Одеський державний університет внутрішніх справ
Кафедра кібербезпеки та інформаційного забезпечення
Факультет підготовки фахівців для підрозділів кримінальної поліції

# КІБЕРБЕЗПЕКА В УКРАЇНІ: ПРАВОВІ ТА ОРГАНІЗАЦІЙНІ ПИТАННЯ

International scientific-practical conference
"Cybersecurity in Ukraine: Legal and Organization Issues"

Матеріали
Міжнародної науково-практичної конференції
19 листопада 2021 року

Одеса 2021

Рекомендовано до друку рішенням кафедри кібербезпеки та інформаційного забезпечення
Одеського державного університету внутрішніх справ
(протокол № від грудня 2021 року)

Всі матеріали надані в авторській редакції та виражають
персональну позицію учасника конференції

Кібербезпека в Україні: правові та організаційні питання: матеріали міжн. наук.
К38 практ. конф., м. Одеса, 26 листопада 2020 р. Одеса : ОДУВС, 2021. _____ с.
ISBN 678-717-7020

У збірнику представлено стислий виклад доповідей і повідомлень, поданих на міжнародну науково-практичну конференцію «Кібербезпека в Україні: правові та організаційні питання», яка відбулася на базі кафедри кібербезпеки та інформаційного забезпечення Одеського державного університету внутрішніх справ 19 листопада 2021 року.

У матеріалах конференції приділено увагу актуальним теоретичним та практичним проблемам забезпечення інформаційної безпеки в Україні. Висвітлюється широкий спектр питань, пов'язаних з удосконаленням правового регулювання та адміністративно-правового забезпечення кібербезпеки в Україні. Розглянуто використання інформаційних систем, технологій та інформаційно-аналітична діяльність правоохоронних підрозділів у боротьбі з злочинністю та надано обґрунтовані рекомендації щодо вдосконалення підготовки персоналу для боротьби з кіберзлочинністю в Україні.

Матеріали всеукраїнської науково-практичної конференції адресовано вченим, працівникам правоохоронних органів, аспірантам (ад'юнктам), слухачам магістратури, студентам та курсантам вищих навчальних закладів.

© ОДУВС, 2021

*Одеський державний університет внутрішніх справ*
*«Кібербезпека в Україні: правові та організаційні питання»*

# ПРОБЛЕМИ ПРАВОВОГО ЗАБЕЗПЕЧЕННЯ КІБЕРЗАХИСТУ В УКРАЇНІ

**Возненко Я. В.**
студент 3 курсу 1 групи факультету №1 ННІПКБ ОДУВС
**Мельнікова О. О.**
викладач кафедри кібербезпеки та інформаційного забезпечення ОДУВС

Кібератаки є найбільшими ризиками, з якими може зіткнутися будь-яка організація. За даними глобального опитування, проведеного ISACA, лише 38% респондентів вважають, що готові до кібератак, решта 83% вважають кібератаки однією з найнебезпечніших загроз для організації. Якщо існує великий обсяг особистої та конфіденційної інформації, що надсилається електронними засобами, несанкціонований доступ до неї може призвести до серйозних наслідків [5].

Враховуючи наведений вище вираз, нам слід визначити терміни. Дотепер у виданнях зустрічаються різні поняття, які вживаються як синоніми, зокрема: «інформаційна безпека», «безпека інформації» та «кібербезпека». Автори, підміняючи ці поняття між собою, вводять суспільство в оману.

Вперше в Україні поняття «інформаційна безпека» визначено в Законі України «Про Основні засади розвитку інформаційного суспільства в Україні на 2007–2015 роки» від 09.01.2007 р. № 537-V [1], в якому інформаційна безпека визначається як стан життєво важливої безпеки, захисту інтересів людини, суспільства та держави, для запобігання заподіянню шкоди через: неповноту, несвоєчасну та малоймовірну інформацію; негативний інформаційний вплив; негативні наслідки використання інформаційних технологій; несанкціоноване поширення, використання та порушення цілісності, конфіденційності та доступності інформації.

Відповідно до Закону України «Про Основні засади розвитку інформаційного суспільства в Україні на 2007–2015 роки» вирішення проблеми інформаційної безпеки має здійснюватися шляхом: створення повноцінної інформаційної інфраструктури держави та забезпечення критичних елементів; підвищення рівня координації діяльності державних органів щодо виявлення, оцінки та прогнозування загроз інформаційній безпеці, запобігання таким загрозам та забезпечення ліквідації їх наслідків, здійснення міжнародного співробітництва з цих питань; удосконалення нормативно-правової бази забезпечення інформаційної безпеки, зокрема захисту інформаційних ресурсів, боротьби з комп'ютерною злочинністю, захисту персональних даних, а також забезпечення правопорядку в інформаційній сфері; розгортання та розвиток Національної системи конфіденційного зв'язку як сучасної безпечної транспортної основи, здатної інтегрувати географічно розподілені інформаційні системи, в яких обробляється конфіденційна інформація [1]. Як бачимо, поняття «інформаційна безпека» набагато ширше поняття безпеки інформації і зовсім до нього не зводиться.

Стандарт ISO/IES 27032 визначає «кібербезпеку» через категорію безпеки кіберпростору – збереження конфіденційності, цілісності та доступності інформації в кіберпросторі. Водночас кіберпростір – це середовище, що виникає в результаті функціонування на основі єдиних принципів та за загальними правилами інформаційних, телекомунікаційних та інформаційно-комунікаційних систем [7]. Відповідно до ГОСТ України ISO / IEC 27032: 2016 р. 4.21, кіберпростір - це складне середовище, що виникає в процесі взаємодії людей, програмного забезпечення та Інтернет-сервісів за допомогою технологічних пристроїв або взаємопов'язаних мереж, що не існують у будь-якій фізичній формі [8].

Закон України «Про основні засади забезпечення кібербезпеки України» заклав загальну архітектуру національної системи кібербезпеки та розподілив завдання та повноваження між основними суб'єктами кібербезпеки (Національний координаційний центр кібербезпеки, Міністерство оборони, Генеральний штаб Збройних Сил України, Державна служба спеціального зв'язку та захисту інформації, Служба безпеки, Національна поліція, Національний банк, розвідувальні органами України), передбачає створення умов для залучення підприємств, установ та організацій незалежно від форми власності, що діють у сфері електронних комунікацій, захисту інформації та/або власників (розпорядників) об'єктів критичної інфраструктури, наукових установ, навчальних закладів, організацій, громадських об'єднань та громадян.

Реалізація положень Стратегії кібербезпеки України та Закону України «Про основні засади забезпечення кібербезпеки України» передбачає розробку та застосування якісно нового законодавства у сфері кібербезпеки на основі досвіду, накопиченого за п'ять років гібридної війни, усвідомлення та впровадження досвіду та правил ЄС та НАТО. Зокрема, мають бути розроблені такі нормативно-правові акти: Закон України «Про критичну інфраструктуру та її охорону», постанови Кабінету Міністрів України, зокрема: «Порядок формування переліку об'єктів критичної інформаційної інфраструктури», «Порядок формування переліку об'єктів критичної інформаційної інфраструктури»,

«Загальні вимоги до кіберзахисту об'єктів критичної інфраструктури», «Про затвердження Протоколу спільних дій головних суб'єктів інформаційної інфраструктури».

Необхідно створити реєстр об'єктів критичної інформаційної інфраструктури, перелік об'єктів критичної інфраструктури, реєстр аудиторів інформаційної безпеки. Результатом впровадження цих нормативних актів має стати Комплексний огляд сектору безпеки та оборони, частиною якого має бути огляд стану кіберзахисту критичної інформаційної інфраструктури, державних інформаційних ресурсів та інформації, захист якої необхідний за законом.

Важливим кроком на шляху створення сучасної системи кіберзахисту в Україні стало прийняття постанови Кабінету Міністрів України від 19 червня 2019 р. № 518 «Про затвердження Загальних вимог до кіберзахисту об'єктів критичної інфраструктури» [3], де встановлено: визначення загальних вимог до кіберзахисту об'єктів критичної інфраструктури; встановлення обов'язкових заходів щодо забезпечення захисту від кібератак; запобігання порушенню конфіденційності; цілісність і доступність інформаційних ресурсів; стабільне функціонування.

Слід зазначити, що розвиток законодавства у сфері кібербезпеки в Україні безпосередньо пов'язаний з євроінтеграційними прагненнями України та розвитком правового регулювання електронної комерції в рамках СОТ.

Особливої уваги заслуговують ті, які визначені Директивою 2008/114/ЕС. Наскрізні критерії ESI, зазначені в пункті 1, включають: 1) критерій нещасних випадків (оцінюється потенційна кількість загиблих або травмованих); 2) критерій економічних результатів (оцінюється значущість економічних втрат та/або погіршення якості продукції чи послуг, включаючи потенційні екологічні наслідки); 3) критерій соціальних наслідків (оцінюється вплив на довіру населення, фізичні страждання, порушення повсякденного життя, у тому числі ненадання основних послуг).

Наскрізний ліміт слід встановлювати з урахуванням тяжкості наслідків пошкодження або руйнування певної інфраструктури. Точні граничні значення наскрізних критеріїв визначаються в кожному окремому випадку відповідними державами-членами для певної критичної інфраструктури. Кожна держава-член щорічно інформує Комісію про кількість інфраструктур у кожному секторі, для яких обговорювалися граничні значення наскрізних критеріїв. Галузеві критерії мають враховувати особливості окремих секторів ЄСІ. Роблячи це, кожна держава-член повинна перевірити, чи існує План безпеки оператора (ОРР) або подібні інструменти вирішення проблем у кожному конкретному ESI, розташованому на її території. Якщо держава-член визначила, що ВРО або подібні інструменти існують і регулярно оновлюються, немає необхідності в подальших діях щодо впровадження. [6]

Ці положення відображені в проекті Закону України «Про критичну інфраструктуру та її захист», а також у проектах постанов Уряду: «Порядку та критеріїв віднесення об'єктів до об'єктів критичної інфраструктури», а також «Порядку формування переліку об'єктів критичної інформаційної інфраструктури».

Необхідно звернути увагу на правове регулювання кібербезпеки в банківському секторі України. Швидкий розвиток нормативного забезпечення у сфері кібербезпеки банківського сектору можливий завдяки незалежній позиції Національного банку, визначеній Законом України «Про Національний банк» [2].

Забезпечення безпеки у кіберпросторі не обмежується заходами державного регулювання та контролю, а в багатьох випадках залежить від свідомої та відповідальної поведінки учасників правовідносин, зокрема суб'єктів господарювання. Кіберзлочинці все більше цікавляться ринком криптовалют та електронної комерції. Використовуючи різні способи здійснення атак, хакери крадуть електронні гроші безпосередньо у їх власників або використовують для цього доступні ресурси – гаманці, біржі тощо. Кібератаки на суб'єктів господарювання та їх діяльність можуть мати абсолютно різні форми. Це може бути фішинг, який здійснюється, наприклад, шляхом надсилання електронних листів співробітникам або використання шкідливого програмного забезпечення.

На сьогодні законодавче регулювання кіберзахисту в Україні перебуває на початку становлення, але пройдено складний етап – визначення стратегії, меж та напрямів державної політики щодо забезпечення кіберзахисту. Звичайно, на цьому шляху ще багато проблем, але є й досягнення.

Найперспективнішими напрямами розвитку національної системи кіберзахисту, на нашу думку, є: удосконалення нормативно-правової бази кіберзахисту об'єктів критичної інфраструктури; впровадження системи незалежного аудиту інформаційної безпеки на об'єктах критичної інфраструктури; створення галузевих центрів реагування на кіберінциденти; розвиток міжнародного співробітництва у сфері кібербезпеки; розробка системи навчання у сфері кібербезпеки; підвищення цифрової грамотності (правил кібергігієни) громадян та культури поведінки у кіберпросторі,

запровадження систем відповідності інформації та, насамперед, створення довірчих відносин між державою та суспільством, для яких держава має відігравати роль служби.

**Література:**

1. Про Основні засади розвитку інформаційного суспільства в Україні на 2007-2015 роки: Закон України від 09.01.2007 р. № 537-V. Відомості Верховної Ради України (ВВР). 2007. № 12. Ст. 102
2. Про Національний банк України. Закон України від 20.5.1999 № 679-XIV. Відомості Верховної Ради України (ВВР). 1999. № 29. Ст. 238.
3. Про затвердження Загальних вимог до кіберзахисту об'єктів критичної інфраструктури. Постанови Кабінету Міністрів України № 518 від 19 червня 2019 року. Офіційний вісник України від 02.07.2019. 2019. № 50. С. 53. Стаття 1697, код акту 94896/2019.
4. ДСТУ ISO/IEC 27032:2016 (ISO/IEC 27032:2012, IDT) «Інформаційні технології. Методи захисту. Настанови щодо кібербезпеки». 27.12.2016. № 448. URL: http://online.budstandart.com/ ua/catalog/doc-page.html?id_doc=69128 (дата звернення: 02.09.2019)
5. Стандарти ISO/IEC захистять від кіберзагроз. 31.08.2016. URL: http://csm.kiev.ua. (дата звернення: 16.11.2021);
6. Directive (EU) 2016/1148 of the European Parliament and of the Council of 6 July 2016 concerning measures for a high common level of security of network and information systems across the Union. OJ L 194, 19.7.2016, p. 1–30
7. ISO/IEC 27032:2012 Information technology – Security techniques – Guidelines for cybersecurity. URL: www.iso.org/standard/44375.html. (дата звернення: 16.11.2021).

**ЗМІСТ**

**СЕКЦІЯ 1.**
**ПРАВОВЕ РЕГУЛЮВАННЯ ЗАБЕЗПЕЧЕННЯ КІБЕРБЕЗПЕКИ В УКРАЇНІ**



**СЕКЦІЯ 2.**
**АДМІНІСТРАТИВНО-ПРАВОВЕ ЗАБЕЗПЕЧЕННЯ КІБЕРБЕЗПЕКИ В УКРАЇНІ**