Інтернет повинна розвиватися та використовуватися відповідально, з урахуванням інтересів суспільства та держави.
* Державно-приватна взаємодія, широка співпраця з громадянським суспільством означає, що забезпечення кібербезпеки є завданням не лише держави, а й приватного сектору та громадянського суспільства.
* Пропорційність та адекватність заходів кіберзахисту реальним та потенційним ризикамозначає, що заходи кіберзахисту повинні бути співмірними з реальними та потенційними кіберзагрозами.
* Реалізація невід’ємного права держави на самозахист відповідно до норм міжнародного права в разі вчинення агресивних дій у кіберпросторі означає, що Україна має право захищатися від кібератак, які становлять загрозу її національній безпеці.
* Пріоритетність запобіжних заходів означає, що необхідно надавати перевагу заходам, які запобігають кібератакам, а не реагують на них.
* Невідворотність покарання за вчинення кіберзлочинів означає, що особи, які вчиняють кіберзлочини, повинні бути притягнуті до відповідальності.
* Пріоритетний розвиток та підтримка вітчизняного наукового, науково-технічного та виробничого потенціалу означає, що необхідно розвивати вітчизняні кібербезпекові технології та створювати умови для їх ефективного використання.
* Забезпечення демократичного цивільного контролю за утвореними відповідно до законів України військовими формуваннями та правоохоронними органами, що провадять діяльність у сфері кібербезпеки означає, що діяльність органів, відповідальних за кібербезпеку, повинна підлягати демократичному цивільному контролю.

Національна система кібербезпеки є складною системою взаємодії між різними важливими структурами в Україні. Ці структури включають Державну службу спеціального зв'язку та захисту інформації, Національну поліцію, Службу безпеки, Міністерство оборони та Генеральний штаб Збройних Сил. Також взаємодіють розвідувальні органи, Національний банк, агентства, спрямовані на забезпечення кібербезпеки та пов'язаних заходів у різних сферах. Ці заходи охоплюють політичні, науково-технічні, інформаційні, освітні, організаційні, правові, оперативно-розшукові, розвідувальні, контррозвідувальні, оборонні та інженерно-технічні аспекти. Крім того, система включає заходи криптографічного та технічного захисту національних інформаційних ресурсів та кіберзахист об'єктів критичної інформаційної інфраструктури.

**Висновок.**Слідвідзначити, щокібербезпека є актуальним і складнимзавданням для сучасних держав, і Україна не залишаєтьсяостороньцьоговажливогопитання. Забезпеченняефективноїкібербезпекивимагає не лишетехнічнихзаходів, але й комплексного підходу, якийохоплюєполітичні, правові, соціальні та економічніаспекти.

Важливимелементом є міжнароднеспівробітництво в галузікібербезпеки, оскількикіберзагрози не маютькордонів. Державиповинніузгоджуватисвоїпідходи та спільнореагувати на виклики, щовиникають у кіберпросторі. Запровадження сучасних систем кіберзахисту, виявлення та реагування на кібератаки є критично важливими аспектами для забезпечення стійкості та безпеки інформаційних систем.

Національна система кібербезпеки в Україні враховує принципи верховенства права, захисту національних інтересів, відкритості та демократичного контролю. Законодавча база та механізми правозахисту, уведені Законом України «Про основні засади забезпечення кібербезпеки України», створюють фундамент для ефективної роботи в цьому напрямку.

Забезпечення кібербезпеки – це невід’ємний елемент національної безпеки, і його успішна реалізація передбачає постійне вдосконалення та адаптацію до змін в кіберзагрозах та технологіях. Співпраця міждержавними і приватними секторами, а також залучення громадянського суспільства, є ключовими елементами успішної стратегії кібербезпеки для будь-якої країни.

**Література:**

1. Стандарти ISO/IEC захистять від кіберзагроз. 31.08.2016. URL: http://csm.kiev.ua. (дата звернення: 05.12.2023).
2. " Про кіберзлочинність. Конвенція Ради Європи від 21.11.2001. *Офіційний вісник України* від 10.09.2007 р. No 65. С. 107. Ст. 2535, код акту 40846/2007.