Анна-Христина Базарницька

Львівський національний університет імені Івана Франка, Львів, Україна

**НАПРЯМИ ПРОТИДІЇ КІБЕРЗЛОЧИНАМ**

Кіберзлочини – невідворотний результат глобалізації інформаційних процесів. Простота та легкість, анонімність та доступність – саме ті характеристики інформаційних технологій, які приваблюють людство, а також притягують увагу осіб, які коять злочини. Зі збільшенням використання інформаційних технологій у різних сферах людської діяльності збільшується і кількість злочинів, які вчиняються за допомогою їх використання. Щороку кількість потерпілих від кібершахраїв постійно зростає. Це зростання є неминучим процесом, адже через недосконале законодавче регулювання відносин у сфері інформаційних технологій не можливо випередити їх розвиток, або ж йти з ним одночасно.

Різні питання у сфері кіберзлочинності багаторазово були об’єктом наукових досліджень як вітчизняних, так і зарубіжних учених. Зокрема, цій проблематиці присвячені праці Р. Калюжного, О. Амеліна, О. Дзьобаня, Ю. Батуріна, М. Карчевського, В. Дзюндзюка, М. Кравцової, В. Бутузова, В. Лісового, В. Номоконова, В. Навроцького, В. Пилипчука, М. Погорецького, В. Шеломенцева, В. Сташиса, О. Юрасова та інших. Незважаючи на наявність великої кількості праць, присвячених дослідженню кіберзлочинів, існує потреба в подальшому вивченні даного поняття, адже на кожному етапі вона має нові особливості та елементи впливу.

Нині у світі приділяється значна увага вивченню проблем боротьби зі злодіяннями в кіберпросторі, які спричинені об’єктивними процесами розвитку інформаційно-телекомунікаційних технологій і введенням їх у різні сфери людської діяльності. Тому боротьба з кіберзлочинністю повинна бути пріоритетною функцією у державі. Результати аналізу кіберзлочинності дозволяють передбачати труднощі у боротьбі з нею з через прийоми вчинення комп’ютерних злочинів, які щороку набувають усе більш нового характеру. До вирішення даної проблеми потрібно підходити комплексно.

Фахівці виокремлюють декілька елементів організації діяльності правоохоронних органів у глобальних інформаційних мережах, серед них:

* вивчення і оцінювання ситуації в мережах;
* проведення найліпшої розстановки сил і засобів, забезпечення взаємодії;
* управління, планування і контроль;
* координація дій суб’єктів правоохоронних органів.

Сукупність потреб, задоволення яких забезпечує існування і можливість прогресивного розвитку громадян, суспільства та держави – це складова національних інтересів, без здійснення яких нереально забезпечити стабільний стан держави і суспільства, із нормальним розвитком країни як незалежного суб’єкта міжнародних відносин.

Важливо зазначити, що перелік напрямів державної політики кібербезпеки не може бути статичним, оскільки відбуваються постійні зміни в кіберсуспільстві, тому існує потреба швидкої реакції та вжиття відповідних заходів.

Українською проблемою є як недосконале законодавство, так і недостатня кількість державних експертів в області комп’ютерно-технічної експертизи.

Щодо напрямів державної політики кібербезпеки, то, вона має бути точно визначена та зафіксована в національному законодавстві. Нині такі спроби було зроблено при розробленні проекту Закону України «Про основні засади забезпечення кібербезпеки України» [1]. В даному законі напрями державної політики визначені у такий спосіб :

* формування захищеного національного сегмента кіберпростору, яке буде забезпечувати безпечне використання цього простору суспільством;
* посилення кібероборони;
* запобігання втручанню у внутрішні справи України і нейтралізація посягань на її інформаційні ресурси з боку інших держав;
* забезпечення повноправної участі України в загальноєвропейській та регіональних системах забезпечення кібербезпеки;
* боротьба з кіберзлочинністю та кібертероризмом;
* дотримання міжнародних зобов’язань у сфері боротьби з кібертероризмом та кіберзлочинністю;
* послаблення рівня вразливості об’єктів кіберзахисту (в т.ч. об’єктів критичної інформаційної інфраструктури).

Основними напрямами державної політики в кібернетичній сфері є:

* забезпечувати інформаційний (кібернетичний) суверенітет України (тобто держава має право здійснювати контроль над власним інформаційним простором через організацію управління процесами створення, збирання, одержання, зберігання, використання, поширення, охорони та захисту інформації відповідно до національних інтересів;
* вдосконалювaти державне регулювaння розвитку інформaційної сфери зaвдяки створенню економічних передумов для розвитку вітчизняної інформaційної інфраструктури, впровадження сучасних технологій у даній сфері, наповнення правдивою інформацією про Україну внутрішнього та світового інформаційного простору. А як напрям державної політики кібербезпеки можна визначити здійснення систематизації кібербезпекового законодавства України, створення необхідних передумов для розвитку кіберсфери в цілому, і зокрема формуванню кібернетичної безпеки;
* вживати комплексні заходи щодо захисту національного кіберпростору та протидії монополізації інформаційної сфери України
* активно залучати ЗМІ до запобігання і протидії корупції, зловживанням службовим становищем, іншим явищам, які загрожують національній безпеці України

Доктрина інформаційної безпеки України визначає національні інтереси України в інформаційній сфері, загрози їх реалізації, напрями і пріоритети державної політики в інформаційній сфері [2]. Вона виокремлює такі напрями державної політики кібернетичної безпеки [3]:

* необхідність створення цілісної системи моніторингу (аналіз, оцінки, прогноз) кіберзагроз та формування способів реагування на них на оперативному, тактичному та стратегічному рівнях;
* вдосконалення системи управління національною системою кібербезпеки (підвищувати рівень відповідальності та контролю за виконанням покладених на суб’єкти кібербезпеки завдань);
* законодавче регулювання механізму виявлення, фіксації, блокування та видалення з кібернетичного простору держави, інформації, що загрожує національним інтересам в кіберсфері;
* створення і розвиток структур, що відповідають за інформаційно-психологічну безпеку, насамперед у Збройних Силах України, з урахуванням практики держав-членів НАТО, а також і в Національній поліції – Кіберполіція, згідно з загальною концепцію розумного балансу розмежування повноважень у реалізації державної кібербезпекової політики її суб’єктами (Варто зазначити, що пріоритетами діяльності Національної поліції України у сфері розвитку інформаційних технологій, уніфікації зв’язку та кіберзахисту є:
* Посилення кібернетичної безпеки та створення передумов унеможливлення витоку службової інформації з баз даних Національної поліції;
* Поліцейська діяльність, керована аналітикою – ILP (Intelligence-Led Policing);
* розвиток і захист технологічної інфраструктури забезпечення кібербезпеки України та побудова ефективної системи стратегічних комунікацій;
* розвиток механізмів взаємодії держави та інститутів громадянського суспільства в реалізації державної кібербезпекової політики, в тому числі і в частині протидії гібридній війні та одному з її проявів — інформаційній агресії проти України та кібернетичним атакам;
* ефективна, проактивна та наступальна боротьба з дезінформацією та ворожою пропагандою з боку Російської Федерації (російська пропаганда негативно впливає на розвиток демократичних європейських країн).
* недопущення використання кібернетичного простору держави в деструктивних цілях або для дій, що спрямовані на дискредитацію України на міжнародному рівні
* виявлення та притягнення до відповідальності, забезпечення невідворотності покарання винних згідно з українським законодавством суб’єктів українського кібернетичного простору, що створені та/або використовуються державою-агресором для ведення кібернетичної війни проти України, та унеможливлення їхньої підривної діяльності.

**Висновки.** Можна стверджувати, що політика кібербезпеки держави визначається, зосереджуючи увагу на національних інтересах та загрозах кібернетичній безпеці України, а також реалізується шляхом втілення належних концепцій, доктрин, стратегій та програм у різних сферах кібернетичної безпеки відповідно до чинного законодавства. Отже, для протидії злочинам, що вчиняються у кіберпросторі, державі варто постійно посилювати безпеку інформаційних систем, вдосконалювати законодавство у сфері кібернетичних злочинів, збільшувати відповідальність за вчинення злочинних дій та інформаційних правопорушень у кіберпросторі, розширювати міжнародне співробітництво України у сфері безпечного використання інформаційних ресурсів.

**Список використаних джерел**

1. Про основні засади забезпечення кібербезпеки України: Закон України від 5 жовтня 2017 року № 2163-VIII.Редакція від 17.08.2022. URL: <http://surl.li/fnjzs>
2. Про рішення Ради національної безпеки і оборони України від 29 грудня 2016 року «Про Доктрину інформаційної безпеки України». Указ Президента України №47/2017
3. Діордіца І. В. Напрями державної кібербезпекової політики. URL: <http://surl.li/ftzbq>