підрозділи, яким необхідно сучасне обладнання та поновлення застарілої техніки. Адже така криміналістична техніка як набір «Молекула» або пересувна криміналістична лабораторія це засоби, які забезпечують якісну роботу слідчих та сприяють розкриттю злочинів.

Список використаних джерел:

1. Криминалистика: учебник / Т.С Волчецкая, В.Я. Колдин, В.Л. Крылов, ред.профессор Н.П. Яблоков 2-е изд.,перераб., 2001. 718 с.

2. Про організацію діяльності органів досудового розслідування Національної поліції України. *URL :* https://zakon.rada.gov.ua/laws/show/z0918-17?lang=ru .

3. Криміналістика: [навч. посіб.] / Р. І. Благута, Р. І. Сибірна, В. М. Бараняк та ін. ; за заг. ред. Є. В. Пряхіна. К. : Атіка, 2012. 496 с.

4. ProZorro публічні закупівлі. Пересувна криміналістична лабораторія на базі транспортного засобу Renault Dokker 1.5D MT Expression або еквіваленту укомплектована криміналістичною та оглядовою технікою. *URL:* https://www.prozorro.gov.ua/tender/UA-2018-07-04-000964-a.

5. ProZorro публічні закупівлі. Витратні матеріали для криміналістичних досліджень. *URL:* https://prozorro.gov.ua/tender/UA-2017-05-03-000523-b.

Сафонова Тетяна Русланівна,
студентка юридичного факультету Дніпропетровського державного університету внутрішніх справ
Науковий керівник:
Коваленко Ілля Олександрович,
адвокат, викладач кафедри кримінально-правових дисциплін Дніпропетровського державного університету внутрішніх справ

ДО ПИТАННЯ ПРОТИДІЇ КІБЕРЗЛОЧИННОСТІ

У XXI столітті кібернетична безпека є одним із найважливіших питань, що дає поштовх до глибокого аналізу, розробки та впровадження високотехнологічних рішень для запобігання та виявлення кіберзагроз.

Як зазначено в законодавстві, кібербезпека - це захист життєво важливих інтересів людини та громадянина, суспільства та держави в процесі використання кіберпростору, що забезпечує стійкий розвиток інформаційного суспільства та цифрового комунікаційного середовища,

своєчасне виявлення, запобігання та нейтралізацію реальних та потенційних загроз для України [1, п. 5 ч. 1 ст. 1].

Для багатьох напрямків діяльності важливо забезпечити інформаційну безпеку, включаючи галузі науки, техніки та технологій (насамперед ІТ), які ускладнюють безпеку кіберпростору держави, деякі об'єкти, згадані в її інфраструктурі тощо. Такими об'єктами, зокрема, є:

- ІТ підтримки кіберпростору країни (підприємства, установи тощо);
- інформаційні ресурси країни (підприємства, установи тощо);
- ІС та інтелектуальні системи різних класів;
- технології забезпечення об'єктів різного рівня;
- процеси управління кібербезпекою об'єктів різної природи [2, с. 81].

Варто зазначити, що розвиток ІТ-технологій сприяє поширенню технік та технологій кібератак, а хакери мають багато можливостей для використання вразливості кібербезпеки та досягнення своїх злочинних цілей. Кібератаки - це спрямовані (навмисні) дії в кіберпросторі, які здійснюються за допомогою електронних комунікацій (включаючи інформаційно-комунікаційні технології, програмне забезпечення, апаратні засоби, інші технічні та технологічні засоби та обладнання) і спрямовані на досягнення однієї або декількох наступних цілей: порушення конфіденційності, цілісності, доступності електронних інформаційних ресурсів, що обробляються (передаються, зберігаються) в комунікаційних та / або технологічних системах, отримуючи несанкціонований доступ до таких ресурсів; порушення безпеки, стійкого, надійного та регулярного режиму роботи комунікаційних та / або технологічних систем; використання системи зв’язку, її ресурсів та електронних комунікацій для кібератак проти інших об’єктів кіберзахисту [1, п. 4 ч. 1 ст. 1].

Сьогодні одним із найпоширеніших видів кібератак є фішинг. Фішинг - це низка шахрайських дій, спрямованих на розкрадання персональних даних користувачів Інтернету та неправомірне привласнення коштів за допомогою отриманої інформації. Як правило, зловмисники полюють на паролі, номери банківських карток, а також на конфіденційні дані клієнтів для різних платіжних систем, інтернет-банкінгу та онлайн-кредитних послуг. Крім того, кіберзлочинці діють за різними схемами, бо ж сфера їх діяльності максимально широка.

Для отримання цінної інформації хакери використовують:

1. Розсилку спаму на електронні адреси. Фішинг-листи виглядають як повідомлення надійної організації. Однак, натиснувши на посилання, ви не зможете отримати доступ до фактичного веб-сайту компанії. Натомість ви потрапляєте в пастку шахрая.

2. СМС-повідомлення з посиланнями на фішинг-сайти чи вірусні матеріали. Ця схема працює трохи інакше, ніж електронна розсилка, оскільки жертвам зазвичай пропонують брати участь у неіснуючих

розіграшах або надсилати якісь деталі, щоб виграти. Зазвичай текстові повідомлення також вказують на посилання, за яким треба перейти, або номер телефону, який потрібно набрати. Іноді, в таких СМС-повідомлення також просять оплатити вартість доставки неіснуючого призу або інших "пов'язаних" платежів [3].

3. Інтернет-матеріали, замасковані під офіційні джерела. Шахрайство, коли зловмисники копіюють будь-які сайти, часто вони є інтернет-магазинами. При цьому використовуючи схожі доменні імена та однаковий дизайн. Користувачі Інтернету вважають, що вони перебувають на веб-сервері існуючого магазину, який має хорошу репутацію. Після прийняття рішення про придбання товару потерпілий реєструється в системі.

Хоча фішери використовують досить складні схеми для отримання особистої інформації, є кілька важливих рекомендацій, які допоможуть захистити себе:

- обновляйте програмні засоби, зокрема, браузер, антивірус, операційну систему;
- особливо будьте обережні, коли «від банку» потрібна секретна інформація (скажімо, ваш пароль до системи клієнт-банк). Справжній банк спілкується лише захищеним каналом, наприклад, коли ви ввійшли в систему «Клієнт-Банк»;
- ретельно перевіряйте, чи немає в листі розбіжностей. Наприклад, нуль замість літери "О". Наведіть курсор на адресу відправника і подивіться, якою буде реальна адреса. Якщо можливо, порівняйте адресу з попередніми справжніми листами від банку. Перевірка орфографічних помилок;
- ні в якому разі не натискайте на посилання та додатки, вводьте адреси в браузері вручну [4];
- якщо ви відкрили хакерський ресурс та встигли зробити деякі дії, а потім помітили небезпеку, негайно залиште ресурс та очистіть кеш-пам’ять комп’ютера, зробіть повне сканування вірусів, а також надішліть скаргу на підозрілий сайт в Державний департамент кіберполіції [3];
- не відповідайте на СМС, де необхідно вказати реквізити платіжної картки, пароль чи особисті дані, що стосуються безпеки;
- зберігайте спокій. Не поспішайте, перевірте все, перш ніж реагувати;
- відкривайте повідомлення лише з перевірених осіб чи органів;
- якщо ви відповіли на СМС, надали банківські реквізити, а потім запідозрили, що це смішинг (вид фішингу), ви повинні негайно повідомити про це банк [4].

Таким чином, одним із пріоритетних напрямків в політиці країни залишається протидія кіберзлочинності та рівень кібербезпеки. Проте,

нормативне регулювання не встигає за розвитком технологій, що загострює проблему кіберзлочинності. Щороку з'являються нові та вдосконалені види кібератак, як наприклад фішинг. Тому необхідне більш широке розповсюдження інформації про відомі види Інтернет-шахрайства та як захиститися від них.

Список використаних джерел:

1. Закон України «Про основні засади забезпечення кібербезпеки України» від 05.10.2017 № 2163-VIII // (Відомості Верховної Ради (ВВР), 2017, № 45, ст. 403). – [Електронний ресурс]. – Режим доступу: https://zakon.rada.gov.ua/laws/show/2163-19

2. Ткаченко О. Кіберпростір і кібербезпека: проблеми, перспективи, технології / О. Ткаченко, К. Ткаченко // Цифрова платформа: інформаційні технології в соціокультурній сфері. - Київ: Вид. центр КНУКіМ. - 2018. - № 1. - с. 75-86.

3. Дворак І. Що таке фішинг та як від нього захиститися? – [Електронний ресурс]. – Режим доступу: https://loando.ua/statis/shho-take-fishing-ta-yak-vid-nogo-zahistitisya

4. ЕМА. Школа кібербезпеки – [Електронний ресурс]. – Режим доступу: https://www.ema.com.ua/citizens/cyber-safety-school/shahrai-telefonujut-nadsilajut-sms-i-elektronni-listi/

Сенько Анастасія Вадимівна,
аспірант кафедри криміналістики,
судової медицини та психіатрії
Дніпропетровського державного
університету внутрішніх справ
Науковий керівник:
Чаплинський Костянтин Олександрович,
доктор юридичних наук, професор,
завідувач кафедри криміналістики,
судової медицини та психіатрії
Дніпропетровського державного
університету внутрішніх справ

TO THE QUESTION OF CONDUCTING THE INTERVIEW DURING THE INVESTIGATION OF THEFT OF PASSENGER LUGGAGE IN THE AIRPORTS

The investigation of any criminal offense requires the National Police to respond as quickly as possible and to carry out the most appropriate procedural steps at the appropriate stage of the investigation. One of the most common investigative (investigative) actions in criminal proceedings of various categories is interrogation. It also does not lose its relevance in the investigation