реалізований через верховенство правової культури людей.

*Література*

1. Моніна Т., Купчак М.Я. Еволюція явища корупції: історичний ракурс. URL: https://sci.ldubgd.edu.ua/bitstream/123456789/6617/1/.

2. Грищук М. Передумови виникнення та протидії корупції: історико-правові аспекти. URL: http://dspace.wunu.edu.ua/bitstream/316497/38751/1.pdf.

3. Реалізація державної антикорупційної політики в міжнародному вимірі комплексу. URL: http://elar.naiau.kiev.ua/bitstream/123456789/5096/1/.

УДК 342.951:351.82 + 32.019.51(043.2)

**Криволап Є.В.,** здобувач вищої освіти
третього (освітньо-наукового) рівня,
Національний авіаційний університет, м. Київ, Україна

## АДМІНІСТРАТИВНО-ПРАВОВІ ЗАСАДИ ВИЯВЛЕННЯ ТА ПРОТИДІЇ ВРАЗЛИВОСТЯМ ІНФОРМАЦІЙНО-КОМУНІКАЦІЙНИХ СИСТЕМ НА ПІДСТАВІ МЕТОДІВ BUG BOUNTY (БІЛИЙ ХАКІНГ) В УКРАЇНІ

Сьогодні практично жодна сфера людської діяльності не обходиться без використання інформаційних технологій. Але повсюдна інформатизація стала приводом для зловмисників атакувати комп'ютерні інформаційні системи. Таким чином кібератаки стали звичайною справою [1, с. 41-42]. Подальша ворожа діяльність російської федерації проти України ставить завдання приділяти суттєву увагу її захисту від хакерських атак російських проксі-груп.

У цьому контексті заслуговують на увагу останні перспективні нормативно-правові напрацювання у законодавчому полі України. Так, для підвищення ефективності виявлення вразливостей в Україні протягом 2022-2023 рр. офіційно запроваджена так звана система bug bounty – це тестування електронних сервісів із залученням зовнішніх фахівців, яке дає можливість виявити вразливі місця і недоліки в програмних продуктах [2]. Процедура по суті заохочує так званих «білих» хакерів на договірній основі атакувати певні системи з метою перевірки їх стійкості до таких атак і пошуку вразливостей. За знайдені помилки пропонується винагорода. Це дозволяє розробникам усунути помилки, перш ніж ці помилки можуть бути використані у ворожих цілях [3].

Офіційне запровадження даної системи в Україні здійснювалося у 2 етапи [2]. На першому етапі були внесені відповідні зміни у Кримінальний кодекс (КК) України. Так, стаття 361 КК України визнавала кримінально караним «несанкціоноване втручання в роботу інформаційних (автоматизованих), електронних комунікаційних, інформаційно-

комунікаційних систем, електронних комунікаційних мереж. Разом із тим, Законом України від 24.03.2022 року № 2149-IX «Про внесення змін до Кримінального кодексу України щодо підвищення ефективності боротьби з кіберзлочинністю в умовах дії воєнного стану» стаття 361 КК України була доповнена частиною 6, відповідно до якої дії, передбачені цією статтею, не вважаються несанкціонованим втручанням в роботу інформаційних (автоматизованих), електронних комунікаційних, інформаційно-комунікаційних систем, електронних комунікаційних мереж, *якщо вони були вчинені відповідно до порядку пошуку та виявлення потенційних вразливостей таких систем чи мереж*. На другому етапі запровадження системи Bug bounty Кабінет Міністрів України постановою Кабінету Міністрів України від 16.05.2023 р. № 497 затвердив Порядок пошуку та виявлення потенційної вразливості інформаційних (автоматизованих), електронних комунікаційних, інформаційно-комунікаційних систем, електронних комунікаційних мереж (далі – Порядок № 497). Цей Порядок визначає механізм здійснення пошуку та виявлення потенційної вразливості інформаційних (автоматизованих), електронних комунікаційних, інформаційно-комунікаційних систем, електронних комунікаційних мереж. Дія цього Порядку не поширюється на інформаційні (автоматизовані), електронні комунікаційні, інформаційно-комунікаційні системи, електронні комунікаційні мережі, в яких обробляється службова інформація та/або інформація, що становить державну таємницю, розвідувальну таємницю, банківську таємницю.

Пошук потенційної вразливості системи здійснюється на підставі публічної пропозиції. Публічна пропозиція оприлюднюється власником системи на власному офіційному веб-сайті. Публічна пропозиція розробляється власником системи або координатором відповідно до примірної публічної пропозиції про здійснення пошуку та виявлення потенційної вразливості інформаційних (автоматизованих), електронних комунікаційних, інформаційно-комунікаційних систем, електронних комунікаційних мереж і методичних рекомендацій з розроблення публічної пропозиції про здійснення пошуку та виявлення потенційної вразливості інформаційних (автоматизованих), електронних комунікаційних, інформаційно-комунікаційних систем, електронних комунікаційних мереж, що затверджуються Адміністрацією Держспецзв'язку. Така Примірна публічна пропозиція, а також Методичні рекомендації з розроблення публічної пропозиції, затверджені Наказом від 14.07.2023 № 599 Адміністрації Державної служби спеціального зв'язку та захисту інформації України.

Крім інформації та положень, які передбачені безпосередньо Порядком № 497, у Методичних рекомендаціях передбачені підходи до визначення винагороди дослідника, яку визначає власник системи і якщо така винагорода передбачається, у системному зв'язку із виявленими

вразливостями системи. Винагородою може бути: матеріальний подарунок (речі з особливим написом, такі як футболка, чашка, кепка, наплічник тощо); певна сума коштів у національній валюті; інше. Винагорода встановлюється відповідно до категорії виявленої вразливості.

У разі відсутності винагороди власник системи або координатор (у разі його залучення) може заохочувати дослідника, висловлюючи подяку на власному офіційному вебсайті, або здійснювати заохочення будь-яким іншим способом. Також може висловлюватися подяка досліднику, який надав звіт про вразливість, яку було знайдено раніше, або подяка за звіт про вразливість, за яку не передбачена винагорода. Такі повідомлення про подяку висловлюються за згодою дослідника. Власник системи або координатор (у разі його залучення) зазначає випадки, у разі яких винагорода не виплачується. Першочергово це може стосуватися вразливостей в апаратному забезпеченні, операційних системах, драйверах системи, а також некоректних випадків опису вразливості у звіті без детального опису вектора атаки та доказів потенційного завдання збитку або шкоди.

*Література*

1. Філінович В.В. Кібербезпека та загрози авіаційній сфері: правовий аспект. Наукові праці Національного авіаційного університету: Серія «Юридичний вісник. Повітряне і космічне право». 2021. № 3 (60). С. 38-43.

2. Криволап Є.В., Юринець Ю.Л., Бєлкін Л.М. Питання нейтралізації вразливостей інформаційно-комунікаційних систем цивільної авіації: правовий аспект. Наукові праці Національного авіаційного університету: Серія «Юридичний вісник. Повітряне і космічне право». 2023. № 3 (68). С. 16-23.

3. Bug bounty program. From Wikipedia, the free encyclopedia. URL: https://en.wikipedia.org/wiki/Bug_bounty_program

УДК 347.73(043.2)

**Кузьмін А.Р.,** здобувач вищої освіти
третього (освітньо-наукового) рівня,
Національний авіаційний університет, м. Київ, Україна

## МЕХАНІЗМИ ФІНАНСОВОЇ ПІДТРИМКИ УКРАЇНЦІВ В КОНТЕКСТІ ДІЯЛЬНОСТІ МІЖНАРОДНИХ ФІНАНСОВИХ ОРГАНІЗАЦІЙ У ВОЄННИЙ ПЕРІОД

Україна, яка на сьогодні є багатонаціональною країною, стикається з внутрішніми та зовнішніми складнощами з часу російської агресії у лютому 2022 року. Однією з цих проблем стало масове переміщення громадян; їхній виїзд на постійне чи тимчасове проживання в інших країни. Велика кількість українців обрали шлях біженців, прагнучи знайти