частини тіл; предмети, вилучені з місця події: військова техніка, автомобілі, зброя, боєприпаси тощо; 3) проведення слідчих (розшукових) дій потребує залучення великої кількість спеціалістів, зазвичай, вузькопрофільних: вибухотехніків, балістів, знавців зброї, знавців ракетної та авіаційної техніки, артилеристів, механіків, пожежників або працівників ДСНС для огляду місця пожежі, кінологів зі службовими собаками, судово-медичних експертів або лікарів для огляду трупів, спеціалістів-біологів для відбирання зразків ДНК та ін.; 4) складність і небезпека участі спеціаліста у проведенні слідчої (розшукової) дії на певних територіях потребує застосування для відео-, фотофіксації спеціальних засобів (БПЛА) та ін.

Перелік джерел посилання

1. Єдиний державний хаб зі збору доказів воєнних злочинів. URL: https://warcrimes.gov.ua/?fbclid=IwAR2wy_upbhJm_wETWAij57DsooCxnSsNKBidlywazvpMJ2szPw5BvGFZc5g (дата звернення: 14.09.2023).
2. Шепітько В. Ю. Проблеми використання спеціальних знань крізь призму сучасного кримінального судочинства в Україні. *Судова експертиза*. 2014. № 1. С. 11—18.

Шахрайство в інтернеті. Проблемні аспекти державного регулювання

Григорій Іваненко,
Сумський НДЕКЦ МВС України, м. Суми, Україна, e-mail: ivanenko299@gmail.com
Світлана Іванова,
Сумський НДЕКЦ МВС України, м. Суми, Україна

Мета доповіді — розкрити проблемні аспекти державного регулювання інтернет-шахрайства, нові шляхи розв'язання проблем з урахуванням сучасних вимог. Висвітлено специфіку розслідування цієї категорії злочинів, вплив девіантної поведінки потерпілого як каталізатору негативного прогресу. Розглянуто світову практику щодо державного контролю у частині реєстрації мобільних пристроїв, ґаджетів та ін. Співставлено право особи на приватність інформації та необхідність удосконалення системи контролю та захисту такої інформації відповідно до сучасних стандартів.

Ключові слова*: інтернет-шахрайство; латентність; доказова база; оперативність; державне регулювання; приватність.*

Fraud on the Internet. Problematic aspects of state regulation

Gregory Ivanenko, Svetlana Ivanova

This report purpose is to reveal problematic aspects of state regulation of Internet fraud, new ways of solving issues taking into account modern requirements. Investigation specifics of this category of crimes, influence of victim's deviant behavior as a catalyst for negative progress are also highlighted. The world practice regarding state control in terms of registration of mobile devices, gadgets, etc. was considered. The individual's right to privacy of information and the need to improve the system of control and protection of such information in accordance with modern standards are compared.

Keywords*: Internet fraud; latency; evidence base; efficiency; state regulation; privacy.*

Діджиталізація міцно увійшла в усі сфери життя громадян нашої держави. Звичною стала реалізація соціальних потреб через інтернет: спілкування, навчання, купівля-продаж та ін. Саме задоволення людиною базових потреб шляхом використання інтернет-ресурсів є «благодатним ґрунтом» для діяльності віртуальних злодіїв.

На сьогодні інтернет-шахрайство має вагому частку з-поміж злочинів загальнокримінальної спрямованості, тому слід з'ясувати, що таке шахрайство в інтернеті та які особливості його кваліфікації й розслідування.

Згідно зі ст. 190 Кримінального процесуального кодексу України, шахрайство — це заволодіння чужим майном або придбання права на майно шляхом обману чи зловживання довірою [1]. Коли йдеться про інтернет-шахрайство, акцентують увагу на

основній складовій цього злочину — віртуальності, яка від початку розслідування злочинів цієї категорії є перешкодою у формуванні доказової бази, пошуку зачіпок, конкретних відомостей тощо. У випадку з інтернет-шахраями доказова база, яку має слідчий, зазвичай зводиться до мінімуму — усного пояснення потерпілої сторони. Це може додатково обтяжуватися девіантною складовою поведінки потерпілого, зумовленою соціально-економічними чинниками (безробіттям, низьким рівнем життя, обмеженістю відповідальної усвідомленості та ін.). Тому через мінімум даних на початковій стадії розслідування втрачається оперативність у збиранні вкрай необхідної інформації (зокрема, отримання тимчасового доступу до речей і документів інтернет-провайдера з метою визначення облікового запису (записів) злодія або тимчасового доступу до речей і документів оператора мобільного зв'язку з метою отримання роздруківок дзвінків та прив'язок до базових станцій, їх місцезнаходження та ін.).

До того ж латентність цього виду злочину може стати каталізатором негативного прогресу: доволі хитка ймовірність повернути втрачені кошти чи майно підштовхує потерпілого до так званого «пасивного опору» — замовчування, небажання вчасно звертатися до правоохоронних органів, схильність перекладати відповідальність на органи поліції. Своєю чергою, ланцюгова реакція такої бездіяльності призводить до зростання аналогічних злочинів, адже допомагає злочинцю уникнути подальшого покарання, провокує його на вчинення нових протиправних діянь, спираючись лише на примітивний потяг наживи. Водночас такі самі спонукання (корисливість і бажання легкої наживи) знову підштовхують і потенційних жертв на нові «пригоди».

Дослідивши негативну тенденцію зростання кількості інтернет-шахрайств і замкненість цього процесу, можна дійти висновку про відсутність належного регулятора, роль якого має виконувати держава.

На сьогодні позиція державного втручання у припинення онлайн-злочинів межує між регулятором і провокатором. З одного боку, створено механізм розслідування, установлення істини, покарання, а з іншого — відсутня відповідність сучасним вимогам. Реалії сьогодення вимагають від органів поліції максимально швидкого та якісного реагування на такого роду злочини, їх профілактику та протидію.

На нашу думку, одним із методів подолання проблеми, що склалася, є введення інституту реєстру IMEI-кодів, блокування пристрою, код якого не внесено до зазначеного реєстру, та використання паспортних даних під час купівлі SIM-карти. Наприклад, станом на 2013 р. у близько 80 країнах світу було запроваджено обов'язкову реєстрацію абонентів мобільного зв'язку за паспортом, тому контроль через реєстрацію є загальновживаною практикою. Зокрема, у Грузії для купівлі SIM-карти слід обов'язково завітати до салону компанії-постачальника мобільного зв'язку, де лише після надання паспортних даних можна придбати картку; зазвичай термін дії такої картки не перевищує півтора року. У Білорусі абоненти-іноземці також можуть купити SIM-картку, тільки пред'явивши паспорт і заповнивши спеціальну анкету, після цього можна користуватися мережею за допомогою гостьового тарифу [2].

У Конституції України чітко закріплено право на приватність, до якого апелюють противники запровадження такого режиму. Проте ми вважаємо, що реальний стан контролю у сфері захисту приватної інформації від публічного доступу не відповідає сучасним стандартам, упровадження яких допомогло б якісно зменшити рівень онлайн-злочинності.

Перелік джерел посилання

1. Кримінальний кодекс України від 05.04.2001 р. № 2341-III (зі змін. та допов.). URL: https://zakon2.rada.gov.ua/laws/show/2341-14/page#Text (дата звернення: 01.09.2023).
2. Глуховський М. SIM-картка за паспортом. Усі «за» і «проти» / Главком. 10.08.2017. URL: https://glavcom.ua/publications/sim-kartka-za-pasportom-usi-za-i-proti-430454.html (дата звернення: 01.09.2023).