Артем УШАКОВ,
студент 746 ю., гуманітарно-правового факультету
Національного аерокосмічного університету ім. М. Є. Жуковського
«Харківський авіаційний інститут», Харків, Україна

Науковий керівник: Михайло ФІАЛКА,
кандидат юридичних наук, доцент, професор кафедри права
Гуманітарно-правового факультету Національного
аерокосмічного університету ім. М.Є. Жуковського
«Харківський авіаційний інститут», Харків, Україна
e-mail: fialkami70@gmail.com
ORCID: 0000-0001-5599-3335

DOI: https://doi.org/10.32620/pls.2024.5.20

КРИМІНАЛЬНО ПРАВОВЕ ЗАБЕЗПЕЧЕННЯ ЗАХИСТУ ДИСТАНЦІЙНОГО ОСВІТНЬОГО СЕРЕДОВИЩА ВІД НЕСАНКЦІОНОВАНОГО ВТРУЧАННЯ У КОНТЕКСТІ СТ. 361 ККУ

Анотація: *У роботі досліджено кримінально-правове забезпечення захисту освітніх середовищ дистанційного навчання від несанкціонованого втручання у контексті ст. 361 Кримінального кодексу України.*

Зокрема, висвітлено загальнотеоретичні аспекти функціонування правової норми, яка регулює відповідальність за несанкціоноване втручання в інформаційні, електронно-обчислювальні та автоматизовані системи. Розглянуто прикладні аспекти використання ст. 361 для захисту інформаційних ресурсів дистанційного навчання, таких як платформ Mentor та інших аналогічних систем. Окрему увагу приділено питанням кваліфікації кримінальних правопорушень за ст. 361 ККУ у контексті захисту освітніх систем.

Надано рекомендації щодо вдосконалення правового регулювання для посилення кримінально-правового захисту дистанційного навчання. Надано рекомендації щодо вдосконалення правового регулювання та посилення кримінально-правового захисту дистанційного навчання. Робота має практичне значення для удосконалення механізмів захисту освітніх середовищ, формування ефективної законодавчої бази та забезпечення правової захищеності учасників освітнього процесу в цифровому середовищі.

Ключові слова: *кримінальне правопорушення, кримінальний закон, несанкціоноване втручання, освітнє середовище, дистанційне навчання.*

В умовах сучасного розвитку цифрових технологій і вимушеного переходу закладів вищої освіти на дистанційні форми навчання, особливо в періоди кризових ситуацій, зростає вразливість інформаційних систем до кримінально-протиправного впливу. Несанкціоноване втручання в роботу автоматизованих систем навчання не лише порушує права студентів і викладачів, але й ставить під загрозу інформаційну безпеку навчального процесу. З метою захисту цих суспільних відносин і була створена нижчезазначена стаття.

Ст. 361 КК України передбачає кримінальну відповідальність за несанкціоноване втручання в роботу електронно-обчислювальних машин, автоматизованих систем, комп’ютерних мереж чи мереж електрозв'язку. Об'єктом цього правопорушення є інформаційна безпека, а також нормальне функціонування електронних систем. Суб'єктом є фізична особа, яка досягла віку кримінальної відповідальності та володіє необхідною дієздатністю. Об'єктивна сторона проявляється в діях, що порушують роботу вказаних систем і спричиняють певні наслідки, включаючи витік, підробку чи блокування інформації. Суб'єктивна сторона характеризується прямим умислом, коли особа усвідомлює протиправність своїх дій і бажає настання шкідливих наслідків [1].

Аналіз ст. 361 КК України свідчить про її значний потенціал у захисті дистанційного освітнього середовища від несанкціонованого втручання.

Це особливо важливо для університетів, де електронні системи забезпечують освітній процес, включаючи дистанційне навчання, управління навчальними матеріалами та взаємодію між студентами і викладачами.

Електронні комунікаційні системи університету, навчальні портали та системи управління електронною документацією по всім

ознакам можуть виступати предметом злочину за ст. 361. КК України Злочин, визначений цією статтею, полягає в умисному несанкціонованому втручанні, що може призвести до витоку, підробки або блокування інформації, спотворення процесу обробки даних, що завдає шкоди освітньому процесу та порушує права учасників навчання. Важливо розуміти те що наслідки діяння, передбаченого досліджуваною статею можуть бути як матеріальними так і нематеріальними. А. А. Васильєв та Д. В. Пашнєв свого часу влучно зазначили про це. Вони вважають, що «крім матеріальної шкоди, суспільно небезпечні наслідки при вчиненні комп'ютерного злочину можуть виражатись і в нематеріальних видах шкоди, що зумовлено використанням ЕОМ, систем і комп'ютерних мереж для контролю над складними технологічними процесами, об'єктами та управління ними.» [2, с.35].

Система дистанційного навчання Mentor distance learning system (далі – Mentor) потенційно може стати предметом вчинення кримінального правопорушення, передбаченого ст. 361 КК України, якщо щодо неї відбудеться умисне несанкціоноване втручання. Відповідно до ст. 1 ЗУ «Про захист інформації в електронних комунікаційних системах» під такою системою розуміється сукупність інформаційних та електронних комунікаційних систем, які у процесі обробки інформації діють як єдине ціле [3, с.1].

Це втручання може включати несанкціонований доступ, модифікацію або блокування інформації, що зберігається чи обробляється у системі, що, у свою чергу, порушує нормальне функціонування системи та завдає шкоди користувачам і закладу.

Об'єктом кримінально-правового захисту у цьому контексті є інформаційна безпека та захист даних, що забезпечують стабільну роботу системи дистанційного навчання. У випадку системи Mentor такими даними є логіни та паролі студентів, домашні роботи, матеріали лекцій та інші навчальні ресурси, доступні виключно студентам через корпоративні акаунти, а саме об'єктом є загальний стан інформаційної безпеки та захисту цих даних. Несанкціоноване втручання в таку систему може призвести до витоку конфіденційної інформації, підробки чи видалення навчальних матеріалів, що порушує права студентів і викладачів, а також підриває довіру до системи в цілому.

Таким чином, Mentor як електронна комунікаційна платформа, що підтримує освітній процес, підпадає під сферу дії ст. 361 КК України. Захист такої системи від кіберзлочинів є важливим для забезпечення цілісності та безпеки навчальних даних, а також для підтримання належного рівня освітніх послуг.

Діяння, яке не спричинило істотних наслідків, може бути проблематичним для інкримінування за ст. 361 КК України. Ст. 11 КК України встановлює загальні положення про кримінальне правопорушення, згідно з якими діяння вважається таким лише за наявності суспільної небезпеки та істотної шкоди. Це означає, що формальне втручання, яке не спричинило наслідків, може бути визнане малозначним і не тягнути за собою кримінальної відповідальності.

Однак, ч. 1 ст. 361 КК України передбачає кримінальну відповідальність за несанкціоноване втручання, яке порушує нормальну роботу автоматизованих систем чи мереж, навіть якщо воно не спричинило значних наслідків. Така конструкція статті може вказувати на те, що вона є усіченим складом кримінального правопорушення, оскільки сам факт втручання визнається достатнім для інкримінування. З іншого боку, для ч. 2 ст. 361 важливо, щоб втручання призвело до істотної шкоди, наприклад, порушення цілісності інформації чи її втрати, що підвищує серйозність злочину.

Таким чином, для застосування ч. 1 ст. 361 КК України не обов'язково наявність матеріальних наслідків, оскільки акцент робиться на самому факті втручання. Це підкреслює превентивну функцію норми для захисту електронних систем. Водночас, за відсутності наслідків або істотної шкоди, що вимагається ч. 2, дія може бути визнана такою, що не становить суспільної небезпеки (відповідно до ст. 11 КК України).

У контексті захисту системи дистанційного навчання Mentor, важливо враховувати численні аспекти, що забезпечують її стійкість та захист від потенційних зловмисників. Враховуючи вимоги ст. 361 КК України, яка передбачає відповідальність за несанкціоноване втручання в інформаційні системи, є необхідність запровадити комплексний підхід до захисту таких систем, як Mentor.

Перш за все, важливим кроком є правовий аудит та розробка політик конфіденційності. Необхідно забезпечити відповідність внутрішніх політик безпеки та умов користування вимогам законодавства України. Аудит має включати перевірку на відповідність нормативним актам щодо захисту персональних даних та процедур доступу до освітніх матеріалів. Крім того, має бути розроблена чітка політика збереження та обробки конфіденційної інформації, такої як логіни, паролі, домашні роботи та навчальні матеріали, яка визначатиме права й обов'язки користувачів та адміністрації системи.

Другим важливим кроком є створення внутрішніх інструкцій щодо доступу та обробки чутливих даних. Політика безпеки даних повинна регламентувати, як користувачі повинні поводитися з конфіденційною інформацією. Користувачі, у свою чергу, повинні бути ознайомлені з процедурою збереження безпеки своїх акаунтів та інформації. Це включає рекомендації щодо регулярної зміни паролів, використання складних комбінацій для доступу до акаунтів, а також обов'язкове застосування багатофакторної аутентифікації для забезпечення більш високого рівня захисту.

Підбиваючи підсумки варто зазначити що ст. 361 Кримінального кодексу України є важливим правовим інструментом для захисту інформаційної безпеки в умовах цифровізації освітнього процесу. Система Mentor, як платформа дистанційного навчання, підпадає під захист цієї норми, що передбачає кримінальну відповідальність за несанкціоноване втручання. Забезпечення правового і технічного захисту таких систем є

ключовим фактором для збереження стабільності навчального процесу та захисту прав його учасників. Комплексний підхід, що включає аудит безпеки, розробку внутрішніх політик та впровадження технічних заходів, є необхідним для мінімізації ризиків і протидії кіберзагрозам.

Бібліографічні посилання

1. Кримінальний кодекс України : Кодекс України від 05.04.2001 № 2341-III/01-ВР // База даних «Законодавство України»/Верховна рада України URL: https://zakon.rada.gov.ua/laws/show/2341-14#Text (дата звернення: 13.11.2024).
2. Пашнєв, Д. В. Особливості кваліфікації злочинів у сфері використання ЕОМ (комп'ютерів), систем та комп'ютерних мереж і мереж електрозв'язку. с. 36. URL: https://dspace.univd.edu.ua/server/api/core/bitstreams/79fce3d4-4a69-4cff-a559-60b25a1f0767/content (дата звернення: 13.11.2024).
3. Про захист інформації в інформаційно-телекомунікаційних системах: Закон України від 05.07.1994 № 80/94-ВР // База даних «Законодавство України»/Верховна рада України URL: https://zakon.rada.gov.ua/laws/show/80/94-вр#Text (дата звернення: 13.11.2024).

A. Ushakov, M. Fialka

Criminal legal provision of the protection of the distance educational environment against unauthorized interference in the context of article 361 of the criminal code.

Abstract: The study examines the criminal law framework for protecting educational environments in distance learning from unauthorized interference within the context of Article 361 of the Criminal Code of Ukraine. In particular, it highlights the general theoretical aspects of the functioning of the legal norm that regulates liability for unauthorized interference in information, electronic computing, and automated systems.

The practical aspects of applying Article 361 to safeguard information resources of distance learning platforms, such as Mentor and other similar systems, are explored. Special attention is given to the qualification of criminal offenses under Article 361 of the Criminal Code of Ukraine in the context of protecting educational systems. Recommendations are provided to improve legal regulation and strengthen criminal law protection of distance learning.

Additional recommendations aim at enhancing legal frameworks to ensure stronger criminal law protection of distance education. The study has practical significance for improving mechanisms for safeguarding educational environments, forming an effective legislative framework, and ensuring the legal protection of participants in the educational process in a digital setting.

Key words: criminal offense, criminal law, unauthorized interference, educational environment, distance learning.

Зразок для цитування:

Ушаков А., Фіалка М. Кримінально правове забезпечення захисту дистанційного освітнього середовища від несанкціонованого втручання у контексті ст. 361 ККУ. Пропілеї права та безпеки: наук. журнал. Національний аерокосмічний університет ім. М.Є. Жуковського «Харківський авіаційний інститут», 2024. № 5. С. 73-75. DOI: https://doi.org/10.32620/pls.2024.5.20.