Яременко О. І.,
кандидат наук з державного управління,
доцент, декан факультету права,
публічного управління і менеджменту
Цюпра Т. В.,
здобувачка вищої освіти СВО Магістр
факультету права, публічного управління і менеджменту
Вінницького державного педагогічного університету
імені Михайла Коцюбинського

УПРАВЛІННЯ КІБЕРНЕТИЧНОЮ БЕЗПЕКОЮ ОРГАНІЗАЦІЇ: СТАНДАРТИ ЄВРОПЕЙСЬКОГО СОЮЗУ

В сучасному світі інформація є одним із найбільш вартісних активів будь-якої організації. Суб'єкти господарювання, державні органи, органи місцевого самоврядування і громадські організації володіють величезними за обсягами та різними за видами, цінністю і правовим режимом інформаційними ресурсами, які мають, як правило, цифрову форму, що актуалізує проблему управління кібернетичною безпекою організації.

Метою даної статті є аналіз європейських стандартів управління кібернетичною безпекою організації.

Європейський Союз має тривалий досвід формування політики управління кібербезпекою. Так, ще у 2004 році було засновано Агентство Європейського Союзу з кібербезпеки (ENISA). Пункт 15 Регламенту Європейського Парламенту та Ради від 10 березня 2004 року № 460/2004 «Про створення Європейського агентства з мережевої та інформаційної безпеки» передбачає, що агенція повинна сприяти високому рівню мережевої та інформаційної безпеки в Співтоваристві та розвивати її на користь громадян, підприємств та організацій державного сектору в Європейському Союзі, таким чином, сприяючи безперебійному функціонуванню внутрішнього ринку [1].

З метою ефективного захисту прав громадян в мережі Інтернеті у 2016 році було прийнято правовий акт Союзу у сфері кібербезпеки у формі Директиви 2016/1148 Європейського Парламенту та Ради щодо заходів забезпечення високого спільного рівня безпеки мережевих та інформаційних систем. Директива встановила вимоги щодо національних стандартів у сфері кібербезпеки, окреслила механізми посилення стратегічної та оперативної співпраці між державами-членами та запровадила ряд зобов'язань для організацій щодо вжиття заходів безпеки інформаційних систем та обов'язок повідомляти про кіберінциденти в секторах, які є життєво важливими для економіки та суспільства [2].

Одним із напрямків діяльності Європейського Союзу є регулювання сертифікації у сфері кібербезпеки, яка розглядається як ключовий фактор підвищенні довіри та безпеки до цифрових продуктів, послуг і процесів. В Законі Європейського Союзу про кібербезпеку зазначається, що цифровий

єдиний ринок, і, зокрема, економіка даних та Інтернет речей, можуть процвітати лише за умови впевненості громадськості в тому, що такі продукти, послуги та процеси забезпечують певний рівень кібербезпеки. Цей закон визначив, що діяльність у сфері сертифікації кібербезпеки покладається на ENISA, яка була визнана як ключова організація для створення системи сертифікації у співпраці з державними службами, галузевими організаціями та організаціями стандартизації. Акт ЄС про кібербезпеку надає агенції постійний мандат і надає їй більше ресурсів і нових завдань [3].

Важливе значення для формування кібербезпеки організацій має діяльність Міжнародної організації зі стандартизації (ISO) та Міжнародної електротехнічної комісії (IEC), які утворюють спеціалізовану систему всесвітньої стандартизації. Зокрема, ними створено ISO/IEC 27002 - міжнародний стандарт, який містить вказівки для організацій, які прагнуть створити, запровадити та вдосконалити систему управління інформаційною безпекою (ISMS), орієнтовану на кібербезпеку. ISO/IEC 27002 пропонує найкращі практики та цілі контролю, пов'язані з ключовими аспектами кібербезпеки, включаючи контроль доступу, криптографію, безпеку людських ресурсів та реагування на інциденти. Стандарт служить практичним планом для організацій, які прагнуть ефективно захистити свої інформаційні активи від кіберзагроз [5].

Таким чином, Європейський Союз вживає правових, організаційних і технічних заходів щодо забезпечення кібербезпеки організацій. Україні необхідно використовувати цей досвід, зокрема, в частині сертифікації інформаційно – комунікаційних продуктів, послуг і процесів, що може бути предметом подальших досліджень в цьому напрямку.

Список використаних джерел:

1. Regulation (EC) No 460/2004 of the European Parliament and of the Council of 10 March 2004 establishing the European Network and Information Security Agency. *Official Journal of the European Union L 077 , 13.03.2004.*

2. 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 194, 19.7. 2016.*

3. Regulation (EU) 2019/881 of the European Parliament and of the Council of 17 April 2019 on ENISA (the European Union Agency for Cybersecurity) and on information and communications technology cybersecurity certification and repealing Regulation (EU) No 526/2013 (Cybersecurity Act). *Official Journal of the European Union L 7.6.2019*

4. Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC *Official Journal of the European Union.*

5. Information security, cybersecurity and privacy protection. Information security controls international standard ISO/IEC 27002 / Third edition 2022-02.