ПЕРСПЕКТИВИ РОЗВИТКУ КІБЕРЗАХИСТУ В УКРАЇНІ

Лісова А.,
здобувач вищої освіти обліково-фінансового факультету,
Миколаївський національний аграрний університет,
м. Миколаїв, Україна
Бурковська А. В.,
канд. екон. наук, доцент кафедри фінансів,
банківської справи та страхування,
Миколаївський національний аграрний університет,
м. Миколаїв, Україна

Досліджено розвиток кібернетичного простору та перспективи розвитку кіберзахисту в Україні.

Ключові слова: *кіберзахист, кібернетичний простір, інформаційні технології.*

У сучасному світі інформаційних технологій дуже стрімко розвивається кібернетичний простір, який являє собою найпотужніший механізм у економічній і соціальній сфері України. Комп'ютеризація формує принципово нове інформаційне суспільство і має значний невичерпний характер. Результатом даного процесу є стрімкий рух кібернетичних загроз, які в свою чергу також не відстають від сучасних тенденцій.

За таких умов необхідна міцна протидія загрозам у національній безпеці. Така протидія вже набула високого значення у світі, але в кожній країні свій рівень ризику і своя тенденція до вирішення даного питання. Для посилення безпеки провідні країни мають перспективу до об'єднання зусиль та формування єдиного механізму. На створення та реалізацію підходів щодо кіберзахисту у складові національної безпеки країн впливає Організація Північноатлантичного договору (НАТО).

Нова Стратегічна концепція оборони та безпеки країн-членів НАТО, що була прийнята главами держав та урядів під час Лісабонського саміту країн-членів НАТО 19 листопада 2010 року, фактично прирівняла загрози кібератакдо

військових загроз, що, у свою чергу, передбачає можливість відповіді на масовані кібератаки із застосуванням національних збройних сил[1]. Кібератаки стали одним з найбільш небезпечних викликів безпеці країн-членів Альянсу, а забезпечення кібернетичної безпеки було зазначено в якості другого за значимістю пріоритету НАТО[1]. Доктрина НАТО з кібербезпеки, у свою чергу, відзначає співробітництво з країнами-партнерами у сфері розбудови системизабезпечення кібернетичної безпеки Альянсу в якості ключового механізму заходів НАТО із забезпечення кіберзахисту[1].

Національна система України потребує розбудови в кібербезпеці. Найвагомішим доказом цього є те, що кібератаки застосовуються для фінансових установ та державних органів, які практично є основною складовою всієї держави – її оборони, національної безпеки та функціонуванням цілісної системи. Важливу частину роботи з убезпечення громадян від найбільш розповсюджених кіберзлочинів здійснює Національна поліція України (НП). У його структурі створеноспеціальне Управління боротьби з кіберзлочинністю, на яке покладено низку завдань. Зокрема, до основних завдань Управління відноситься організаційне та практичне забезпечення реалізації державної політики щодо попередження та протидії злочинам і правопорушенням, що вчиняються з використанням інформаційних технологій та телекомунікаційних мереж (у сфері інформаційно-телекомунікаційних технологій, у сфері електронних платежів і господарської діяльності, зокрема, порушення прав інтелектуальної власності та заняттягральним бізнесом, злочини проти інформаційної безпеки, у тому числі незаконні дії зі спеціальними технічними засобами негласного отримання інформації), а також протидії легалізації доходов, отриманих від таких злочинів і правопорушень [2].

Державна служба спеціального зв’язку та захисту інформації відповідно до своїх завдань безпосередньо включена до забезпечення кібербезпеки держави. Зокрема, серед її профільних завдань визначено:

– забезпечення формування і реалізації державної політики у сферах захисту державних інформаційних, телекомунікаційних та інформаційно-

телекомунікаційних систем криптографічного та технічного захисту інформації, використання і захисту державних електронних інформаційних ресурсів, телекомунікацій, користування радіочастотним ресурсом України; участь у формуванні і реалізації державної політики у сфері електронного документообігу органів державної влади та органів місцевого самоврядування. Стратегічні аспекти кібербезпеки України розробленні та впровадженні електронного цифрового підпису в органах державної влади та органах місцевого самоврядування;

– забезпечення функціонування, безпеки та розвитку державної системи урядового зв'язку і Національної системи конфіденційного зв'язку;

– здійснення державного контролю за станом криптографічного та технічного захисту інформації, яка є власністю держави, або інформації з обмеженим доступом, вимога щодо захисту якої встановлена законом, протидії технічним розвідкам, а також за додержанням технічних вимог керівних документів у сфері надання послуг електронного цифрового підпису;

– розроблення та здійснення заходів щодо розвитку телекомунікаційних мереж, поліпшення їх якості, забезпечення доступності і сталого функціонування [3].

Отже, кіберзахист в Україні лише починає посягати досвід провідних країн. Неможливість повністю захистити національну економіку та інші сфери призводить до неймовірної потужності проблем. Тому витягувати на новий рівень кібербезпеку займає одну із перших позицій у цільовому спрямуванні.

ЛІТЕРАТУРА:

1. Стратегічна концепція оборони та безпеки членів Організації Північноатлантичного договору від 19.11.2010 р. // Офіційний сайт Організації Північноатлантичного договору / Організація Північноатлантичного договору. URL: https://www.nato.int/cps/uk/natohq/official_texts_68580.htm.

2. Управління боротьби з кіберзлочинністю // Міністерство внутрішніх справ України URL: http://mvs.gov.ua/mvs/control/main/uk/publish/article/544754.

3. Основні завдання Державної служби спеціального зв'язку та захисту інформації України // Державна служба спеціального зв'язку та захисту інформації України URL: http://www.dstszi.gov.ua/dstszi/control/uk/publish/article?art_id=89831&.

Annotation: *The development of cyber space and prospects of development of cyber defense in Ukraine are investigated.*

Key words: *cyber defense, cyberspace, information technology.*