

зі строю деякі компоненти комп'ютера, а вони в свою чергу можуть коштувати декілька сотень і навіть тисячі доларів США.

Тому зараз на інформаційній безпеці зосереджено багато зусиль та уваги, так як в нашій країні ненадійно ведеться інформаційна політика. Інформаційна безпека – це захищеність, збереження інформаційних ресурсів від випадкових, зловмисних або надзвичайних внутрішніх / зовнішніх впливів і збоїв. Тому загальна задача Інформаційної безпеки полягає в мінімізації збитку, в прогнозі і безперервному запобіганні таких впливів.

Задля підвищення власної безпеки потрібно користуватись антивірусними програмами, бажано платними, адже рівень захисту в них на рівень вищий ніж у безкоштовних версіях. Завжди використовувати брандмауер, він на базовому рівні захистить ваш ПК від небажаних вірусних програм, також користуватися ліцензійним програмним забезпеченням та слідкувати за оновленнями [4].

Цих рекомендацій буде достатньо для звичайних користувачів, але якщо у вас підприємство, то не слід економити на інформаційній безпеці, краще звернутись до професіоналів, щоб потім не платити двічі [5].

«Хто володіє інформацією, той володіє світом», – сказав колись Уїнстон Черчилль.

#### **Список використаних джерел:**

1. [http://24tv.ua/sbu\\_objasnila\\_kak\\_preodolet\\_opasnyj\\_virus\\_petyaa\\_n835231](http://24tv.ua/sbu_objasnila_kak_preodolet_opasnyj_virus_petyaa_n835231)
2. <https://tsn.ua/ukrayina/ukrayina-zaznala-ataki-vid-virusa-zdirnika-yak-pracyuye-petya-a-ta-yak-uberegtisya-vid-kiberataki-952450.html>
3. <https://twitter.com/ServiceSsu/status/898514969184133121>
4. <https://www.volynnews.com/news/society/virus-zdyrnyk-PetyaA-atakuvav-kompiutery-cherez-MEdoc/>
5. <http://www.afa.biz.ua/2009-04-17-10-56-52/39-2009-04-17-10-55-51/241-2012-02-06-13-43-08>

**Ігнатенко О.І., Грабовський А.Ю.**

*студенти,*

*Навчально-науковий інститут інформаційної безпеки*

*Національної академії Служби безпеки України*

## **МІЖНАРОДНІ СТАНДАРТИ ЗАХИСТУ ІНФОРМАЦІЇ З ОБМЕЖЕНИМ ДОСТУПОМ**

Розвиток інформаційно-комунікаційних технологій (далі – ІКТ) став каталізатором численних соціальних, культурних, економічних і політичних процесів як на національному рівні, так і в глобальному масштабі. На зміну індустріальній епосі прийшла постіндустріальна – інформаційна епоха, в якій головну роль відіграють нові технології і інформація. І саме тому виникло глобальне інформаційне суспільство, в якому прискорилися всі процеси обміну і отримання інформації [1, с. 72]. Сьогодні рівень розвитку сектора ІКТ

визначає роль держави в світовій економіці і її політичну вагу на міжнародній арені. Нинішній етап розвитку інформаційних технологій характеризується можливістю масового інформаційного впливу на індивідуальну і суспільну свідомість аж до проведення великомасштабних інформаційних війн, в результаті чого неминучою протиположністю принципу свободи інформації стає принцип інформаційної безпеки.

Цей принцип обумовлений глобальною інформаційною революцією, стрімким розвитком і повсюдним впровадженням новітніх інформаційних технологій і глобальних засобів телекомунікацій. Проникаючи в усі сфери життєдіяльності держав, інформаційна революція розширює можливості розвитку міжнародного співробітництва, формує планетарний інформаційний простір, в якому інформація набуває властивостей найціннішого елемента національного надбання, його стратегічного ресурсу, виникає необхідність в розподілі та стандартизації, набутті передових практик з захисту інформації.

Інформація з обмеженим доступом – це відомості оприлюднення та доступ до яких правомірно обмежений розпорядником такої інформації, а правовий статус передбачений законодавством.

Варто зазначити, що відповідно до Закону України «Про інформацію», інформація з обмеженим доступом за своїм правовим режимом поділяється на конфіденційну, таємну та службову інформацію [9]. До таємної інформації, в свою чергу, відноситься державна, комерційна, службова, професійна, військова, банківська, адвокатська, лікарська таємниці, а також таємниця страхування, усиновлення, голосування, нотаріальних дій, листування, телефонних розмов, телеграфної та іншої кореспонденції [7, с. 23-25].

На сьогодні світовою тенденцією є уніфікація захисту прав і свобод людини, їх єдино образне тлумачення і реалізація, на що спрямована велика кількість універсальних міжнародних правових актів, у тому числі у сфері захисту інформації з обмеженим доступом, серед яких:

- Загальна декларація прав людини [4];
- Міжнародний пакт про громадянські та політичні права [9];
- Конвенція про міжнародне право спростування [7] та ін.

Загальні принципи інформаційної безпеки містяться у підсумкових документах ВСПС – Женевській Декларації принципів 2003 року [3] і Туніській Програмі для інформаційного суспільства 2005 року [10]. Женевський План дій 2003 року передбачає необхідність уживання належних заходів для боротьби з незаконним і шкідливим контентом у засобах масової інформації, не зазіхаючи при цьому на свободу слова. Він закликає держави і їх уряди дотримуватися етичних норм при використанні інформаційних і комунікаційних технологій, які базуються на засадах: 1) сприяння загальному благу, справедливості, дотриманні миру, свободи, рівності, солідарності, терпимості, колективної відповідальності; 2) підтримки гідності і цінності людської особистості; поваги прав людини, зокрема права на свободу думки, совісті та релігії; 3) недоторканності приватного життя і особових даних. Підсумкові документи Женевського етапу ВСПС закликають усіх дієвих осіб інформаційного суспільства, особливо державні органи, до вживання відповідних дій і запобіжних заходів, визначених

законодавством, проти зловживань при використанні інформаційних комп'ютерних технологій (далі ІКТ), таких як: незаконні та інші дії, мотивовані расизмом; расова дискримінація, ксенофобія і пов'язана з ними нетерпимість; ненависть, насильство; усі форми жорстокого поводження з дітьми, включаючи педофілію і дитячу порнографію; торгівля людьми і їх експлуатація [2, с. 59]. Туніська Програма для інформаційного суспільства 2005 року закликає до відповідального використання і трактування інформації засобами масової інформації відповідно до найвищих етичних та професійних стандартів. Саме на заклик Туніського саміту Генеральна Асамблея ООН у березні 2006 року своєю резолюцією проголосила 17 травня Всесвітнім днем інформаційного суспільства.

Слід брати до уваги, що на сьогоднішній день зростання комп'ютеризації при обробленні персональних даних (наприклад, у банківській кредитній та страховій сферах, при працевлаштуванні, адресному маркетингу, у статистиці) змусив замислитись над багатьма практичними питаннями. Розвиток нових інформаційних технологій, електронної торгівлі та вільний обмін інформацією також породжує побоювання відносно дотримання вимог безпеки та поваги основних прав та свобод. Для захисту права на недоторканність приватного життя та запобігання незаконного доступу до інформації з обмеженим доступом Радою Європи розроблена чітка правова база, яка встановлює стандарти у галузі захисту інформації.

В основному міжнародно-правовому документі Ради Європи у галузі захисту даних – Конвенції про захист фізичних осіб при автоматичному обробленні персональних даних (СЕД №108) прописані загальні принципи захисту інформації [5]. Прийняття даної конвенції Ради Європи було продиктовано необхідністю дотримання балансу між правом на недоторканність приватного життя й правом на інформацію та забезпечило рівний ступінь захисту цих прав у різних державах. На сьогодні це єдиний інструмент, що має обов'язкову правову силу та універсальну сферу застосування, який відкритий для всіх держав, у тому числі, які не є членами Ради Європи. Окрім даної Конвенції Радою Європи також прийнята ціла низка рекомендацій з питань захисту даних, які стосуються різних аспектів оброблення інформації. Держави-учасники повинні забезпечити включення у своє законодавство основних принципів Конвенції відносно персональних даних всіх фізичних осіб на своїй території.

В умовах зростання потоків даних особистого характеру між різними державами був прийнятий Додатковий протокол до конвенції, що стосується спостережних органів та транскордонної передачі даних (СЕД №181). Його мета – забезпечити підчас такого обміну ефективний захист основних прав та свобод, зокрема, права на недоторканність приватного життя. Тому Рада Європи адаптує загальні принципи, викладені в Конвенції, до конкретних вимог різних режимів обробки даних. Ці принципи та вказівки у галузі захисту даних закріплені у рекомендаціях, що не мають юридично обов'язкового характеру, але можуть бути враховані в нормативно-правових актах, якщо країна інтегрується в європейську спільноту. Згідно Додаткового протоколу до

конвенції, для забезпечення виконання законодавства держави також повинні заснувати незалежний орган по захисту даних або ряд таких органів.

В свою чергу, вважаємо, що основні принципи забезпечення захисту інформації з обмеженим доступом повинні бути запроваджені й у вітчизняному законодавстві та відображені в Законі України «Про інформацію». Велика кількість правових питань, що потребують врегулювання у сфері обігу інформації з обмеженим доступом, створюють передумови для розробки та прийняття Закону України «Про інформацію з обмеженим доступом» чи відповідного розділу в Кодексі України про інформацію з обмеженим доступом.

Отже, закріплення на міжнародному рівні норм, що визначають необхідність правового захисту інформації з обмеженим доступом, відображають сталу тенденцію в розвитку інформаційних відносин, що виникають у процесі обігу такої інформації, зокрема збільшення обсягів використання персональних даних громадян.

### Список використаних джерел:

1. Бутнік-Сіверський, О. Б. Інноватика та інтелектуальна економіка (теоретико-методологічний аспект) / О. Б. Бутнік-Сіверський // Теорія і практика інтелектуальної власності. – 2007. – № 6. – С. 68–81.
2. Войскунский А. Е. Зависимость от Интернета: актуальная проблема / А. Е. Войскунский // Социальные и психологические последствия применения информационных технологий. – 2014. – № 1 – С. 58–68.
3. Женевська Декларація принципів, Женева, 12 грудня 2003 р. [Електронний ресурс]. – Режим доступу: <http://nkrzi.gov.ua/index.php>
4. Загальна декларація прав людини від 10.12.1948 2003 р. [Електронний ресурс]. – Режим доступу: [http://zakon2.rada.gov.ua/laws/show/995\\_015](http://zakon2.rada.gov.ua/laws/show/995_015)
5. Конвенція про захист осіб у зв'язку з автоматизованою обробкою персональних даних № 108 від 28 січ. 1981 р. [Електронний ресурс]. – Режим доступу : [http://zakon1.rada.gov.ua/laws/show/994\\_326](http://zakon1.rada.gov.ua/laws/show/994_326)
6. Конвенція про міжнародне право спростування від 16.12.1952 2003 р. [Електронний ресурс]. – Режим доступу: [http://zakon2.rada.gov.ua/laws/show/995\\_319](http://zakon2.rada.gov.ua/laws/show/995_319)
7. Марущак А.І. Правові основи захисту інформації з обмеженим доступом : [курс лекцій]. – К. : КНТ, 2007. – 208 с.
8. Міжнародний пакт про громадянські і політичні права від 16.12.1966 2003 [Електронний ресурс]. – Режим доступу: [http://zakon2.rada.gov.ua/laws/show/995\\_043](http://zakon2.rada.gov.ua/laws/show/995_043)
9. Про інформацію: Закон України від 02.10.1992 № 2657-ХІІ [Електронний ресурс]. – Режим доступу: <http://zakon3.rada.gov.ua/laws/show/2657-12>.
10. Туніська програма для інформаційного суспільства, 18 листопада 2005 [Електронний ресурс]. – Режим доступу: <http://nkrzi.gov.ua/index.php>