ДЄС). Високий представник представляє Союз у питаннях, пов'язаних із СЗППБ; веде діалог з третіми країнами і міжнародними організаціями; висловлює позицію Союзу у міжнародних організаціях і на міжнародних форумах. При виконанні наданих йому повноважень він спирається на Європейську службу зовнішньополітичної діяльності (ст. 27 ДЄС). Він також організовує координацію дій держав-членів у міжнародних організаціях і на міжнародних конференціях; отримує інформацію від Д.Ч. про діяльність міжнародних установ; консультується з Європейським парламентом з питань СЗППБ і СПБО, а також інформує його про розвиток цих напрямів діяльності Союзу (ст. 34 ДЄС).

Література

1. Договір про Європейський Союз [Електронний ресурс]. — Режим доступу: http://zakon0.rada.gov.ua
2. Гердеґен М. Європейське право / М. Гердеґен; пер. з нім. – К.: «К.І.С.», 2008. – 528 с.
3. Договір про функціонування Європейського Союзу [Електронний ресурс]. — Режим доступу: http://zakon0.rada.gov.ua
4. Право Європейського Союзу: підручник / за ред. В.І. Муравйова. – К.: Юрінком Інтер, 2015. – 704 с.

УДК 342.9+341.123(043.2)

Канча А. С., студентка,
Навчально-науковий Гуманітарний інститут,
Національний авіаційний університет, м. Київ
Науковий керівник: Юринець Ю.Л., к.ю.н., доцент

ЗАХИСТ ІНФОРМАЦІЇ В ІНФОРМАЦІЙНИХ СИСТЕМАХ

В умовах стрімкого розвитку інформатизації суспільства найбільш актуальним є захист інформації, поданої в електронній формі, саме цей вид, з огляду на нематеріальний характер, високу здатність до трансформації й передачі є найбільш вразливим до протиправних дій. Інформація в електронній формі обробляється, передається та розповсюджується за допомогою інформаційно-телекомунікаційних систем, будучи їх основним наповненням. В Україні останнім часом створено достатньо широку нормативно-правову базу для проведення діяльності із захисту цього виду інформації. Причому можна виділити два аспекти захисту інформації в інформаційно-телекомунікаційних системах: 1) встановлення стандартів і вимог щодо характеристик інформаційних систем, які мають забезпечувати дієвість цієї системи; 2) безпосереднє правове регулювання діяльності із захисту інформації.

Наприклад, Закон України «Про телекомунікації» (ст. 1) виділяє дві

характеристики безпеки інформаційних систем і мереж: 1) інформаційна безпека телекомунікаційних мереж; 2) сталість телекомунікаційної мережі. Стаття 9 Закону України «Про телекомунікації» визначено обов'язки операторів і провайдерів телекомунікацій щодо забезпечення відповідних характеристик і властивостей засобів телекомунікацій [2].

Правовою основою діяльності із захисту інформації є Закон України «Про захист інформації в інформаційно-телекомунікаційних системах». Відповідно до ст. 1 цього Закону, захист інформації в системі – це діяльність, спрямована на запобігання несанкціонованим діям щодо інформації в системі. Сама ж автоматизована система є такою, що виконує автоматизоване оброблення даних і в складі якої є технічні засоби їх оброблення (засоби обчислювальної техніки і зв'язку), а також методи і процедури, програмне забезпечення [1].

Закон визначає п'ять основних видів несанкціонованих дій з інформацією:

1) блокування інформації в системі – дії, внаслідок яких унеможливлюється доступ до інформації в системі; 2) виток інформації – результат дій, внаслідок яких інформація в системі стає відомою або доступною фізичним та/або юридичним особам, що не мають права доступу до неї; 3) знищення інформації в системі – дії, внаслідок яких інформація в системі зникає; 4) порушення цілісності інформації в системі – несанкціоновані дії щодо інформації в системі, внаслідок яких змінюється її зміст.

Важливим аспектом інформаційної безпеки є захист інформації яка передається, зберігається та обробляється за допомогою комунікаційних систем різних типів. Щодо цього в Україні вже створено низку нормативно-правових актів.

Об'єктами захисту від неправомірних зазіхань є: інформація, що обробляється в автоматизованій системі; права власників цієї інформації та власників автоматизованої системи; права користувача [4].

Захист інформації полягає у застосуванні сукупності організаційно-технічних заходів і правових норм для запобігання заподіянню шкоди інтересам власника інформації чи автоматизованої системи та особам, які користуються інформацією.

Закон України «Про захист інформації в автоматизованих системах» визначає: відносини між суб'єктами в процесі оброблення інформації в автоматизованих системах, загальні вимоги до захисту інформації в АС і порядок організації цього захисту, відповідальність за порушення норм цього закону та засади міжнародної співпраці України у сфері автоматизованих систем [3].

Конкретний зміст вимог до захисту інформації залежить насамперед від права власності на конкретну інформації, що обробляється за допомогою автоматизованої системи. Так, за ст. 11 Закону України «Про

захист інформації в автоматизованих системах», вимоги і правила захисту інформації, яка є власністю держави, або інформації, захист якої гарантується державою, визначаються відповідними нормативно-правовими актами. Ці вимоги є обов'язковими для власників автоматизованих систем, де така інформація обробляється, а для інших суб'єктів права власності на інформацію такі вимоги мають лише рекомендаційний характер.

Політика із захисту інформації в автоматизованих системах визначається Верховною Радою України, а державне управління в цій сфері здійснює Кабінет Міністрів України. Державне управління у сфері захисту інформації в автоматизованих системах передбачає: проведення єдиної технічної політики захисту інформації; розроблення концепції, вимог, нормативно-технічних документів і науково-методичних рекомендацій захисту інформації в автоматизованих системах; затвердження порядку організації, функціонування та контролю за виконанням заходів захисти оброблюваної в автоматизованій системі інформації, яка є власністю держави, а також рекомендацій щодо захисту інформації - власності юридичних та фізичних осіб; створення відповідних структур для захисту інформації в автоматизованих системах; здійснення контролю захищеності оброблюваної в автоматизованих системах інформації, яка є власністю держави тощо [3].

Нормами законодавства встановлено комплексний характер захисту інформації. Зокрема, захист державних інформаційних ресурсів в автоматизованих системах, що належать до інформаційно-телекомунікаційних систем, здійснюється через запровадження комплексної системи захисту інформації (КСЗІ). Основними в комплексній системі захисту інформації є технічний та криптографічний захист, а також комплекс заходів організаційного характеру, який передбачає встановлення відповідних режимів діяльності об'єктів інформаційних систем, контроль за дотриманням правил і норм здійснення захисту інформації, контроль за діяльністю суб'єктів захисту інформації тощо.

Література

1. Про захист інформації в інформаційно-телекомунікаційних системах: Закон України від 05.07.1994 р. № 80/94-ВР // Відомості Верховної Ради України. – 1994. – № 31. – Ст. 286.

2. Про телекомунікації: Закон України від 18.11.2003 р. № 1280-IV // Відомості Верховної Ради України. – 2004. – № 12. – Ст. 155.

3. Василюк В.Я. Інформаційна безпека держави: курс лекцій / В.Я. Василюк, С.О. Климчик. – К.: Скіф, 2008. – 136 с.

4. Марущак А.І. Інформаційне право: навч. посіб. / А.І. Марущак. – К.: КНТ, 2007. – 532 с.