УДК 004.056

Л. О. Майданевич
Г. В. Шелепало

ТЕХНІЧНИЙ ЗАХИСТ ІНФОРМАЦІЇ: ОСОБЛИВОСТІ ПРОЦЕСУ

Вінницький національний технічний університет

Анотація

В доповіді розглянуто особливості процесу технічного захисту інформації. З'ясовано, що цей процес має: відповідати державній політиці у сфері ТЗІ (з пріоритетом національних інтересів); бути скоординованим та розмежованим згідно компетенцій суб'єктів системи технічного захисту інформації; стати основою для розвитку сучасних інформаційних технологій, державних інформаційних ресурсів, технологічного переозброєння промисловості України. Результати дослідження можуть бути використанні для подальшого теоретичного та практичного процесу технічного захисту інформації, насамперед, застосовуючи трансдисциплінарний та міждисциплінарний підходи.

Ключові слова: технічний захист інформації, класифікація джерел загроз інформації, вразливості інформаційної безпеки.

Abstract

The report examines the features of the process of technical protection of information. It is established that this process should: correspond to the state policy in the field of technical protection of information (TPI, with the priority of national interests); be coordinated and delimited in accordance with the competencies of the subjects of the system of technical protection of information; become the basis for the development of modern information technologies, state information resources, technological re-equipment of the industry of Ukraine. The results of the study can be used for further theoretical and practical process of technical protection of information, primarily using transdisciplinary and interdisciplinary approaches.

Keywords: technical protection of information, classification of sources of information threat, vulnerabilities of information security.

Вступ

В 1997 році в Україні була схвалена Концепція технічного захисту інформації. В цій Концепції передбачалося, що «технічний захист інформації – це діяльність, спрямована на забезпечення інженерно-технічними заходами порядку доступу, цілісності та доступності (унеможливлення блокування) інформації з обмеженим доступом, а також цілісності та доступності відкритої інформації, важливої для особи, суспільства і держави» [1]. Надалі, в Україні було прийнято ряд нормативно-правових актів та проведено організаційно-технічні заходи, які були спрямовані щодо покращення технічного захисту інформації.

Результати дослідження

Згідно Указу Президента від 27 вересня 1999 року N 1229/99 було затверджено Положення про технічний захист інформації в Україні. В цьому Положенні, найперше, було надано офіційне визначення засадничим для технічного захисту інформації (ТЗІ) термінам, а саме: «конфіденційність – це властивість інформації бути захищеною від несанкціонованого ознайомлення; цілісність – це властивість інформації бути захищеною від несанкціонованого спотворення, руйнування або знищення; доступність – це властивість інформації бути захищеною від несанкціонованого блокування» [2].

Особливістю забезпечення конфіденційності, цілісності та доступності інформації є використання відповідних методів, насамперед, комплексних методів з обов'язковим використанням трансдисциплінарного та міждисциплінарного підходів у протистоянні загрозам безпеці інформації. Ці три принципи (тріада) є основою міжнародних стандартів (ISO, NIST) та використовуються при побудові ефективних систем технічного захисту інформації від відомих загроз. Відомі загрози інформації можна означити за джерелами загроз інформації.

Таблиця 1 – Класифікація джерел загроз інформації [3]

Антропогенні джерела	*Техногенні джерела*	*Стихійні джерела*
Зовнішні антропогенні джерела: - кримінальні структури; - потенційні злочинці та хакери; - недобросовісні партнери; - представники організацій, що взаємодіють з питань технічного забезпечення (енерго-, водо-, тепло-постачання тощо); - представники наглядових організацій та аварійних служб; - представники силових структур; - співробітники спецслужб (державних, закордонних спецслужб) та/або особи які діють за їх завданням	*Зовнішні техногенні джерела:* - засоби зв'язку; - мережа інженерних комунікацій (електро-, водо-, газо – постачання, каналізація тощо); - транспорт тощо	*Зовнішні стихійні джерела:* - пожежі; - землетруси; - повені; - урагани; - магнітні бурі; - радіоактивне випромінювання; - різноманітні непередбачені обставини та форс-мажорні обставини
Внутрішні антропогенні джерела: - основний персонал (користувачі, розробники, програмісти); - представники служби захисту інформації (адміністратори); - технічний персонал, який обслуговує будівлі та приміщення (електрики, сантехніки, прибиральники тощо), в яких розташовані компоненти ІКС	*Внутрішні техногенні джерела:* - неякісні технічні засоби оброблення інформації; - неякісні програмні засоби оброблення інформації; - допоміжні засоби (охоронна-, пожежна- сигналізація, телефон тощо); - інші технічні засоби, що застосовуються в організації	

Водночас, вищевказані джерела загроз інформації (наприклад, на об'єкті критичної інфраструктури) можуть стати такими лише через певні вразливості, що призводять до порушення безпеки інформації. Тобто, вразливості обумовлюються існуючими недоліками на об'єкті, а джерела загроз їх використовують як основу для порушення безпеки інформації.

Таблиця 2 – Вразливості інформаційної безпеки [3]

Групи	*Особливі примітки*
Об'єктивні вразливості	- випромінювання технічних засобів (електромагнітні, електричні, звукові); - закладки (апаратні, програмні); - такі, що визначаються особливостями елементів (елементи здатні до електроакустичного перетворення; елементи, що піддаються впливу електромагнітного поля); -такі, що визначаються особливостями об'єкта захисту (місцезнаходження об'єкта, організацією каналів обміну інформацією)
Суб'єктивні вразливості	- помилки/халатність (при підготовці та використанні програмного забезпечення; при експлуатації технічних засобів; некомпетентні та/або ненавмисні дії); - порушення (режиму захисту та оборони; режиму експлуатації технічних засобів та програмного забезпечення; використання інформації); - психогенні (психологічні, психічні, фізіологічні)
Випадкові вразливості	- збої та відмови (відмови у та несправності технічних засобів; старіння та розмагнічування носіїв інформації; збої програмного забезпечення; збої електроживлення)

Висновки

Специфіка процесу технічного захисту інформації, найперше, обумовлена відомими та потенційними вразливостями інформаційної безпеки. Цей процес також має: відповідати державній політиці у сфері ТЗІ (з пріоритетом національних інтересів); бути скоординованим та розмежованим згідно компетенцій суб'єктів системи технічного захисту інформації; стати основою для розвитку сучасних інформаційних технологій, державних інформаційних ресурсів, технологічного переозброєння промисловості України. Результати дослідження можуть бути використанні для подальшого теоретичного та практичного процесу технічного захисту інформації, насамперед, застосовуючи трансдисциплінарний та міждисциплінарний підходи.

СПИСОК ВИКОРИСТАНОЇ ЛІТЕРАТУРИ

1. Про затвердження Концепції технічного захисту інформації в Україні. *Постанова Кабінету Міністрів України від 08.10.1997 № 1126*. URL : https://zakon.rada.gov.ua/go/1126-97-%D0%BF (дата звернення: 14.05.2025)

2. Про Положення про технічний захист інформації в Україні. *Указ Президента України від 27.09.1999 № 1229/99*. URL : https://zakon.rada.gov.ua/go/1229/99 (дата звернення: 14.05.2025)
3. Технічний захист інформації: теоретичні основи та організаційно-технічне забезпечення. Навч.посіб. / В.М.Богуш, В.Д.Бровко, О.С.Кобус, В.Д.Козюра. Київ : Видавництво Ліра-К, 2023. 484 с.

Майданевич Леонід Олександрович – канд. філос. наук, старший викладач кафедри захисту інформації факультету інформаційних технологій та комп'ютерної інженерії Вінницького національного технічного університету, адвокат (Рада адвокатів Вінницької області), м. Вінниця, email: lmaidanevych@gmail.com
Шелепало Галина Василівна – канд. фіз-мат. наук, доцент кафедри захисту інформації факультету інформаційних технологій та комп'ютерної інженерії Вінницького національного технічного університету, адвокат (Рада адвокатів Вінницької області), м. Вінниця, email: kraynichuk@ukr.net

Maidanevych Leonid – Candidate of Philosophical Sciences, Senior Lecturer, Department of Information Security, Faculty of Information Technology and Computer Engineering, Vinnytsia National Technical University, Lawyer, Vinnytsia Bar Council, Vinnytsia, e-mail: lmaidanevych@gmail.com
Shelepalo Halyna – PhD (Eng), Associated Professor, Department of Information Security, Faculty of Information Technology and Computer Engineering, Vinnytsia National Technical University, Vinnytsia, email: kraynichuk@ukr.net.