ключову роль у спрощенні координації та оптимізації діяльності цих бот-мережей, роблячи їх більш потужними та важкими для розуміння загрозами.

Незважаючи на потенційні загрози, пов'язані з використанням штучного інтелекту, він також може мати позитивний вплив на захист критичної інфраструктури. Штучний інтелект може допомогти виявити аномалії мережі та аномальну активність. Це може вказувати на кібератаку. Він також може бути використаний для прогнозування майбутніх загроз та підготовки до можливих атак. Автоматизовані системи, побудовані на основі штучного інтелекту, можуть швидко реагувати на кібератаки, блокувати шкідливі дії та відновлювати системи.

Щоб ефективно використовувати штучний інтелект для захисту критичної інфраструктури, необхідно враховувати кілька аспектів. Розробка надійних моделей і алгоритмів, здатних розпізнавати нові типи загроз, є важливим завданням. Також необхідно захистити сам ШІ від атак і маніпуляцій, щоб уникнути помилкових рішень і неправильного використання систем захисту.

Також важливо враховувати питання конфіденційності та етики при використанні штучного інтелекту для збору та обробки даних. Необхідно забезпечити належний рівень захисту та конфіденційності інформації про критично важливу інфраструктуру.

Загалом, штучний інтелект може бути потужним інструментом захисту критичної інфраструктури, але його використання вимагає комплексного підходу, ретельної оцінки ризиків та застосування відповідних заходів безпеки для забезпечення надійності та захисту системи.

Література

1. Що потрібно знати про штучний інтелект. bizmag. URL: http://surl.li/nppkr
2. Що таке інфраструктура: чим цивільна відрізняється від критичної. fakty. URL: https://fakty.com.ua/ua/ukraine/20221101-shho-take-infrastruktura-chym-czyvilna-vidriznyayetsya-vid-krytychnoyi/

Антощук С. А.

курсант факультету № 4 Харківського національного університету внутрішніх справ

Лучик В. Є.

професор кафедри протидії кіберзлочинності факультету № 4 Харківського національного університету внутрішніх справ, доктор економічних наук, професор

КІБЕРШАХРАЙСТВО В УКРАЇНІ В УМОВАХ ВІЙНИ

Галузь інформаційних технологій вимагає від зловмисника відповідних навичок, але вчиняти такі злочини може практично будь-хто, хто має вільний доступ до інтернету – кібершахрайство є абсолютно новим явищем, оскільки воно безпосередньо пов'язане з останніми досягненнями.

Українці воюють в інформаційному просторі, так як і на полі бою з 24 лютого 2022 року. Через вплив війни на свідомість та поведінку людей їх дії в більшості випадків є протиправними. В період війни не лише ворог провокує інформаційні атаки для підриву обороноздатності України, але й також ті, хто прагне скористатися перенавантаженістю правоохоронних органів і нажитися на коштах громадян. За перші півтора місяці війни кіберзлочинність в Україні неухильно зростала.

Зростання кількості онлайн-шахраїв, які маніпулюють вразливими українцями та іноземцями, є нагальною проблемою, з якою бореться наша правоохоронна система. Як наслідок, кіберзлочинність, зокрема, онлайн-шахрайство, зростає.

За статистикою, за 10 місяців 2023 року облікували 73160 кримінальних проваджень за ст. 190 про шахрайство. Цьогоріч зафіксували в 1,3 рази більше випадків, аніж загалом за попередні два 2021-2022 роки – 55933. Натомість від початку осені відкритих проваджень про шахрайство істотно поменшало на 17%. Восени середня кількість нових проваджень зменшилася на 17%.

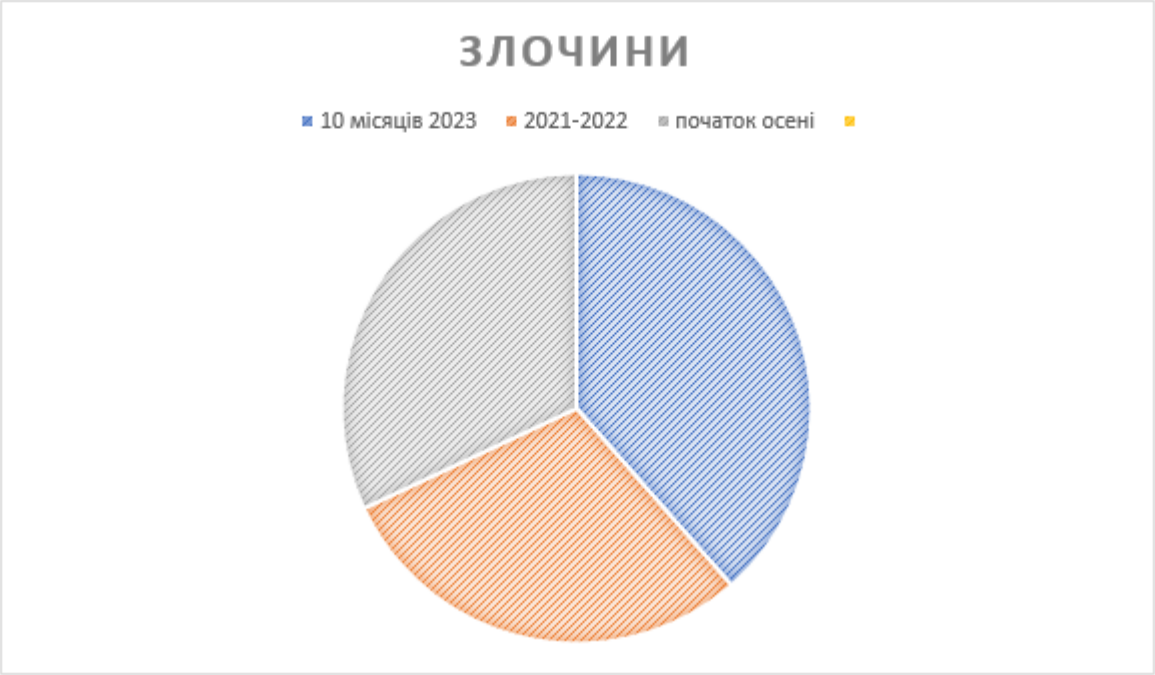

Рис. 1. Статистика скоєння кіберзлочинів за 2021-2023рр.

Відповідно до Кримінального кодексу України шахрайство – це заволодіння чужим майном або придбання права на майно шляхом обману чи зловживання довірою (ст.190 КК України). Здійснення даного кримінального правопорушення в інтернеті науковці називають «кібершахрайством».

Відповідно до п. 8 ч. 1 ст. 1 [2], кіберзлочин (комп'ютерний злочин)– суспільно небезпечне винне діяння у кіберпросторі та/або з його використанням, відповідальність за яке передбачена законом України про кримінальну відповідальність (ККУ) та/або яке визнано злочином міжнародними договорами України. До того ж це кримінальні правопорушення, передбачені розділом XVI КК України («Злочини у сфері використання електронно-обчислювальних машин (комп'ютерів, систем та комп'ютерних мереж і мереж електрозв'язку»), та зареєстровані кримінальні провадження із кваліфікуючою відміткою в картці про кримінальне правопорушення – «з використанням високих інформаційних технологій і телекомунікаційних мереж».

Війна в інформаційному просторі завдає такої ж шкоди, як і на полі бою. Після початку війни парламент покращив Кримінальний та Кримінально-процесуальний кодекси, вдосконаливши підстави та процесуальні механізми притягнення до відповідальності кіберзлочинців. Ці зміни сконцентровані у двох законодавчих актах [4],[5].

Дійсно, посилення відповідальності за правопорушення, перелічені у відповідному законодавстві, підвищило ефективність боротьби з кіберзлочинністю.Розширення сфери діяльності правоохоронних органів, які розслідують кіберзлочини, посилення санкцій та додаткова криміналізація певних діянь стримують потенційних шахраїв, але

проблема полягає в тому, що кримінологічні дослідження ґрунтуються майже виключно на кримінальних даних, тоді як дослідження соціальних, економічних, політичних, демографічних, організаційних та інших причин кібершахрайства є відсутність таких досліджень є проблемою.

Більшість випадків шахрайства сталися під час купівлі або продажу товарів онлайн (52,7%). Наступними за поширеністю були фішингові посилання (18,6%). Наступними за поширеністю були злом акаунтів у соціальних мережах (12%) та телемаркетинг (10,2%).

Особи, винні у порушенні законодавства у сферах національної безпеки, електронних комунікацій та захисту інформації, якщо кіберпростір є місцем та/або способом здійснення кримінального правопорушення, іншого винного діяння, відповідальність за яке передбачена цивільним, адміністративним, кримінальним законодавством, несуть відповідальність згідно із законом.

Висновки. Таким чином, боротьба з кібершахрайством в Україні здійснюється за трьома основними напрямами, а саме: запобігання кіберзлочинам; загальна організація боротьби з кіберзлочинністю; застосування кримінальної відповідальності та покарання осіб, які вчиняють кіберзлочини.

Література

1. Відкриті дані Опендатабот з посиланням на дані Генеральної прокуратури України. https://uworld.news/news/shakhrai-staly-aktyvnishymy-nizh-do-1006442.html
2. Про основні засади забезпечення кібербезпеки України : Закон України від 05 жовт. 2017 No 2163-VIII. https://zakon.rada.gov.ua/laws/show/2163-19#Text
3. Левківська Я. І. Вплив воєнного стану на трансформування та розвиток інтернет-шахрайства в Україні. http://dspace.onua.Edu.ua/handle/11300/19993
4. «Про внесення змін до Кримінального процесуального кодексу України та Закону України «Про електронні комунікації» з питання підвищення ефективності досудового розслідування «за гарячими слідами» та протидії кібератакам» No 2137-IX від 15 березня 2022 року. https://ips.ligazakon.net/document/view/T222137?an=1
5. Про внесення змін до Кримінального кодексу України щодо підвищення ефективності боротьби з кіберзлочинністю в умовах дії воєнного стану від 24.02.2022 No 2149-IX. https://zakon.rada.gov.ua/laws/show/2149-20#Text.
6. Стаття 12 із змінами, внесеними згідно із Законом України від 17.06.2020 р. N 720-IX. https://zakon.rada.gov.ua/laws/show/720-20#Text.

Баб'як А. В.

завідувач кафедри оперативно-розшукової діяльності факультету №2 ІПФПНП Львівського державного університету внутрішніх справ, кандидат юридичних наук, доцент

ІНФОРМАЦІЙНО-АНАЛІТИЧНЕ ЗАБЕЗПЕЧЕННЯ ОПЕРАТИВНИХ ПІДРОЗДІЛІВ НАЦІОНАЛЬНОЇ ПОЛІЦІЇ

Вдосконалення інформаційно-аналітичного забезпечення оперативно-розшукової діяльності є одним із напрямів підвищення результатів діяльності оперативних підрозділів Національної поліції. Над окресленою проблемою працює чимало