розслідування. Тому використання технічних засобів є необхідним для належного виконання покладених на поліцію повноважень, ефективного забезпечення публічної безпеки та порядку та протидії злочинності.

Бібліографічні посилання

1. Інструкція із застосування органами та підрозділами поліції технічних приладів і технічних засобів, що мають функції фото- і кінозйомки, відеозапису, засобів фото- і кінозйомки, відеозапису. URL: https://zakon.rada.gov.ua/laws/show/z0028-19#Text (дата звернення: 23.10.2021).
2. Chula Vista PD Drone Program Uses AirData to Provide Full Transparency to Community. URL: https://www.google.com/amp/s/dronelife.com/2021/10/07/chula-vista-pd-drone-program-uses-airdata-to-provide-full-transparency-to-community/amp/ (дата звернення: 23.10.2021).
3. У Японії з'являться дрони-поліцейські. URL: https://ishop.if.ua/novyny/u-yaponiyi-zyavlyatsya-drony-policeyski (дата звернення: 23.10.2021).
4. Китайська поліція знаходить підозрюваних через окуляри. URL: https://www.google.com/amp/s/www.bbc.com/ukrainian/news-42979942.amp (дата звернення: 23.10.2021).
5. Національна поліція отримала понад 30 нових БПЛА. URL: https://defence-ua.com/news/natsionalna_politsija_otrimala_ponad_30_novih_bpla_foto-2537.html (дата звернення: 23.10.2021).

Волкова А. В., курсант 2-го курсу
факультету підготовки фахівців
для органів досудового розслідування
Науковий керівник – Прокопов С. О.,
старший викладач кафедри
економічної та інформаційної безпеки
Дніпропетровського державного
університету внутрішніх справ

ФІШИНГ – ОСНОВА КІБЕРАТАК

Проблема фішингу з кожним роком стає все більш поширеною. Фішинг – це атака, заснована на соціальній інженерії, яка проводиться через недоліки кібербезпеки для обману користувачів з метою крадіжки їх логінів, паролів і грошей [1].

Основною метою фішингу є отримання цінних даних, які можуть бути продані або використані зловмисником для здійснення заборонених дій проти майна людини, таких як вимагання, викрадення грошей або особистих даних. Фішинг існує впродовж багатьох років, за цей проміжок часу кіберзлочинці розробили достатній спектр методів інфікування жертв. Зловмисники, які займаються фішингом, найчастіше представляються

працівниками банків чи інших фінансових установ для того, аби змусити жертву фішингу заповнити фальшиву форму та отримати дані її облікових записів. Крадіжка інформації, тобто фішинг – поширена проблема, яка здійснюється шляхом розсилки спаму або підроблених електронних листів. Цей тип атаки припускає отримання користувачем шахрайського листа, що містить посилання на шкідливий вебсайт, який призначений для збору інформації та особистих даних користувача.

Відповідно до статистики в Україні протягом червня 2021 року на інформаційні ресурси державних органів було скоєно понад 50 тисяч кібератак, які своєчасно та успішно були усунені. Система захищеного доступу державних органів до мережі «Інтернет» заблокувала 50 571 атаку різних видів, що на 17 % більше, ніж попередні рази. У системі реагування на кіберінциденти та кібератаки на об'єктах моніторингу зафіксовано 1 177 118 підозрілих подій, а саме: отримання прав користувача – 49 %; спроби отримання прав адміністратора – 22 %; підозріле застосування кодів та нестандартних протоколів – 8 %. А основна кількість інцидентів стосується саме поширення шкідливого програмного забезпечення – 74 %, а також фішингу – 25 %.

В останні роки фішингові сайти стали великою проблемою. Є безліч методів розпізнавання фішингових сайтів, але внаслідок постійного розвитку виду цього шахрайства, зробити це буває складно. Для того щоб не зіткнутися з фішингом, важливо дотримуватися певних правил: користуватися лише перевіреними та захищеними офіційними сайтами, платіжними сервісами; увійшовши на невідомий сайт, з незнайомим іменем – не вводити конфіденційну інформацію в наведені поля; перебуваючи на банківських сайтах, важливо стежити, щоб було встановлено захищене з'єднання HTTPS, для того аби була можливість перевірити відповідність сертифікату HTTPS та захищеність сайту від кібератак.

Отже, дуже часто бувають ситуації, коли на пошту або в особисте повідомлення надходять дивні посилання, які складно ідентифікувати, важливо ніколи не переходити за посиланнями, тому що саме такі повідомлення надсилають злочинці під час використання методів поширення вірусів, фішингових сайтів. Якщо таке посилання надійшло від друга, варто переконатися у тому, що воно не становить загрози вашим персональним даним, бо у наш час є багато схем зламування облікових записів і надсилання шахрайських розсилок, про які ніхто і не здогадується. Боротися з фішингом дуже легко, якщо підвищувати власну грамотність: приділяти увагу деталям та намагатися зберегти приватні дані, паролі та іншу важливу інформацію від посягань кіберзлочинців.

Бібліографічні посилання

1. Кіберзлочинність в Україні: вебсайт. URL:
2. https://www.science-community.org/ru/node/%2016132
3. Здійснення кібератак на державні інформаційні ресурси: вебсайт. URL: https://www.google.com/amp/s/ua.interfax.com.ua/news/telecom/750914-amp.html