2. Цькування // Вікіпедія : віл. енцикл. URL: https://uk.wikipedia.org/ wiki/ Цькування (дата звернення: 28.10.2018).

3. Найдьонова Л. А. Кібер-булінг або агресія в інтернеті: способи розпізнання і захист дитини // Методичні рекомендації / Серія: На допомогу вчителю. Вип. 4. К., 2011. 34 с.

4. Кібермоббінг // Вікіпедія : віл. енцикл. URL: https://uk.wikipedia.org/ wiki/Кібермоббінг (дата звернення: 28.10.2018).

5. Жительницу Сочи посадили за доведение до суицида через «Одноклассники». URL: http://lulzne.ws/irl/view/645/ (дата звернення: 28.10.2018).

6. За «Интернет-троллю в США может грозить до 25 лет лишения свободы» // Free Torents URL: http://free-torrents.org/forum/viewtopic.php?t= 159133 (дата звернення: 28.10.2018).

7. 19-летнего серба посадили за угрозы президенту в Facebook // Newsland. 05.04.2012 URL: http://newsland.com/user/4297728425/content/19-letnego-serba-posadili-za-ugrozy-prezidentu-v-facebook/4322971 (дата звернення: 28.10.2018).

8. Англичанин получил тюремный срок за интернет-троллинг // Аргументы и факты. Aif.ru. 15.09.2011 19:55. URL: http://www.aif.ru/society/ web/264179 (дата звернення: 28.10.2018).

Одержано 30.10.2018

УДК 341.41

Альона Леонідівна ШЕВЧЕНКО,
викладач кафедри міжнародного і європейського права
юридичного факультету
Харківського національного університету імені В. Н. Каразіна

ЗАБЕЗПЕЧЕННЯ ІНФОРМАЦІЙНОЇ БЕЗПЕКИ ПЕРСОНАЛУ МІЖНАРОДНОГО КРИМІНАЛЬНОГО СУДУ

Використання інформаційних та комунікаційних технологій (далі – ІКТ) відіграє провідну роль у багатьох сферах суспільного життя, зокрема у системах правосуддя. Так, ІКТ широко застосовуються при здійсненні правосуддя, зокрема, для поліпшення обробки інформації, передачі та публікації, дотримання прав учасників процесу, тощо. Разом із тим, застосування ІКТ може мати й негативні наслідки у сфері інформаційної безпеки, зокрема витік інформації, можливість внесення змін до інформаційних джерел або виведення з ладу усієї електронної системи суду. Такі протиправні дії завдають шкоди як окремим учасникам міжнародного кримінального судочинства, так й інформаційній безпеці суду в цілому. З огляду на зазначене, забезпечення інформаційної безпеки є невід'ємною частиною відправлення ефективного і незалежного правосуддя та дотримання прав учасників міжнародного кримінального судочинства, зокрема

осіб, які забезпечують реалізацію задач міжнародного кримінального судочинства.

Діяльність МКС щодо забезпечення інформаційної безпеки повинна бути оцінена з урахуванням існуючого рівня загрози в певний момент часу. Загальний рівень загрози інформаційним активам Суду та системам інформаційних технологій (ІТ) значно збільшився у період 2014-2016 рр. Крім того, слід зазначити, що найважливішою тенденцією є збільшення частоти, різноманітності та складності кібератак, спрямованих на комп'ютерні системи та системи зв'язку МКС [1].

Відповідно до оцінки рівня майбутніх кіберзагроз, прогнозується збільшення останніх, оскільки Суд поступово розширює свої сфери зацікавленості. Подібним чином, оскільки діяльність та інтереси Суду розширюються, збільшується попит на більш захищені ІТ та комунікаційні системи. У свою чергу, з огляду на те, що сфери застосування ІКТ розширюються, збільшується відповідно кількість об'єктів, які знаходяться під ризиком кібератак [1].

МКС, поряд з більшістю інших користувачів інтернет-технологій, піддається суцільнім загрозам кібератак та небажаної кіберактивності, зокрема атаки «Відмова в обслуговуванні.2 (DoS), «атаки «фішингу» сканування вразливості, вірусної інфекції, а зовсім недавно - викрадення. Зловмисне (шкідливе) програмне забезпечення являє собою значний елемент регулярних нападів на Суд, і його широко використовують для спроб несанкціонованого доступу, створення нелегальних каналів зв'язку, пошкодження або експорту даних та збирання інформації [1].

Співробітники Суду та посадові особи також прямо чи опосередковано знаходяться у групі ризику кібер-загроз, адже у своїй повсякденній діяльності використовують комп'ютери, мобільні пристрої, електронну пошту та інші засоби, які мають вихід до мережі Інтернет. Кібератаки у різноманітних формах широко застосовуються проти персоналу МКС для збору інформації, отримання доступу до конфіденційних даних та інших дій, що перешкоджають діяльності Суду в цілому.

З огляду на вищеозначене, акти (статути, правила процедури і доказування, регламенти тощо) МКС містять положення про регулювання питань інформаційної безпеки. Важливу увагу у внутрішніх актах МКС (адміністративні інструкції, накази, інформаційні циркуляри тощо) приділено забезпеченню інформаційної безпеки, зокрема, передбачено класифікацію інформації згідно з рівнем ризику, встановленням порядку використання мобільних пристроїв і портативних запам'ятовуючих засобів, встановленням порядку доступу третіх осіб до інформації тощо.

Згідно з положеннями РС МКС, Суд створює надійну, захищену та ефективну електронну систему, яка забезпечує підтримку повсякденного управління судовими та адміністративними справами

Суду і провадження в Суді. Секретаріат несе відповідальність за функціонування системи, згаданої в пункті 1 цього положення, враховуючи при цьому конкретні вимоги, пов'язані з судовою діяльністю Суду, в тому числі необхідність забезпечити автентичність, точність, конфіденційність і збереження судових протоколів і матеріалів. Документи, рішення і розпорядження передаються до Секретаріату для реєстрації, за можливості, в електронній формі (положення 26 (1-3) РС МКС) [2].

Наказ Голови МКС «Політика інформаційної безпеки» (далі – Наказ) закріплює положення, що стосуються забезпечення інформаційної безпеки Суду. Так, зокрема, вказано, що ця політика спрямована на захист конфіденційності, цілісності і доступності інформації від загроз, включаючи помилки, шахрайство, саботаж, тероризм, вимагання, шпигунство, порушення конфіденційності, переривання обслуговування, крадіжки і стихійне лихо, будь то внутрішні або зовнішні, навмисні чи випадкові загрози. Суд вимагає, щоб важлива для його функціонування інформація була захищена належним чином щоб захистити громадськість та інтереси Суду [3].

Важливою гарантією забезпечення інформаційної безпеки персоналу МКС є закріплена Наказом норма, згідно з якою Суд має активно підтримувати серед співробітників і посадових осіб поінформованість і знання про інформаційну безпеку та пов'язану з нею політику, процедури, стандарти і керівні принципи, що стосуються інформаційної безпеки. Працівники та посадові особи зобов'язані негайно повідомляти про будь-які підозрілі інциденти, віруси, програмні збої в роботі, недоліки або загрози, які виникають або можуть виникнути щодо інформації та інформаційних систем Суду. На Офіцера з інформаційної безпеки покладаються обов'язки із забезпечення інформаційної безпеки Суду та координації і контролю відповідних заходів. Крім того, Офіцер з інформаційної безпеки надає МКС і його органам консультації про ризики, можливості і заходи щодо інформаційної безпеки [3].

Адміністративна інструкція ICC/AI/2007/002 «Інформаційна безпека в мобільних пристроях і портативних накопичувальних носіях» вказано, стосується конфіденційної інформації на мобільних пристроях і портативних накопичувальних носіях, які використовуються співробітниками Суду. Безпечне використання мобільних пристроїв і портативних носіїв інформації у Суді дозволить зменшити ризик розголошення конфіденційної інформації і пов'язані з цим негативні наслідки через втрату або крадіжку. Велика частина цієї інформації є вразливою в тому сенсі, що її несанкціоноване розкриття або зміна можуть поставити під загрозу репутацію Суду, мати негативні наслідки для справи, свідків, співробітників, посадових осіб тощо. Такій інформації має бути забезпечено захист у встановленому порядку [4].

Користувачами Суд визначає всіх співробітників, виборних посадових осіб МКС, фахівців і стажистів/клерків, консультантів, робітників за контрактом та інших осіб, які отримали доступ до ІКТ-ресурсів. AI ICC/AI/2007/002 визначено, що за користування і захист мобільних пристроїв і портативних запам'ятовуючих засобів несе відповідальність користувач. Користувачі не повинні підключати мобільні пристрої до інших мереж, окрім мережі Суду. Адміністратори відділу ІКТ можуть підключати мобільні пристрої PDA до мережі Суду для проведення випробувань, монтажу, технічного обслуговування і резервування [4].

Для боротьби з кіберзагрозами, які спрямовані на підрив нормального функціонування ІТ-інфраструктури МКС, Суд здійснює, відповідно до оціночних ризиків, численні перевірочні, детективні та інформаційні кампанії, спрямовані на підвищення рівня інформаційної безпеки. Зважаючи на наявні можливості МКС щодо забезпечення інформаційної безпеки персоналу та Суду в цілому, слід однак зазначити, що кібербезпека потребує нових, а іноді й новаторських методів для виявлення та протидії постійно зростаючому діапазону атак. Так, МКС оснащує свої приміщення необхідною технікою, а також інвестує у свою кібербезпеку (160 тис. євро – за 2016 рік) задля стійкого захисту власних інформаційних систем.

Таким чином, належний доступ до інформації та передача інформації безумовно покращує ефективність міжнародних судових органів, дає рівні можливості всім учасникам судового процесу. Однак важливо зазначити, що використання ІКТ у роботі МКС становить ризик для користувачів цих послуг. У безпосередню небезпеку потрапляють бази даних МКС, які містять конфіденційну інформацію, зокрема стосовно учасників судового процесу. Така інформація може бути використана злочинним шляхом. Для запобігання таким незаконним діям МКС приймає відповідні акти (адміністративні вказівки, директиви, інформаційні циркуляри, тощо), які створюють правову основу для належного функціонування та забезпечення інформаційної безпеки персоналу і Суду в цілому.

Список бібліографічних посилань

1. Second Court's report on the development of performance indicators for the International Criminal Court. URL: https://www.icc-cpi.int/itemsDocuments/ICC-Second-Court_report-on-indicators.pdf.

2. REGULATIONS OF THE COURT. URL: https://www.icc-cpi.int/NR/rdonlyres/B920AD62-DF49-4010-8907-E0D8CC61EBA4/277527/ Regulations_of_the_Court_170604EN.pdf.

3. Presidential Directive Information Security Policy ICC/PRESD/G/2005/001. URL: https://www.icc-cpi.int/resource-library/Documents/RegulationsRegistryEng.pdf.

4. Administrative Instruction ICC/AI/2007/002. URL: https://www.icc-cpi.int/resource-library/Vademecum/Information%20Security%20for%20Mobile %20Devices%20and%20Portable%20Storage%20Media.PDF.

Одержано 02.11.2018