яким здійснюється досудове розслідування. Таким чином, можна дійти до висновку, що керівник органу досудового розслідування є важливою процесуальною фігурою у взаємозв'язку між прокурором – процесуальним керівником досудового розслідування та слідчим – особою, яка власне здійснює розслідування [1, с. 78].

На підставі проведеного дослідження можна стверджувати, що взаємодія прокурора, слідчого та оперативних підрозділів національної поліції під час проведення слідчих (розшукових) дій є важливою та необхідною умовою розслідування кримінальних правопорушень. Ця взаємодія реалізується у двох формах: взаємодія між прокурором і слідчим та взаємодія між слідчим та працівником оперативного підрозділу. Прокурор організовує діяльність слідчого у формі процесуального керівництва, а останній у свою чергу дає доручення співробітникам оперативних підрозділів. При цьому керівник органу досудового розслідування виступає в цій взаємодії своєрідною зв'язною ланкою для забезпечення реалізації доручень прокурора слідчим.

Список використаних джерел

1. Процесуальне керівництво прокурором досудовим розслідуванням: організаційно правові та криміналістичні основи: наук.-практ. посіб. / кол. авт. – [2-ге вид., переробл.] – К.: Національна академія прокуратури України, 2016. – 796 с.

2. Кримінальний процесуальний кодекс України: Закон України від 13.04.2012 № 4651-VI [Електронний ресурс] – Режим доступу: https://zakon.rada.gov.ua/laws/show/4651-17/conv#n387.

3. Кодекс України про адміністративні правопорушення (статті 1 - 212-24): Закон України від 07.12.1984 № 8073-X [Електронний ресурс] – Режим доступу: https://zakon.rada.gov.ua/laws/show/80731-10/conv#n2005.

Вейц Аркадій Михайлович,
аспірант кафедри криміналістики
Національного університету «Одеська юридична академія»

ДЕЯКІ ПИТАННЯ КРИМІНАЛІСТИЧНОГО АНАЛІЗУ КІБЕРЗЛОЧИНІВ, ВЧИНЕНИХ ЗА УЧАСТЮ СЛУЖБОВОЇ ОСОБИ АБО ТАКОЇ, ЯКА ЗДІЙСНЮЄ ПРОФЕСІЙНУ ДІЯЛЬНІСТЬ, ПОВ'ЯЗАНУ З НАДАННЯМ ПУБЛІЧНИХ ПОСЛУГ

Сьогодні «кібернетична» складова службової та професійної діяльності обумовлює необхідність вирішення при розслідуванні службових злочинів комплексних завдань, тобто завдань, пов'язаних з доказуванням не окремого кримінального правопорушення, регламентованого Розділом XVII Кримінального кодексу України, а комплексу органічно взаємопов'язаних злочинних дій, серед яких досить часто присутні злочини в сфері використання комп'ютерної техніки, які

вчинені службовою особою або такою, яка здійснює професійну діяльність, пов'язану з наданням публічних послуг. Акцентуємо, що за даними Департаменту кіберполіції в 2020 році в провадженні органів Національної поліції знаходилось 1004 кримінальних проваджень, відкритих за ст. 362 «Несанкціоновані дії з інформацією, яка оброблюється в електронно-обчислювальних машинах (комп'ютерах), автоматизованих системах, комп'ютерних мережах або зберігається на носіях такої інформації, вчинені особою, яка має право доступу до неї» та ст. 363 «Порушення правил експлуатації електронно-обчислювальних машин (комп'ютерів), автоматизованих систем, комп'ютерних мереж чи мереж електрозв'язку або порядку чи правил захисту інформації, яка в них оброблюється» КК України. Вказані показники на 30% більші у порівнянні з 2019 роком.

Ознайомлення з матеріалами судово-слідчої практики нажаль вказують на те, що більшість таких правопорушень взагалі залишаються в категорії латентна злочинність, адже в провадженнях, що вже направлені за ознаками кіберзлочину до суду, фігурують невстановлені особи, які виходячи з матеріалів справ мали доступ до інформації, що зберігається в електронних ресурсах з обмеженим доступом, відповідно могли відносити до категорії службових осіб або таких, що здійснюють професійну діяльність, пов'язану із наданням публічних послуг.

В. М. Бутузов, С. А. Буяджи, А. Ф. Волобуєв, І. О. Воронов, С. В. Демедюк, М. В. Карчевський, О. І. Котляревський, М. О. Кравцова, О. М. Лепеха, М. Ю. Літвінов, О. І. Мотлях, І. М. Осика, Л. П. Паламарчук, Д. В. Пашнєв, А. В. Реуцький, О. А. Самойленко та багато інших науковців приділяли увагу розслідуванню злочинів, передбачених ст. 361–363-1 КК, без конкретизації їх зв'язку з іншими видами злочинів, підкреслюючи потребу дослідження традиційних злочинів, вчинених у кіберпросторі, в тому числі й вчинених службовою особою.

Визначити напрямки розслідування таких злочинів та запропонувати алгоритми проведення слідчих дій можливо за умови криміналістичного аналізу службової злочинної діяльності у кіберпросторі. Використовуючи комплексний підхід до проблем розслідування кіберзлочинів та службових злочинів, спираючись на результати аналізу матеріалів судово-слідчої практики, можемо запропонувати окремі позиції щодо криміналістичного аналізу означеної вище злочинної діяльності у кіберпросторі.

Так, кіберзлочини, що вчиняються за участю службової особи або такою, що здійснює професійну діяльність, крім безпосереднього предмета посягання (майнових цінностей), мають додатковий предмет посягання, яким виступають у більшості випадків державні електронні інформаційні ресурси. На сьогодні законодавство України містить перелік пріоритетних державних електронних інформаційних ресурсів, які на думку А.І. Марущака та С. Г. Петрова визначаються такими в контексті

запровадження електронної взаємодії реєстрів [1, с. 16]. До таких віднесено: Державний земельний кадастр, Державний реєстр актів цивільного стану громадян, Державний реєстр виборців, Державний реєстр загальнообов'язкового державного соціального страхування, Державний реєстр обтяжень рухомого майна, Державний реєстр речових прав на нерухоме майно, Державний реєстр фізичних осіб-платників податків, Електронна система охорони здоров'я, Єдина державна електронна база з питань освіти, Єдина інформаційна система Міністерства внутрішніх справ, Єдиний державний автоматизований реєстр осіб, які мають право на пільги, Єдиний державний демографічний реєстр, Єдиний державний реєстр Міністерства внутрішніх справ стосовно зареєстрованих транспортних засобів та їх власників, Єдиний державний реєстр судових рішень, Єдиний державний реєстр юридичних осіб, фізичних осіб-підприємців та громадських формувань, Єдиний реєстр довіреностей, Єдиний реєстр документів, що дають право на виконання підготовчих та будівельних робіт і засвідчують прийняття в експлуатацію закінчених будівництвом об'єктів, відомостей про повернення на доопрацювання, відмову у видачі, скасування та анулювання зазначених документів, Єдиний реєстр об'єктів державної власності, Реєстр платників податку на додану вартість [2]. Однак, відповідно до Положення про Реєстр інформаційних, телекомунікаційних та інформаційно-телекомунікаційних систем органів виконавчої влади, а також підприємств, установ і організацій, що належать до сфери їх управління, такі ресурси повинні містити інформацію, яка є власністю держави, а необхідність її захисту повинна бути визначена законодавством [3]. Тому фактично цей перелік предметів посягання при вчиненні кіберзлочинів може бути розширений, наприклад, до них можна віднести офіційні веб-ресурси державних органів, більшість з яких мають широкий функціонал щодо внесення персональних даних за допомогою електронних ключів, Портал «Дія», Єдиний державний портал адміністративних послуг, електронні ресурси критичної інфраструктури тощо.

Крім того, вважаємо за потрібним звернути увагу на особу злочинця, яка сьогодні через наявність в неї спеціальних повноважень щодо інформації в ресурсі вкрай рідко залишає так звані «інформаційні», «віртуальні» або «цифрові» сліди – нетрадиційні сліди, що містяться в електронному середовищі. З огляду на безпосередність доступу до предмета посягання такої особи важливим буде визначення її кінцевого злочинного наміру та ступеню онлайн-загрози, яку створила така особа. В цьому сенсі на початку 2021 року Міністерство внутрішніх справ задекларувало створення сучасного класифікатору онлайн-загроз. Під час конференції з питань безпеки людини в онлайн-просторі «Міжнародна конференція «Безпечний онлайн 2020: Сучасні виклики» з врахуванням напрацювань світової спільноти, презентовано класифікатор, який максимально відповідатиме українським реаліям та контенту. Так, класифікатор онлайн-загроз включає такі кіберзагрози: дезінформація та маніпуляція; порушення авторських прав; пропаганда насильства,

терористичної та екстремістської діяльності; розповсюдження через Інтернет заборонених та обмежених до продажу товарів та послуг; шахрайство в онлайн-просторі; доступ дітей до шкідливого контенту; жорстоке поводження з дітьми в мережі Інтернет, сексуальна експлуатація та розбещення дітей у кіберпросторі; надмірне використання екранного часу; кіберпереслідування та кіберцькування; пропаганда суїциду та самокалічення [4]. Враховуючи сьогоднішний функціонал службових осіб та осіб, що надають професійні послуги, використовуючи свої повноваження щодо державних електронних інформаційних ресурсів, вважаємо. що такий класифікатор може бути суттєво розширений, а особа злочинця класифікована враховуючи ступінь загрози, яку вона створює щодо відповідного ресурсу.

Наприкінці зазначимо, що дослідження питань криміналістичного аналізу кіберзлочинів вчинених за участю службової особи або такої, яка займається професійною діяльністю, пов'язаною із наданням публічних послуг, можна вважати перспективним напрямком розроблення в контексті окремих криміналістичних методик.

Список використаних джерел

1. Марущак А.І., Петров С.Г. Зміст поняття «Державні електронні інформаційні ресурси». Інформація і право. 2018. №4(27). С. 15-21.

3. Деякі питання організації електронної взаємодії державних електронних інформаційних ресурсів: Постанова Міністрів України від 10.05.18 р. № 357. Урядовий кур'єр. 30.05.18 р. № 100. С. 3.

3. Постанова Кабінету міністрів України від 3 серпня 2005 року № 688. URL: https://ips.ligazakon.net/document/TM025913

4. В Україні створено класифікатор онлайн-загроз. URL: https://jurliga.ligazakon.net/ua/news/201038_v-ukran-stvoreno-klasifkator-onlayn-zagroz

Власенко Сергій Олександрович,
ад'юнкт відділу докторантури
та ад'юнктури Національної академії
внутрішніх справ

АКТУАЛЬНІ ПРОБЛЕМИ РОЗСЛІДУВАННЯ ТА ЗАПОБІГАННЯ НЕЗАКОННОМУ ЗАВОЛОДІННЮ ТРАНСПОРТНИМИ ЗАСОБАМИ

Складність розслідування кримінальних правопорушень, які кваліфікуються за статтею 289 Кримінального кодексу України, пов'язана із рядом чинників, у тому числі із ретельною підготовкою до вчинення кримінальних правопорушень, вчиненням вказаних злочинних діянь організованими злочинними угрупованнями, які мають високий рівень матеріально-технічного забезпечення і корупційні зв'язки у державних та правоохоронних органах. Нерідко незаконне заволодіння транспортними засобами набуває ознак кримінального «бізнесу», учасники котрого