УДК 004.056

Л. М. Ткачук
Р. О. Крохмаль

Становлення кібербезпеки в ЄС

Вінницький національний технічний університет

Анотація

У статті розглядається становлення кібербезпеки в ЄС і країнах-членах на законодавчому рівні з позицій системного підходу. Виявлено проблемні аспекти підвищення якості і стану кібербезпеки.

Ключові слова: інноваційні технології, кібербезпека, стратегія.

Abstract.

The article deals with the issues of establishing cybersecurity in the EU and its member-states at the legislative level as viewed from the point of a systematic approach. The authors identified problematic aspects of improving cybersecurity quality and conditions.

Key words: *innovations, cybersecurity , strategy.*

Вступ

На сьогодні існує чимало праць з питань кібербезпеки, в тому числі й питань кібербезпеки в ЄС, але статей, присвячених дослідженням цих питань з системного підходу небагато. Автори звертають увагу на роботи, де обговорюються проблеми якості безпеки інформаційно-комунікаційних систем [1; 2]. В роботах авторів А. В. Войціховського, С. В. Демедюка, І. М. Забари, О. Ю. Запорожця, В. К. Конаха, В. А. Ліпкана, Р. В. Лук'янчука, А. М. Орлеана та Є. Б. Тіхомірова вивчалися в основному питання законодавчого характеру в ЄС або в окремих країнах у конкретні часові періоди.

Розглядаючи ж дану проблему, потрібно звертати увагу на всі договори щодо питань пов'язаних з кібербезпекою ЄС, а також розглянути актуальність цих договорів згідно технологічного прогресу світу.

Результати дослідженя

У нинішню промислову та інформаційну епоху кібербезпека розглядається як головна проблема. На сьогоднішній день ЄС працює на багатьох фронтах для покращення кібер-стійкості, але потребує більшої підтримки з боку своїх держав-членів.

Через стрімкий розвиток технологічного прогресу у світі виникли проблеми кібербезпеки. У зв'язку з цим інформаційно-комунікаційні системи неодноразово розглядалися на різних міжнародних та національних рівнях.

Початком боротьби з міжнародною та національною кіберзлочинністю стала Конвенція Ради Європи про кіберзлочинність, яка відбулася у Будапешті 2001 року. Її було ратифіковали більше ніж півсотню країн, а серед країн-учасників були й країни, що не є країнами-членами Ради Європи, такі як США, Канада, Японія, Мексика, Австралія та інші.

Після цього Генеральна Асамблея ООН прийняла Резолюцію, зміст якої був пов'язаний саме з питаннями забезпечення кібербезпеки [3]. Завдяки цьому кроку у більшості країн-членів було створено національні стратегії кібербезпеки та національні план із захисту інформаційної інфраструктури.

Знаковою подією сталося ухвалення в рамках ЄС (2013 р.) Стратегії кібербезпеки, метою якої можна вважати відкритий, надійний і безпечний кіберпростір, роботу над відповідною директивою було розпочато після її оприлюднення.

Стратегія та відповідні доповнення до неї що отрималит назву: «Порядок денний» були оприлюднені навесні 2015 року. Пізніше, в липні 2016 року Європейська Комісія презентувала «Додаткові заходи по сприянню розвитку індустрії кібер-захисту».У цьому ж році була ухвалена Директива ЄС 2016/1148 щодо заходів по забезпеченню високого загального рівня безпеки мережевих та інформаційних систем у всьому Союзі [4].

Директива є значним кроком до збільшення кіберстійкості ЄС та створення спільної відповіді на кіберзагрози в ЄС [5].

Лоренцо Пупілло, старший науковий співробітник і керівник напрямку кібербезпеки в CEPSInitiative висловив таку думку: «Сучасна війна сформована зростаючими явищами міжнародних кібер-атак на державній арені. Стійкість – це ключ до такої загрози».

Згодом у вересені 2017 року Європейська комісія оприлюднила оновлену редакцію Стратегії

кібербезпеки. Даний договір був призначений для поліпшення захисту критично важливої інфраструктури Європи, а також підвищення цифрового самоствердження ЄС щодо інших регіонів світу.

Також слід мати на увазі, що незважаючи на всі вищезазначені договори, ЄС немає ні належним чином певної стабільності, ні досить ясного пояснення того, як він має подолати інституційну фрагментацію і відсутність правових повноважень в питаннях кібербезпеки [6].

В цілому ЄС має достатньо сучасне законодавство з кібербезпеки, але, на жаль, воно неспроможне захистити його від кібератак та підтримувати кібербезпеку цього об'єднання.

Так, в епоху інформаційного суспільства більшість проблем кібербезпеки викликана відставанням сучасної законодавчої бази від науково-технічного прогресу в галузі інформаційних технологій.

За декілька останніх десятиліть відбулася така потужна технологічна революція в галузі використання комп'ютерів та телекомунікацій, яка принципово призвела до зміни та збільшення апаратного парку, а також суттєвого прискорення швидкості передачі даних, охоплення світового простору інформаційними наземними і мобільними комунікаційними мережами. Все це супроводжувалося збільшенням пропускної спроможності, взаємозв'язаності та швидкодії інформаційних систем.

Висновки

Таким чином, процес становлення кіберзаконодавства в країнах-членах ЄС розпочався у 2001 році й досі набирає оберти, створюючи нове законодавство в цій галузі, але, незважаючи на існуючу сучасну низку документів щодо кібербезпеки, вона досі залишається досить вразливою, незалежно від ступеня розробки і стану законодавства.

СПИСОК ВИКОРИСТАНОЇ ЛІТЕРАТУРИ

1. Василенко М. Підвищення стану кібербезпеки інформаційно-комунікаційних систем: якість в контексті удосконалення інформаційного законодавства / М. Василенко // Юридичний вісник. – 2018. – № 3. – С. 17–24.

2. Василенко М. Якість кібербезпеки інформаційно-комунікаційних систем (ІКС) та деякі законодавчі питання щодо її підвищення / М. Василенко // Юридичний вісник. – 2018. – № 4.

3. Резолюція Генеральної Асамблеї ООН «Створення глобальної культури кібербезпеки» від 20 грудня 2002 р. № 57/239 [Електронний ресурс]. – Режим доступу : http://www.un.org/ru/ga/second/57/second_res.shtml.

4. Directive (EU) 2016/1148 of the European Parliament and of the Council of 6 July 2016 concerning measures for a high common level of security of network and information systems across the Union // Official Journal of the European Union. – 2016. – L. 194. – P. 1–30.

5. Tauwhare, R. (2016). Improving cybersecurity in the European Union: the Network and Information Security Directive. Journal of Internet Law, 19(2), 1–12.

6. The EU's Revised Cybersecurity Strategy [Електронний ресурс]. – Режим доступу : https://www.swp-berlin.org/ fileadmin/contents/products/comments/ 2017C47_bdk_etal.pdf.

Ткачук Людмила Миколаївна – доцент кафедри менеджменту та безпеки інформаційних систем, кандидат економічних наук, заступник декана з навчально-методичної роботи Факультету менеджменту та інформаційної безпеки ВНТУ, e-mail: ludatkachuk2017@gmail.com.

Крохмаль Роман Олександрович – студент групи КІТС-18б, Факультет менеджменту та інформаційної безпеки, Вінницький національний технічний університет, Вінниця, e-mail: romakrohmal23455@gmail.com.

Tkachuk Lyudmyla Mykolayivna – associate professor of Department of Management and Security of Information Systems, candidate in economics, deputy dean for educational and methodological work of the Faculty of Management and Information Security of VNTU, e-mail: ludatkachuk2017@gmail.com.

Krokhmal Roman Alexandrovich – student of CITS-18b, Faculty of Management and Information Securi- ty, Vinnytsia National Technical University, Vinnytsia, e-mail: romakrohmal23455@gmail.com.