Таким чином, ефективний захист держави в кіберпросторі вимагає комплексного підходу, бо лише поєднання технологічних, правових та освітніх заходів дозволяє мінімізувати ризики маніпуляцій та забезпечити інформаційну безпеку держави.

Список використаних джерел:

1. Про основні засади забезпечення кібербезпеки України : Закон України від 05 жовт. 2017 р. № 2163-VIII. *Відомості Верховної Ради України*. 2017. № 45. Ст. 403.

2. У серпні поточного року СБУ заблокувала 43 кібератаки на українські органи влади. *СБУ* : [сайт]. URL: https://ssu.gov.ua/novyny/u-serpni-potochnoho-roku-sbu-zablokuvala-43-kiberataky-na-ukrainski-orhany-vlady.

3. Disinformation as a Weapon: Media Tactics and Psychological Warfare in the Ukrainian Conflict. URL: https://sjps.fsvucm.sk/index.php/sjps/article/view/584.

4. *Кіберполіція* : [сайт]. URL: https://cyberpolice.gov.ua/.

Голікова Мілена Олексіївна
студентка 107_СПД н.гр. ННІ права та психології НАВС

Науковий керівник:
Швець Микола Миколайович
викладач кафедри інформаційних технологій ННІ права та психології НАВС

КІБЕРШПИГУНСТВО, КІБЕРШАХРАЙСТВО ТА КІБЕРАТАКИ

Сучасний світ більше не уявляється без диджиталізації, кожен з нас поступово, але невпинно входить до цифрового середовища. Однак не варто забувати, що цифровий світ несе не тільки можливості, але й нові загрози. Кібершпигунство, кібершахрайство та кібератаки – це різні грані сучасних інформаційних війн та злочинності. Розуміння їхньої природи є першим кроком до надійного захисту власних даних та національної безпеки.

Всі ці три поняття є різновидами кіберзлочинів та направлені на різні об’єкти нашого життя. Нагадаємо, що відповідно до Закону України «Про основні засади забезпечення кібербезпеки України» (далі – Закон), ***кіберзлочином*** (або комп’ютерним злочином) називають суспільно небезпечне винне діяння у кіберпросторі та/або з його використанням, відповідальність за яке передбачена законом України про кримінальну відповідальність та/або яке визнано злочином міжнародними договорами України [1].

Дане поняття дозволяє нам зрозуміти, що приставка «кібер-» вказує на те, що певне суспільно небезпечне діяння скоєно з використанням комп'ютерів, комунікаційних систем, електронних комунікацій, мережі Інтернет тощо. Розглянемо кожен із цих різновидів окремо і почнемо із кібершпигунства.

Відповідно до зазначеного вище Закону, під терміном «***кібершпигунство***» розуміють шпигунство, що здійснюється у кіберпросторі або з його використанням. Якщо казати більш простими словами, це незаконне отримання конфіденційної інформації або розвідувальних даних за допомогою комп'ютерних технологій [2].

Основними «жертвами» таких злочинів можуть стати великі корпорації, сегрегатори даних, фінансові, медичні та урядові установи, тобто ті організації, які володіють великими масивами конфіденційної інформації або ж інформації з обмеженим доступом. Злочинці, що вчиняють кібершпигунство, можуть мати різноманітну мотивацію, включаючи економічні вигоди, політичні цілі або здійснення шантажу.

Захист від кібершпигунства повинен бути реалізований на всіх рівнях. Починаючи від спеціалізованих тренінгів для співробітників і персоналу (наприклад, навчання з кібербезпеки і заходи з розпізнавання підозрілих активностей), закінчуючи підвищенням рівня захищеності серверів, на яких зберігають дані та співпрацею з професіоналами у сфері кібербезпеки.

Наступним видом кіберзлочинів є ***кібершахрайство***. Фактична кінцева ціль кібершахраїв майже така сама, як і у кібершпигунів – отримання персональних даних. Єдина різниця у тому, що кібершпигуни діють непомітно, а кібершахраї – відкрито, а часто навіть нахабно [3].

Злодії, які займаються викраденням даних, зазвичай, отримують особисту інформацію, таку як паролі, номери ID, кредитних карток або номери соціального страхування, та використовують ці дані від імені жертви. Викрадена конфіденційна інформація може бути використана для різних незаконних цілей, зокрема для отримання кредитів, здійснення онлайн-покупок або для отримання доступу до медичних та фінансових відомостей жертви.

Розрізняють наступні найпопулярніші методи кібершахрайства: фішинг, вішинг (телефонне шахрайство), смішинг (або смс-фішинг), байтінг, а також «кетфішинг».

Фішинг – це один з різновидів шахрайства в Інтернеті з метою отримання незаконного доступу до конфіденційних даних користувачів. Для фішингу часто застосовуються підробні веб-сторінки, а також шкідливе програмне забезпечення.

Вішинг – вид шахрайства, при якому зловмисники за допомогою телефонного зв'язку змушують людину повідомити їм свої конфіденційні банківські або персональні дані або стимулюють до здійснення певних дій зі своїм банківським рахунком або банківською картою. Найчастіше шахраї маскуються під служби підтримки банку або ж телефонного оператора.

Смішинг (або смс-фішинг) – злочинна схема спрямована на перехід користувачем за шкідливим посиланням з SMS-повідомлення. Це може бути посилання від ніби-то банку, або ж повідомлення із зламаного акаунта із проханням «проголосувати за дитину у конкурсі».

Байтінг – це техніка соціальної інженерії (метод маніпуляції діями людини), яку використовують зловмисники, при якій жертві підкидають що-небудь, щоб вона почала діяти.

Основними методами захисту від кібершахраїв є і залишається обізнаність та обережність. Варто завжди перевіряти підозрілі посилання, використовувати надійні рішення безпеки для своїх акаунтів та остерігатись підозрілих та занадто привабливих пропозицій.

Під терміном «***кібератака***» відповідно до Закону розуміють спрямовані (навмисні) дії в кіберпросторі, які здійснюються за допомогою засобів електронних комунікацій (включаючи інформаційно-комунікаційні технології, програмні, програмно-апаратні засоби, інші технічні та технологічні засоби і обладнання) та спрямовані на досягнення однієї або сукупності таких цілей: порушення конфіденційності, цілісності, доступності електронних інформаційних ресурсів, що обробляються (передаються, зберігаються) в комунікаційних та/або технологічних системах, отримання несанкціонованого доступу до таких ресурсів; порушення безпеки, сталого, надійного та штатного режиму функціонування комунікаційних та/або технологічних систем; використання комунікаційної системи, її ресурсів та засобів електронних комунікацій для здійснення кібератак на інші об’єкти кіберзахисту. Якщо говорити простіше, то кібератака – це спроба несанкціонованого доступу, пошкодження чи знищення комп’ютерних систем, мереж, програм або інформації [4].

Ці атаки можуть бути спрямовані на отримання конфіденційної інформації, завдання шкоди або порушення нормального функціонування цифрових систем. Кібератаки можуть здійснюватися з використанням вірусів, фішингу, DDoS-атак та інших методів, які використовуються для незаконного доступу чи завдання шкоди в цифровому середовищі.

На сьогоднішній день, в рамках існування гібридної війни із рф, кібератаки становлять найбільшу загрозу для національної безпеки нашої країни. Кібератаки відбуваються мало не кожного дня. Деякі із них агресивні DDoS-атаки, деякі непомітні із використанням вірусів або фішингу. Кіберпідрозділи Національної поліції та Служби безпеки України старанно стоять на сторожі, готові відбивати атаки ворога кожного дня.

Отже, в роботі розкрито поняття трьох різновидів кіберзлочинів, а саме: кібершпигунство, кібершахрайство та кібератаки. Наведено основні методи захисту від них.

Список використаних джерел:

1. Про основні засади забезпечення кібербезпеки України : Закон України від 05.10.2017 № 2163-VIII. *Законодавство України : офіц. вебпортал ВРУ*. URL: https://zakon.rada.gov.ua/laws/show/2163-19 (дата звернення: 19.02.2026).
2. Кібершпигунство. *StopFraud* : [сайт]. URL: https://stopfraud.gov.ua/cybersecurity-in-work/kibershpygunstvo-i315 (дата звернення: 19.02.2026).
3. Кібершахрайство: фішинг, вішинг, смішинг, бейтінг. *Kopirait* : [сайт]. URL: https://kopirait.com.ua/kibershahrajstvo-fishyng-vishyng-smishyng-bejting/ (дата звернення: 19.02.2026).
4. Кібератака. *StopFraud* : [сайт]. URL: https://stopfraud.gov.ua/cybersecurity-in-wartime/kiberataka-i270 (дата звернення: 19.02.2026).

Савчин Євгенія Андріївна
студентка 117_СПД н.гр. ННІ права та психології НАВС

Науковий керівник:
Тарасенко Володимир Петрович
кандидат фізико-математичних наук, доцент кафедри інформаційних технологій ННІ права та психології НАВС

КІБЕРБЕЗПЕКА КРИТИЧНОЇ ІНФРАСТРУКТУРИ: ВИКЛИКИ ІННОВАЦІЙ І ЗАГРОЗ ЦИФРОВИХ ТЕХНОЛОГІЙ

Захист критичної інфраструктури від кіберзагроз є однією з ключових умов забезпечення стабільності та безпеки сучасних держав. Критична інфраструктура включає такі сектори, як енергетика, водопостачання, транспорт, телекомунікації, охорона здоров’я, фінансові послуги та державне управління. Ці системи забезпечують функціонування суспільства і будь-яке порушення їхньої роботи може призвести до значних соціальних та економічних наслідків, таких як перебої в наданні послуг, загроза для життя людей та економічні втрати. Тому кібербезпека відіграє критичну роль у захисті систем від потенційних кіберзагроз.

Метою даного дослідження є вивчення основних принципів і підходів до захисту критичної інфраструктури в умовах сучасних кіберзагроз.

Основні завдання включають аналіз існуючих ризиків, вивчення методів захисту операційних і інформаційних технологій, що використовуються в управлінні критичними об’єктами, та оцінка можливостей застосування новітніх технологій, таких як ШІ і Інтернет речей, для покращення кіберзахисту.