1. URL : https://subj.ukr-lit.com/osnovi-informacijno-analitichno%D1%97-diyalnosti-zaxarova-i-v-5-2-informacijno-analitichni-poslugi-riznovidi-xarakteristika/
2. URL : http://megalib.com.ua/book/22_Informaciino_analitichna_diyalnist. html
3. URL : https://r.donnu.edu.ua/bitstream/123456789/1516/1/22_%D0%9C%D0%B0%D0%BA%D0%B5%D1%82_%D0%9A%D0%BE%D0%B2%D0%B0%D0%BB%D1%8C%D1%81%D0%BA%D0%B0%D1%8F_%D0%86%D0%90%D0%94.pdf

ПАШКЕВИЧ Ольга
здобувач вищої освіти 3 курсу
спеціальність 262 «Правоохоронна діяльність» факультету підготовки фахівців для підрозділів кримінальної поліції
ЧОРНА Аліна
старший викладач кафедри кримінального права та кримінології Дніпропетровського державного університету внутрішніх справ

ЗАПОБІГАННЯ ЗЛОЧИННОСТІ У СФЕРІ ІНФОРМАЦІЙНИХ ТЕХНОЛОГІЙ В УМОВАХ ВОЄННОГО СТАНУ

У зв’язку з повномасштабним вторгненням рф в Україну 24 лютого 2022 року в Україні введено воєнний стан[1].Дана тема наразі є особливо актуальною в Україні, адже в умовах воєнного стану кіберзлочинці активно займаються зломом державних серверів, дезінформацією населення, використанням фейкових профілів у соціальних мережах. На сьогодні широко поширені кібершахрайства, під час яких зловмисники під виглядом різноманітних платежів мають намір дізнатися банківські реквізити громадян, щоб заволодіти грошима. Визначення поняття «Злочинність у сфері інформаційних технологій»- це сукупність правопорушень, які вчиняються за допомогою комп’ютерних систем, мереж та програмного забезпечення з метою незаконного доступу до інформації, крадіжки даних, шахрайства, поширення шкідливих програм тощо.

Вивченням історичного походження та причин злочинності у сфері інформаційних технологій, розвитку цього виду системи запобігання злочинності дослідники почали займатися порівняно недавно. До таких вчених можна віднести О.С. Алавердова, Ю.М. Батуріна, П.Д. Біленчука, А.В. Войцехівського, М.Д. Діхтяренка, К.Ю. Ісмайлова, С.М. Круля та ін.

Варто зазначити, що кіберзлочинність, порівняно з традиційними видами злочинності в Україні (вбивства, корисливі кримінальні

правопорушення тощо), є відносно новим явищем і найбільшою загрозою XXI століття водночас, адже інформаційні технології також є способом вчинення багатьох традиційних кримінальних правопорушень[2, с.442]. Такий злодій стає бойовою силою, а основним його засобом є кібератаки та хакерство. Зокрема, в умовах війни інформаційний простір використовуватимуть не лише супротивники для підриву обороноздатності України, а й можуть зазнати атак ті, хто прагне нажитися на ситуації перевантаженості правоохоронних органів. Із кожним днем кількість кіберзлочинів зростає, і їх кількість значно зростає. Збільшуються нові види злочинів, кожен з яких вимагає вибору відповідного методу боротьби, але це створює певні проблеми. Основна причина полягає в тому, що кіберзлочинців набагато важче зловити, ніж звичайних злочинців.

Після повномасштабного вторгнення рф на територію України різко зросла кількість злочинів у сфері інформаційних технологій. Держава-агресор використовує інтернет-технології для поширення дезінформації, ворожої ідеологічної пропаганди про вторгнення в Україну. Тому відбулося удосконалення притягнення до кримінальної відповідальності таких злочинців і зміни в законодавстві відбулися саме в Законі України «Про внесення змін до Кримінального кодексу України щодо підвищення ефективності боротьби з кіберзлочинністю в умовах дії воєнного стану» від 24.03.2022 №2149-IX внесено зміни до Розділу XVI [3]. Передбачається кримінальна відповідальність в ч.1 ст.361 за несанкціоноване втручання в роботу інформаційних (автоматизованих), електронних комунікаційних, інформаційно-комунікаційних систем, електронних комунікаційних мереж; в ч.2 ст.361 вчинені повторно або за попередньою змовою групою осіб. Раніше дії передбачені в ч.1 ст.361 вважалися основним складом кримінального правопорушення, а тепер ч.3 ст.361 стали його особливо кваліфікованим складом. Тож відповідні зміни стосуються посилення кримінальної відповідальності за злочини у сфері інформаційних технологій та розширення обмежень щодо діяльності правоохоронних органів щодо розкриття таких злочинів.

Зрозуміло, що Україна перебуває на ранніх етапах впровадження інституцій та механізмів у сфері кібербезпеки, але вже створено певну законодавчу базу, яку необхідно дотримуватися та вдосконалювати. З розвитком інформаційних технологій кіберзлочинність також покращилася, і вона проявляється в різних сферах особистого життя та діяльності, а також суспільства в цілому.

Аби запобігти таким злочинам потрібно встановити сучасні засоби кіберзахисту, які допоможуть виявити та запобігти кібератакам, це може включати використання антивірусного програмного забезпечення, систем виявлення вторгнень та інших заходів.Також навчання та підвищення кваліфікації: організовувати навчальні курси та семінари для спеціалістів у галузі кібербезпеки.Це допоможе покращити їхні навички та знання, а також

підготувати нових фахівців. Важливим залишається співпраця з правоохоронними органами, важливо підтримувати співпрацю з поліцією та іншими правоохоронними органами, це допоможе виявити та розслідувати злочини у сфері інформаційних технологій. Встановити ефективну систему відповідальності. Законодавство повинно передбачати відповідальність за злочини у сфері інформаційних технологій. Це може включати штрафи, покарання та інші більш серйозніші санкції.

Отже, запобігання злочинності в сфері інформаційних технологій є важливим завданням, особливо в умовах воєнного стану. Україна потребує подальшого розвитку своїх інформаційних технологій, оскільки такі злочинці принаймні на крок випереджають механізми, які мають відповідні державні інституції для боротьби з цим видом злочинності. Тому лише завдяки належному рівню, можливе нормальне функціонування мереж і систем, які з кожним днем все більше і більше інтегруються в наше соціальне життя.

1. Про введення воєнного стану в Україні: Указ Президента України № 64 від 24.02.2022 р. URL : https://www.president.gov.ua/documents/642022-41397.

2. Бодунова О.М Історико-правові аспекти виникнення злочинності у сфері інформаційних технологій. Електронне наукове видання «Аналітично-порівняльне правознавство». 2023 р. С.441-445

3. Закон України «Про внесення змін до Кримінального кодексу України щодо підвищення ефективності боротьби з кіберзлочинністю в умовах дії воєнного стану» 2149- IX від 24.03.2022 р. URL : https://zakon.rada.gov.ua/laws/show/2149-20#Text

ПЕКАРСЬКИЙ Сергій
к. ю. н., доцент, доцент кафедри оперативно-розшукової діяльності та інформаційної безпеки факультету № 3 Донецького державного університету внутрішніх справ

БАЗА ДАНИХ «РОЗШУК» У ДІЯЛЬНОСТІ ПІДРОЗДІЛІВ КРИМІНАЛЬНОЇ ПОЛІЦІЇ

В умовах повномасштабної агресії росії проти України актуалізувалося питання розшукової роботи підрозділів кримінальної поліції Національної поліції України. Починаючи з кінця лютого 2022 року підрозділи кримінальної поліції у складі сил безпеки та оборони залучаються до проведення безпекових та стабілізаційних заходів. На нашу думку доцільним