ВІД РЕДАКЦІЙНОЇ КОЛЕГІЇ

Неофіційний переклад

ПОСТАНОВА
Ради Європейського Союзу № 2005/222/JHA від 24 лютого 2005 року

“ПРО ЗАХОДИ У ЗВ’ЯЗКУ З НАПАДАМИ НА ІНФОРМАЦІЙНІ СИСТЕМИ”

Рада Європейського Союзу,
Беручи до уваги Договір про Європейський Союз, і зокрема його статті 29, 30 (1)(a), 31 (1)(e) і 34 (2)(b),
Беручи до уваги пропозиції Комісії Європейського Союзу,
Беручи до уваги позицію Європейського парламенту, оскільки:

(1) Метою цієї Рамкової постанови є покращення співробітництва між судовими та іншими компетентними органами, включаючи поліцію й інші спеціалізовані правоохоронні служби держав-членів, шляхом гармонізації норм кримінального законодавства в державах-членах в сфері нападів на інформаційні системи.

(2) Випадки нападів та зростаюча стурбованість з приводу організованої злочинності щодо терористичних нападів на інформаційні системи як складові критичної інфраструктури* держав-членів, є загрозою для створення більш безпечного простору свободи та правосуддя і тому вимагають відповідних заходів на рівні Європейського Союзу.

(3) Такі загрози вимагають ефективної реакції шляхом комплексного підходу до телекомунікаційних мереж та інформаційної безпеки, як це підкреслено в Плані дій “Електронна Європа”, в повідомленні Комісії “Телекомунікаційна мережа та інформаційна безпека: пропозиції щодо основних принципів європейської політики” і в Рішенні Ради від 28 січня 2002 року “Про загальні підходи і конкретні дії в галузі мережевої та інформаційної безпеки”.

(4) Необхідність подальшого підвищення обізнаності про проблеми, пов’язані з інформаційною безпекою, та забезпечення практичної допомоги також підкреслені в Рішенні Європейського парламенту від 5 вересня 2001 року.

(5) Прогалини і відмінності в законодавствах держав-членів у цій галузі можуть ускладнити боротьбу з організованою злочинністю і тероризмом, а також ефективне поліцейське і судове співробітництво у зв’язку з нападами на інформаційні системи. Транснаціональність і безмежність сучасних інформаційних систем та напади на такі системи підкреслюють нагальну необхідність прийняття додаткових заходів для гармонізації кримінального законодавства.

(6) План дій Ради і Комісії про те, як найкращим чином реалізувати положення Амстердамського договору “Про простір свободи, безпеки та правосуддя”, Європейська рада в м. Тампере, що тривала з 15 по 16 жовтня 1999 року, Європейська рада в Санта-Марія-да-Фейра, що тривала з 19 по 20 червня 2000 року, а також Резолюція Європейського парламенту від 19 травня 2000 року закликали прийняти законодавчий акт з метою запобігання злочинам в сфері високих технологій.

(7) Необхідно доповнювати роботу, виконану міжнародними організаціями, зокрема Ради Європи про гармонізацію кримінального права та роботу Великої вісімки щодо транснаціонального співробітництва в сфері високотехнологічної злочинності, забезпечивши в Європейському Союзі єдиний підхід в цій області. Цей заклик отримав розвиток в Повідомленні

---

* *Від перекладача*. Критична інфраструктура – всі об’єкти та системи, порушення або пошкодження яких призведе до катастрофічних наслідків для здоров’я та життя громадян, порушить діяльність органів влади, нормальне функціонування економіки, підірве віру населення в економічні і політичні інститути.

Комісії до Ради Європи, Європейського парламенту, Економічного і соціального комітету та Комітету регіонів про “Створення більш безпечного інформаційного суспільства, підвищення безпеки інформаційних інфраструктур і боротьби з комп’ютерною злочинністю”.

(8) Кримінальне законодавство щодо нападів на інформаційні системи має бути гармонізованим для того, щоб забезпечити найбільш ефективне поліцейське і судове співробітництво, а також для того, щоб внести свій вклад у боротьбу з організованою злочинністю і тероризмом.

(9) Всі держави-члени ратифікували Конвенцію Ради Європи від 28 січня 1981 “Про захист осіб у зв’язку з автоматизованою обробкою персональних даних”. Персональні дані, на які розповсюджуються ця Рамкова постанова, мають бути захищені відповідно до вищезазначених у Конвенції принципів.

(10) Загальні тлумачення в цій сфері, зокрема, тлумачення понять “інформаційна система” і “комп’ютерні дані”, мають важливе значення для забезпечення послідовного підходу в державах-членах при застосуванні цієї Рамкової постанови.

(11) Необхідно виробити загальний підхід до складових елементів кримінальних злочинів, зокрема до несанкціонованих доступу і втручання в інформаційну систему та до даних.

(12) В інтересах боротьби з комп’ютерною злочинністю, кожна держава-член має забезпечити ефективну співпрацю судових органів під час розкриття злочинів, про які йде мова у статтях 2, 3, 4 і 5.

(13) Необхідно уникати застосування заходів надмірної криміналізації, особливо того, що стосується дрібних справ.

(14) Держави-члені повинні забезпечити штрафні санкції за напади на інформаційні системи. Такі штрафні санкції повинні бути ефективними, пропорційними і суворими.

(15) Доцільно передбачити більш суворе покарання, коли напади на інформаційні системи скоєно в рамках злочинної організації, як це визначено у Спільному Акті Європейського Союзу № 98/733 від 21 грудня 1998 року “Про здійснення кримінальних злочинів, в тому числі кримінальними організаціями в державах-членах”. Якщо такий напад призвів до серйозних пошкоджень або завдав значної шкоди, доцільно передбачити більш суворі покарання.

(16) Відповідні заходи забезпечення ефективних дій проти нападів на інформаційні системи мають бути передбачені метою співробітництва між державами-членами. Для обміну інформацією держави-члени повинні використовувати існуючу мережу оперативних пунктів контакту, про які йде мова у Рекомендації Ради “Про контактні пункти, що надають 24-годинну послугу боротьбі з високотехнологічної злочинністю” від 25 червня 2001 року.

(17) Цілі даної Рамкової постанови, які передбачають забезпечити удосконалення та розвиток співробітництва між судовими органами шляхом усунення можливих бар’єрів, а також щоб в усіх державах-членах були передбачені міри покарання щодо ефективних, відповідних і стримуючих кримінальних санкцій, не можуть бути достатньою мірою досягнуті державами-членами на національному рівні, щоб бути загальними та гармонізованими. Такі цілі можуть бути досягнуті тільки на рівні Союзу. Тому Союз може вжити заходів відповідно до принципу субсидіарності, зазначеного у статті 5 Договору про Європейський Союз. Відповідно до принципу пропорційності, викладеного в цій статті, ця Рамкова постанова не виходить за межі необхідного для досягнення цих цілей.

(18) Ця Рамкова постанова визнає основні права та принципи, визначені в статті 6 Договору про Європейський Союз і відображені в Хартії основних прав Європейського Союзу, зокрема в главі II і VI;

Прийняла цю Рамкову постанову:

Стаття 1. Визначення

Для цілей цієї Рамкової постанови застосовуються наступні визначення:

(а) **“інформаційна система”** означає будь-який пристрій або групу взаємопов’язаних чи суміжних пристроїв, одна або кілька з яких, відповідно до програми, здійснює автоматизовану обробку комп’ютерних даних, а також їх зберігання, обробку, відновлення або передачу з метою їх експлуатації, використання, охорони та захисту;

(b) **“комп’ютерні дані”** означають будь-яке представлення фактів, інформації або понять у формі, придатній для їх обробки в інформаційній системі, включаючи програми для виконання системою своїх функції;

(c) **“юридична особа”** означає будь-яку особу, яка має такий статус відповідно до чинного законодавства, за винятком держав або інших державних органів, а також за винятком громадських міжнародних організацій;

(d) **“несанкціонований”** означає доступ або втручання до інформаційної системи без дозволу від власника, чи іншого суб’єкта права, або яке заборонено відповідно до національного законодавства.

Стаття 2. Несанкціонований доступ до інформаційних систем

1. Кожна держава-член має вжити необхідних заходів для забезпечення того, щоб несанкціонований доступ до всієї або будь-якої частини інформаційної системи прирівнювався до кримінального злочину, за виключенням випадків, які не є значними.

2. Кожна держава-член може прийняти рішення про те, що положення параграфу 1 застосовується тільки в тих випадках, коли злочин скоєно шляхом порушеннями заходів безпеки.

Стаття 3. Несанкціоноване втручання в інформаційну систему

Кожна держава-член має вжити необхідних заходів для забезпечення того, щоб навмисні серйозні перешкоди функціонуванню інформаційної системи або його переривання шляхом введення, передачі, пошкодження, вилучення, погіршення якості, зміни або поширення комп'ютерних даних, що не є доступними для загального доступу, прирівнювалися до кримінального злочину, якщо відповідні дії є несанкціонованими.

Стаття 4. Несанкціоноване втручання до даних

Кожна держава-член має вжити необхідних заходів для забезпечення того, щоб несанкціоноване навмисне видалення, пошкодження, погіршення якості, зміна або поширення комп'ютерних даних інформаційної системи, що не передбачені для загального доступу, прирівнювалися до кримінального злочину, якщо відповідні дії є несанкціонованими, принаймні за виключенням випадків, коли вони є незначними.

Стаття 5. Підбурювання до пособництва, співучасть, спроба здійснення злочинів

1. Кожна держава-член має забезпечити, щоб підбурювання до пособництва і співучасть у скоєнні злочинів, зазначених в статтях 2, 3 і 4, прирівнювалися до кримінальних злочинів.

2. Кожна держава-член має забезпечити, щоб спроба здійснення злочинів, зазначених у статтях 2, 3 і 4, прирівнювалася до кримінальних злочинів.

3. Кожна держава-член може прийняти рішення не застосовувати положення пункту 2 до злочинів, зазначених у статті 2.

Стаття 6. Покарання

1. Кожна держава-член має вжити необхідних заходів для забезпечення того, щоб до злочинів, про які йде мова в статтях 2, 3, 4 і 5, застосовувалися ефективні і відповідні кримінальні покарання.

2. Кожна держава-член має вжити необхідних заходів для того, що до злочинів, про які йде мова в статтях 3 і 4, застосовувалися кримінальні покарання у вигляді принаймні від одного до трьох років позбавлення волі.

Стаття 7. Обтяжуючі обставини

1. Кожна держава-член має вжити необхідних заходів для забезпечення того, щоб до злочинів, про які йде мова в статті 2(2), а також до злочинів, про які йде мова в статтях 3 і 4, засто-

совувалися кримінальні покарання у вигляді принаймні від двох до п'яти років позбавлення волі, у випадку якщо такі злочини скоєно в рамках кримінальної організації, як визначено у Спільному Акті 98/733/JHA.

2. Держава-член може також вживати заходів, про які йде мова в пункті 1, у випадку якщо злочин завдав серйозного збитку.

Стаття 8. Відповідальність юридичних осіб

1. Кожна держава-член має вжити необхідних заходів до того, що юридичні особи могли бути притягнуті до відповідальності за злочини, зазначені у статтях 2, 3, 4 і 5, які біли скоєні в їх інтересах будь-якою фізичною особою, що діє самостійно або як представнику юридичної особи та яка займає керівну посаду у юридичній особі, базуючись на:

(а) повноваженнях представляти відповідну юридичну особу; або

(б) повноваженнях приймати рішення від імені відповідної юридичної особи; або

(с) правах виконувати контролюючі функції і цій юридичній особі.

2. Крім випадків, передбачених у пункті 1, держави-члени повинні забезпечувати, щоб юридична особа могла бути притягнута до відповідальності, якщо відсутність нагляду або контролю з боку особи, про яку йде мова в пункті 1, зробило можливим вчинення особою під її керівництвом, злочинів, зазначених у статтях 2, 3, 4 і 5, в інтересах цієї юридичної особи.

3. Відповідальність юридичної особи відповідно до пунктів 1 і 2 не знімає необхідність кримінального процесу проти фізичних осіб, які беруть участь у скоєнні злочинів, зазначених у статтях 2, 3, 4 і 5, як виконавці, підбурювачі і співучасники.

Стаття 9. Покарання для юридичних осіб

1. Кожна держава-член має вжити необхідних заходів для забезпечення того, щоб до юридичної особи, що несе відповідальність згідно зі статтєю 8(1), застосовувалися ефективні і співрозмірні заходи покарання, які повинні включати такі санкції, як:

(а) позбавлення права на суспільні пільги чи допомогу;

(b) тимчасове або постійне позбавлення права займатися комерційною діяльністю;

(с) поміщення під судовий нагляд; або

(d) ліквідація за рішенням суду.

2. Кожна держава-член має вжити необхідних заходів для забезпечення того, щоб до юридичної особи, що несе відповідальність згідно зі статтєю 8(2), застосовувалися ефективні і співрозмірні санкції/заходи.

Стаття 10. Юрисдикція

1. Кожна держава-член встановлює свою юрисдикцію стосовно злочинів, зазначених у статтях 2, 3, 4 і 5, якщо злочин було скоєно:

(а) на частині або на всій її території; або

(б) одним з її громадян, або

(с) в інтересах юридичної особи, офіс якої розташований на території цієї держави-члена.

2. При встановленні своєї юрисдикції відповідно до пункту (1) (а) кожна держава-член повинна забезпечити, щоб юрисдикція розповсюджувалася на випадки, коли:

(а) правопорушник скоює злочин, фізично знаходячись на її території, незалежно від того чи скоєно відповідний злочин проти інформаційної системи на її території; або

(b) злочин скоєно проти інформаційної системи на її території незалежно від того, чи знаходиться правопорушник, що скоює злочин, фізично на її території.

3. Держави-члени, які відповідно до свого законодавства не передають своїх громадян іншим державам, повинні вжити необхідних заходів для встановлення своєї юрисдикції у таких рамках щоб це дало можливість переслідувати у судовому порядку, у разі необхідності, за злочини, зазначені в статтях 2, 3, 4 і 5, якщо вони здійснені одним з громадян відповідної держави-члена за межами території даної держави.

4. Якщо злочин підпадає під юрисдикцію більш ніж однієї держави-члена і будь-яка із зацікавлених держав може на законних підставах здійснювати судовий процес на підставі тих самих фактів, такі держави-члени повинні співпрацювати, щоб вирішити, яка з них буде здійснювати такий судовий процес проти правопорушників з метою, якщо це можливо, централізації здійснення процесу в одній державі-члені. Для цього держави-члени можуть звертатися в будь-який орган, створений в рамках Європейського Союзу, з метою сприяння співробітництву між судовими органами та координації їх дій. Необхідно звернути увагу на наступні фактори:

- держава-член має бути тією, на території якої було скоєно злочин відповідно до пункту 1 (a) і пункту 2;
- держава-член має бути тією, злочинець якої є її громадянином;
- держава-член має бути тією, у якій злочинець був знайдений.

5. Держава-член може прийняти рішення не застосовувати чи застосовувати лише в особливих випадках або при особливих умовах правила щодо юрисдикції, викладені в пунктах 1 (b) і 1 (c).

6. Держави-члени повинні інформувати Генеральний секретаріат Ради та Комісії, якщо вони прийняли рішення застосувати пункт 5, з вказівкою конкретних випадків або обставин, при яких він застосовується.

Стаття 11. Обмін інформацією

1. З метою обміну інформацією стосовно правопорушень, зазначених у статтях 2, 3, 4 і 5, та відповідно до правил захисту даних держави-члени повинні забезпечувати, щоб вони були доступні 24 години на добу сім днів на тиждень через існуючу мережу оперативних контактних пунктів.

2. З метою обміну інформацією про злочини, пов’язані з нападами на інформаційні системи, кожна держава-член має проінформувати Генеральний Секретаріат Ради та Комісії про свій контактний пункт. Генеральний Секретаріат направляє цю інформацію іншим державам-членам.

Стаття 12. Впровадження

1. Держави-члени має вжити необхідних заходів для виконання положень цієї Рамкової постанови до 16 березня 2007 року.

2. До 16 березня 2007 року держави-члени мають надіслати до Генерального Секретаріату Ради та Комісії тексти положень, що відображатимуть в їх національному законодавстві зобов'язання, які накладаються на них в рамках цієї Рамкової постанови. До 16 вересня 2007 року на основі письмового звіту Комісії, підготовленого на базі отриманої інформації, Рада має оцінити ступінь дотримання державами-членами положень цієї Рамкової постанови.

Стаття 13. Набуття чинності

Ця Рамкова постанова набуває чинності з дати її публікації в Офіційному журналі Європейського Союзу.

Брюссель, 24 лютого 2005 р.

Переклад з англ. – Віри Брижко.
Режим доступу: *// www.eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=CELEX:32005F0222:EN:NOT*

* * * * * * * * * * * * * * * * *