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

ОСНОВНІ ПОНЯТТЯ І КЛАСИФІКАЦІЯ КІБЕРЗЛОЧИННОСТІ

Ляпкін М.Д.
студент 3 курсу 2 групи факультету №1 ННІПКБ ОДУВС
Мельнікова О. О.
викладач кафедри кібербезпеки та інформаційного забезпечення ОДУВС, к.ю.н.

На даний момент існує проблема забезпечення безпеки, а також не санкціонованого доступу до засекречених інформаційних даних, якими неправомірні здобувачі такої інформації можуть скористатися для отримання матеріальної вигоди або задоволення своєї допитливості.

Несанкціоноване отримання такої інформації може завдати шкоду окремим фізичним і юридичним особам, місцевій інфраструктурі, національній економіці а також загальнодержавній безпеці. Наприклад, у грудні 2015 року Туреччина зазнала кібератаку, що вплинула на роботу мереж, які використовуються банками, засобами масової інформації та органами виконавчої влади в країні. В результаті кібератаки на електроенергетичну систему були виведені з ладу системи розподілу електроенергії в нашій державі, залишивши без світла приблизно 230 000 жителів.

Через таку кількість негативних наслідків кібератак їх можна використовувати також для війни, як інформують СБУ "Більшість хакерських атак скерована російськими спецслужбами, які намагаються отримати віддалений доступ до комп'ютерів українських держорганів. Потім вони планують спотворювати чи знищувати дані, поширювати фейки нібито від імені держструктур, а також дискредитувати дії української влади». А отже безпека кіберпростору – це ще один воєнний фронт на якому також потрібно не поступатися зовнішнім ворогам.

І для того щоб забезпечити персонал для боротьби з кіберзлочинністю в Україні спочатку потрібно визначити основні поняття.

Кіберпростір – це Інтернет мережа в якій за допомогою електронно-обчислювальної техніки здійснюється спілкування людей.

Кіберзлочин – це вид правопорушення, що вчиняється із застосуванням електронно-обчислювальної техніки і полягає в викраденні секретної інформації яка зберігається на електронних засобах накопичення інформації. Він вчиняється як правило для шантажу або на замовлення, може здійснюватись як одноособово, так і за участю груп осіб.

Найбільш страшніше те, що з розвитком електронно-обчислювальної техніки, хоча і розвиваються засоби захисту від кібератак, цей розвиток допомагає правопорушникам отримувати нові засоби та методи обходу безпеки.

Сьогодення для здійснення кібератак непотрібні знання в сфері інформаційних технологій, тому що кожна особа з відповідним програмним забезпеченням може здійснювати кібератаки, простота здійснення таких атак створює напруженість засобів забезпечення безпеки що може створювати вразливості.

Злочинці вигадали багато способів використання вразливостей серед них поширеним є фішинг – це більш схоже на шахрайство, коли цілям атак відправляються повідомлення від імені відомих компаній або організацій які визивають довіру, однак вони є підробленими. Ціль фішингу – отримання конфіденційної інформації від користувачів (паролів, логінів, даних особових рахунків і банківських карт). У листах особу ввічливо просять оновити чи підтвердити правильність персональної інформації або інформують про які-небудь проблеми з даними, а після цього направляють на підроблений сайт, де необхідно ввести облікові дані. Якщо потерпіла особа вводить свої дані на таких сайтах, то злочинцям стають відомі ці дані та вони можуть використати їх з метою крадіжки персональних даних, персональних коштів або іншого. Фішинг є одним з найпоширеніших видів кібератак.

Вірус – це комп'ютерна програма, яка встановлюється без відома та проти волі користувача на його комп'ютер або інший пристрій, а також здатна до самокопіювання. Вірус можна отримати різними способами. Наприклад, зберігатися на інтернет сторінках чи поштових скринях. Також вірус буває вбудований у завантажену програму, яка «випускає» вірус на волю, після встановлення або запуску такої програми. Після чого вірусна програма може заблоковувати доступ до файлів або операційну систему.

Соціальна інженерія – це спосіб отримання інформації від користувачів, полягає у застосуванні шахраями тактики, завдяки якій вони переконують «жертву» розкрити конфіденційну інформацію. Тактики можуть бути різними: від видавання себе за співслужбовця, знайомого або друга до різноманітних погроз із вимогою встановити програмне забезпечення.

Шкідливе програмне забезпечення – до таких програм належать так звані «трояни», програми-шпигуни. Достатньо часто вони встановлюються разом з іншою, корисною програмою, яку вирішила завантажити «жертва». Такі програми можуть таємно записувати всі натискання на клавіші, читати файли на жорсткому диску і дані браузера.

Злом – це цілеспрямована діяльність, спрямована на проникнення у бази даних або систему шляхом обходу встановленого механізму безпеки.

У Кримінальному кодексі України ці злочини закріплено в розділі 16 «Кримінальні правопорушення у сфері використання електронно-обчислювальних машин, їх систем та комп'ютерних мереж і мереж електрозв'язку» і представлено такими нормами:

ст. 361 – несанкціоноване втручання в роботу електронно-обчислювальних машин, автоматизованих систем, комп'ютерних мереж чи мереж електрозв'язку;

ст. 361-1 – створення з метою використання, розповсюдження або збуту шкідливих програмних чи технічних засобів, а також їх розповсюдження або збут;

ст. 361-2 – несанкціоновані збут або розповсюдження інформації з обмеженим доступом, яка зберігається в електронно-обчислювальних машинах (комп'ютерах), автоматизованих системах, комп'ютерних мережах або на носіях такої інформації;

ст. 362 – несанкціоновані дії з інформацією, яка оброблюється в електронно-обчислювальних машинах, автоматизованих системах, комп'ютерних мережах або зберігається на носіях такої інформації, вчинені особою, яка має право доступу до неї;

ст. 363 – порушення правил експлуатації електронно-обчислювальних машин автоматизованих систем, комп'ютерних мереж чи мереж електрозв'язку або порядку чи правил захисту інформації, яка в них оброблюється;

ст. 363-1 – перешкоджання роботі електронно-обчислювальних машин автоматизованих систем, комп'ютерних мереж чи мереж електрозв'язку шляхом масового розповсюдження повідомлень електрозв'язку.

В Україні доволі часто трапляються кібератаки, що свідчить про непідготовленість органів щодо забезпечення безпеки у інформаційному просторі, на нашу думку це пов’язано, по перше, швидкістю розвитку техніки, хакерів та методів злому – це означає, що інформація про них застаріває і потрібно стежити за її актуальністю та підвищувати рівень обізнаності у цій сфері, по друге залучати спеціалістів тому, що найчастіше вразливість є не в самій системі а в особах які її використовують, підвищити загальнонаціональну обізнаність як захистити себе та свої дані.

Ця проблема стосується не тільки України а також і багатьох інших держав. Яскраві приклади: Stuxnet є спеціалізованою розробкою спецслужб Ізраїля та США, спрямованою проти ядерного проекту Ірану. Це перший відомий комп'ютерний червяк, що перехоплює та модифікує інформаційний потік між програмованими логічними контролерами марки Simatic S7 та робочими станціями SCADA-системи Simatic WinCC фірми Siemens. Таким чином, червяк може бути використаний як засіб несанкціонованого збору даних (шпигунства) та диверсій.

В епоху швидкого й активного розвитку електронно-обчислювальної техніки вони стають невід'ємною складовою життя суспільства, робочих процесів і діяльності державних органів та юридичних осіб, а тому особливу увагу слід приділити заходам підвищення безпеки в інформаційному просторі.

Література

1. Кримінальний кодекс України: закон України від 05. 04. 2001 р. № 2341-III : за станом на 07. 03. 2018 р. № 2292-19. URL: http://zakon2.rada.gov.ua.
2. Закон України «Про інформацію» від 02.10.1992 № 2657-12. URL: http://zakon.rada.gov.ua/laws/show/2657-12
3. Ліпкан В.А. Систематизація інформаційного законодавства України : монографія / В. А. Ліпкан, В. А. Залізняк ; за заг. ред. В. А. Ліпкана. К. : О. С. Ліпкан, 2012. 304 с.

ЗМІСТ

СЕКЦІЯ 1.
ПРАВОВЕ РЕГУЛЮВАННЯ ЗАБЕЗПЕЧЕННЯ КІБЕРБЕЗПЕКИ В УКРАЇНІ

СЕКЦІЯ 2.
АДМІНІСТРАТИВНО-ПРАВОВЕ ЗАБЕЗПЕЧЕННЯ КІБЕРБЕЗПЕКИ В УКРАЇНІ