Андрій Микитюк
студент 1стн курсу спеціальності 208 «Агроінженерія».
Науковий керівник: **Гаврилюк В. М.**
канд. екон. наук, асистент кафедри математичних дисциплін,
інформатики і моделювання
Подільський державний аграрно-технічний університет,
м. Кам'янець-Подільський

ФОРМУВАННЯ КІБЕРНЕТИЧНОЇ БЕЗПЕКИ УКРАЇНИ

XXI століття це ера інформаційних технологій і сучасний світ практично неможливо уявити без них. Основою даних технологій є широке використання комп'ютерної техніки та новітніх засобів комунікацій. Сьогодні комп'ютери впроваджуються в різноманітні галузі людської діяльності. Усі найважливіші функції сучасного суспільства, так чи інакше, пов'язані з комп'ютерами, комп'ютерними мережами і комп'ютерною інформацією.

Більшість держав світу не встигають за врегулюванням процесів, що спричинені стрімким розвитком інформаційних технологій (кібертехнологій), тобто науково-технічний прогрес відбувається на скільки швидко, що законодавчо врегульовувати відносини кіберпросторі стає надзвичайно важко.

Питанням кіберзлочинності займаються такі зарубіжні та українські вчені як: Волчинская Е., Баурин Ю., Дашян М., Дешамп С, Кохутов М., Марков А., Юрасов А. та ін.

Терміни «комп'ютерна злочинність», «кіберпростір» вперше з'явилась в американській, а потім і в іншій іноземній літературі на початку 60-х років минулого століття. «Комп'ютерна злочинність» – це порушення чужих прав та інтересів по відношенню до автоматизованих систем обробки даних [1, с. 387]. За останні 10-15 років сформувалось поняття «кіберзлочинність» – під якою розуміють злочинність в традиційному сенсі цього слова, але яка має місце в мережі Інтернет [2, с.165].

Кіберзлочинність – це поняття, яке охоплює, на нашу думку, комп'ютерну злочинність (де комп'ютер – предмет злочину, а інформаційна безпека – об'єкт злочину) та інші зазіхання, де комп'ютер є знаряддям або способом злочину проти власності, авторських прав, громадської безпеки, моралі тощо. В офіційних матеріалах ЄС міститься таке визначення кіберпростору: «віртуальний простір, в якому циркулюють електронні дані світових портативних комп'ютерів» [3].

У безпековому документі Великобританії Стратегія безпеки кіберпростору для Об'єднаного Королівства: убезпеченіти, безпека та еластичність кіберпростору кіберпростір визначений як «всі форми мережевої, цифрової активності. Він включає в себе контент та дії, що здійснюються через цифрові мережі»[4]. Водночас поняття «кіберпростір» так і не визначене в єдиному на сьогоднішній день міжнародному документі, спрямованому на протидію злочинам у кіберсфері – Конвенції про кіберзлочинність. В ухваленій 2018 року Стратегії кібербезпеки для Німеччини кіберпростір визначається як «вся інформаційна інфраструктура, що доступна через інтернет поза будь-якими територіальними кордонами» [4].

Розповсюдження комп'ютерних вірусів, шахрайства з пластиковими платіжними картками, крадіжки коштів з банківських рахунків, викрадення комп'ютерної інформації та порушення правил експлуатації автоматизованих електронно-обчислювальних систем – це далеко не повний перелік подібних злочинів. Дану категорію злочинів називають: кіберзлочини та комп'ютерні злочини. Оскільки вони використовуються для назви одних і тих самих суспільно-небезпечних діянь, то їх можна вважати синонімами та рівнозначними. У зв'язку з ратифікацією Україною Конвенції про кіберзлочинність 7 вересня 2015 року вважається за доцільне вживати термін «кіберзлочини», але в самій Конвенції відсутнє визначення терміну «кіберзлочинність».

На думку авторів кіберзлочинність – це особливий вид злочинних діянь, що здійснюються у кіберпросторі (або за допомогою його технічних можливостей), несуть у собі суспільну небезпеку і відповідальність за які передбачена законодавством.

Стратегія національної безпеки України зазначає, що Україна має «розробляти та впроваджувати національні стандарти та технічні регламенти застосування інформаційно-комунікаційних технологій, гармонізованих з відповідними європейськими стандартами, у тому числі згідно з вимогами ратифікованої Верховною Радою України Конвенції про кіберзлочинність», однак і досі: в Україні відсутні системні нормативні документи, що описували б загрози Україні саме у кіберпросторі, визнали б їх і формували цілісну державну політику з кібербезпеки; в Україні відсутні загальнонаціональні міжвідомчі координаційні структури; більшість представників відомств, задіяних у системі забезпечення кібербезпеки України, зазначають незадовільне кадрове забезпечення відомств відповідними фахівцями у сфері інформаційної безпеки; не завжди прозорим є розподіл обов'язків спеціальних державних інституцій щодо убезпечення кіберпростору держави.

Дана проблема є продовженням невизначеності нормативного поля, зокрема відсутності стратегічних документів, в яких подібний розподіл обов'язків (можливо із визначенням відповідального органу) було б зроблено.

Україна залишається уразливою (особливо її телекомунікаційна складова), й не в останню чергу через надмірно широке запровадження західних програмних продуктів і використання матеріально-технічної бази іноземного виробництва; відсутні усталені визначення ключових понять і термінів («кіберпростір», «кібербезпека», «кіберзахист», «кібератака», «кібервійна», «кібертероризм», «кіберзброя», «кіберінфраструктура», «критична кіберінфраструктура»), що можуть ефективно застосовуватися в практиці правоохоронної діяльності; не сформоване чинне нормативно-правове поле у сфері кібербезпеки; відсутня Єдина загально державна системи протидії кіберзлочинності з відповідним нормативним забезпеченням[4].

Тому, Україна має продовжити активні кроки на шляху розбудови власної системи кібербезпеки та протидії кіберзлочинам. Доцільно пришвидшити підготовку та подальше прийняття Верховною Радою України Законопроекту про кібернетикну безпеку України. Також варто зазначити, що більшість розвинених

держав світу ухвалили національні стратегії з кібербезпеки та протидії кіберзлочинам, які визначають середньо – та довгострокові пріоритети та завдання державних органів у даній сфері. Україні, крім згаданого Законопроекту про кібернетичну безпеку, доречно також створити відповідний документ. Отже, швидка інформатизація держави та масштаби потенційних наслідків здійснення комплексних злочинів у кіберпросторі, обумовлюють необхідність розгляду даної проблеми на найвищому державному рівні та в найкоротші строки.

Список використаних джерел

1. Дашян М. С. Право информационных магистралей. Москва, 2007. 288 с.

2. Юрасов А. В. Основи электронной коммерции. Учебник. Москва: Горячая линия - Телеком, 2008. 480 с.

3. Glossary and Acronyms (Archived) / European Commission URL: https://europa.eu/european-union/documents-publications/language-and-terminology_en

4. Cyber Security Strategy of the United Kingdom: safety, security and resilience in cyber space.URL: https://www.gov.uk/government/publications/cyber-security-strategy-of-the-united-kingdom