МВС України
Харківський національний університет внутрішніх справ
Науковий парк «Наука та безпека»
Координатор проектів ОБСЄ в Україні

ПРОТИДІЯ КІБЕРЗЛОЧИННОСТІ ТА ТОРГІВЛІ ЛЮДЬМИ

Збірник матеріалів
Міжнародної науково-практичної конференції
(м. Харків, 27 травня 2022 року)

Харків
2022

УДК [351.74:004](477)(08)
П83

Друкується згідно з рішенням оргкомітету
за дорученням Харківського національного університету внутрішніх справ
від 29.04.2022 № 26

Протидія кіберзлочинності та торгівлі людьми : зб. матеріалів міжнарод. П83 наук.-практ. конф. (м. Харків, 27 трав. 2022 р.) / МВС України, Харків. нац. ун-т внутр. справ, Наук. парк «Наука та безпека» ; Координатор проектів ОБСЄ в Україні. – Харків : ХНУВС, 2022. – 66 с.

У матеріалах конференції окреслено найбільш актуальні проблеми протидії кіберзлочинності та торгівлі людьми на сучасному етапі. Проаналізовано питання правового й організаційного забезпечення протидії кіберзлочинності та торгівлі людьми, кримінально-правові, процесуальні та криміналістичні аспекти протидії цьому негативному явищу. Розглянуто відповідний міжнародний досвід, а також кадрове забезпечення правоохоронних органів. Досліджено використання інформаційних технологій і технічних засобів у протидії кіберзлочинності та торгівлі людьми.

УДК [351.74:004](477)(08)

Матеріали викладені в авторській редакції з незначними коректорськими правками.
Відповідальність за точність поданих фактів, цитат, цифр і прізвищ несуть автори.

Електронна копія збірника безоплатно розміщується у відкритому доступі на сайті Харківського національного університету внутрішніх справ (http://www.univd.edu.ua) у розділі «Наука», сторінка «Конференції, семінари, та круглі столи»), а також у репозитарії ХНУВС (http://dspace.univd.edu.ua/xmlui/).

ЗМІСТ

РОЗДІЛ 2.
КРИМІНАЛЬНО-ПРАВОВІ, ПРОЦЕСУАЛЬНІ ТА КРИМІНАЛІСТИЧНІ АСПЕКТИ ПРОТИДІЇ КІБЕРЗЛОЧИННОСТІ ТА ТОРГІВЛІ ЛЮДЬМИ

РОЗДІЛ 3.
ВИКОРИСТАННЯ ІНФОРМАЦІЙНИХ ТЕХНОЛОГІЙ І ТЕХНІЧНИХ ЗАСОБІВ У ПРОТИДІЇ КІБЕРЗЛОЧИННОСТІ ТА ТОРГІВЛІ ЛЮДЬМИ

ВІТАЛЬНЕ СЛОВО

ректора Харківського національного університету внутрішніх справ
доктора юридичних наук, професора, члена-кореспондента
Національної академії правових наук України, заслуженого юриста України,
генерала поліції третього рангу
Валерія Васильовича Сокуренка

Шановні учасники конференції!

Від імені ректорату та Вченої ради Харківського національного університету внутрішніх справ вітаю вас із початком Міжнародної науково-практичної конференції «Протидія кіберзлочинності та торгівлі людьми».

У цьому році конференція проводиться у складних умовах посилення збройної агресії Російської Федерації проти України. Війна, розв'язана Росією, зумовила радикальне збільшення кількості насильницьких злочинів проти українців. Міграційна хвиля спричинила збільшення ризику потрапляння наших громадян до тенет торговців людьми. З'явилися нові схеми кіберзлочинів, а самі правопорушники почали діяти зухваліше, користуючись тим, що правоохоронні органи зайняті на інших ділянках, зокрема у протидії окупантам.

Нові виклики потребують швидких нестандартних дій. У цих умовах украй важливими стають наукові рішення, здатні вплинути на ситуацію, змінити негативні тренди в суспільному житті, створити умови для нормального розвитку соціуму.

Конференція, яка проводиться сьогодні, має на меті серед іншого допомогти практичним працівникам адекватно реагувати на сучасні загрози у праовохоронній сфері, допомогти знайти певні організаційні, юридичні, технічні та управлінські рішення поставлених оперативно-службових завдань.

Тематика наукового заходу є надзвичайно актуальною для нашого суспільства. За 2021 рік в Україні кількість зареєстрованих кіберзлочинів збільшилась на 25 %, а злочинів торгівлі людьми – майже на 12 %. У процесі розслідування цих злочинів правоохоронцям вдалося припинити діяльність декількох сотень правопорушників. Якщо говорити про роботу кіберполіції, то у 2021 році до неї надійшло 48 тисяч звернень громадян про вчинені кіберправопорушення.

До організаційного комітету для включення до збірника конференції було надіслано 34 тези наукових доповідей від 47 авторів. Серед них були вітчизняні вчені, практики, курсанти і студенти, а також представники Китайської Народної Республіки та Латвії.

Сподіваюся, що конференція стане міцною платформою для висловлення власного бачення учасниками напрямів розвитку процесу підготовки правоохоронців у нашій державі, обміну досвідом між науковцями, практичними працівниками та їх колегами з інших країн, а потужний науковий потенціал учасників сприятиме досягненню поставленої мети.

Бажаю всім плідної роботи, творчого натхнення, здоров'я, миру та добра.

РОЗДІЛ 1.
ОКРЕМІ ПИТАННЯ ПРАВОВОГО ТА ОРГАНІЗАЦІЙНОГО ЗАБЕЗПЕЧЕННЯ ПРОТИДІЇ КІБЕРЗЛОЧИННОСТІ ТА ТОРГІВЛІ ЛЮДЬМИ

УДК 65.012.8
ПАВЛІЧЕНКО Катерина Володимирівна,
заступник Міністра внутрішніх справ України

ЩОДО СТАНУ ПРОТИДІЇ ЗЛОЧИНАМ, ПОВ'ЯЗАНИМ ІЗ ТОРГІВЛЕЮ ЛЮДЬМИ В УКРАЇНІ

Ситуація із протидією торгівлі людьми в Україні постійно змінюється. За останні роки правоохоронні органи доклали значних зусиль для того, щоб таке негативне явище якомога рідше зустрічалося в нашій країні. Серед іншого завдяки проведеним заходам вдалося покращити позиції України у глобальних рейтингах, які висвітлюють поточну ситуацію щодо протидії злочинам, пов'язаним із торгівлею людьми.

24 лютого 2022 року наша країна вчергове зазнала підступного удару з боку Російської Федерації, який спровокував у тому числі сплеск злочинів, пов'язаних із торгівлею людьми. Сьогодні ще неможливо повною мірою підрахувати всі кримінальні правопорушення подібної категорії, вчинені окупантами, проте навіть уже виявлені та встановлені факти свідчать про різкий стрибок загальної кількості насильницьких і майнових злочинів, злочинів, повязаних із незаконним переміщенням та експлуатацією наших громадян. Описана ситуація не дає змоги визначити сталу базу для порівняння поточних всеукраїнських показників рівня злочинності у сфері торгівлі людьми із даними за попередні роки, проте проглянути загальну тенденцію в цій сфері цілком дозволяє.

Аналізуючи наявні статистичні відомості щодо злочинів, пов'язаних із торгівлею людьми, можна виходити з того, що з певною кількістю обмежень стан реєстрації правопорушень можна розглядати як індикатор роботи поліції, стан направлених до суду з обвинувальним актом кримінальних проваджень – як індикатор роботи прокуратури, стан засудження – як індикатор роботи судів.

Якщо взяти до уваги відповідні показники за 2013–2021 рр., то можна констатувати таке. За злочинами, відповідальність за які передбачена ст. 149 Кримінального кодексу України, динаміка реєстрації правопорушень спочатку була негативною (–9,23 % у 2014 р., –6,77 % у 2015 р.), але з 2016 р. вона має здебільшого позитивний тренд (3,63 % у 2016 р., 198,24 % у 2017 р., 17,91 % у 2019 р., 11,7 % у 2021 р.), крім 2018 р. (– 21,18 %) та 2020 р. (–35,13 %). Стан представлення звинувачень у суді спочатку показав здебільшого негативну динаміку (–5,17 % у 2014 р., –23,73 % у 2016 р., –35,13 % у 2020 р.), але з 2015 р. динаміка стала здебільшого позитивною: 7,27 % у 2015 р., 115,56 % у 2017 р., 9,27 % у 2018 р., 41,51 % у 2019 р., 11,7 % у 2021 р. Щодо стану притягнення підсудних до відповідальності (засудження), то тут динаміка є здебільшого негативною: –44,62 % у 2014 р., –11,11 % у 2015 р., –18,75 % у 2016 р., –11,53 у 2017 р., –34,78 % у 2018 р., –17,14 % у 2020 р., –17,24 % у 2021 р., проте 133,33 % у 2019 р.

За злочинами, відповідальність за які передбачена ст. 143 Кримінального кодексу України, за незначної кількості правопорушень у 2014 – 2015 рр. можна простежити неоднозначну динаміку щодо реєстрації правопорушень: 50 % у 2014 р. і 66,67 % у 2015 р. У 2016 та 2020 роках усі показники нульові, а з 2017 до 2019 року стало реєструється по два злочини щорічно, у 2021 році – чотири. Що ж стосується індикаторів роботи прокуратури та суду, то їх простежити не уявляється можливим через те, що протягом досліджуваного періоду тільки чотири провадження було передано до суду з обвинувальним висновком (2015 р.), але жодного засудження за цією статтею не відбулося протягом досліджуваного періоду.

За злочинами, відповідальність за які передбачена ст. 146 Кримінального кодексу України, динаміка реєстрації правопорушень здебільшого була негативною (–58,07 % у 2015 р., –33,58 % у 2016 р., –6,16 % у 2017 р., –7,17 % у 2019 р., –27,61 % у 2020 р.), в окремі роки –

позитивною (620,97 % у 2014 р., 10,93 % у 2018 р., 8,27 % у 2021 р.). Водночас стан представлення звинувачень у суді продемонстрував здебільшого позитивну динаміку (22 % у 2015 р., 15,18 % у 2017 р., 62,79 % у 2018 р., 9,04 % у 2019 р., 31,30 % у 2021 р.), проте була зафіксована і негативна (–16,67 % у 2014 р., –8,20 % у 2016 р., –42,8 у 2020 р.). Щодо стану притягнення підсудних до відповідальності (засудження), то тут динаміка є здебільшого негативною: –36,11 % у 2014 р., –27,12 % у 2016 р., –1,61 % у 2018 р., –16,40 % у 2019 р., –43,14 % у 2020 р., проте 28,26 % у 2015 р., 44,19 % у 2017 р., 103,45 % у 2021 р.

За злочинами, відповідальність за які передбачена ст. 147 Кримінального кодексу України, динаміка реєстрації правопорушень була як негативною (–58,54 % у 2015 р., –58,82 % у 2016 р., –57,14 % у 2017 р., –62,5 % у 2020 р.), так і позитивною або нейтральною (925 % у 2014 р., 100 % у 2018 р., 33,33 % у 2019 р., 0 % у 2021 р). Стан представлення звинувачень у суді продемонстрував таку динаміку: 100 % у 2014 р., 25 % у 2015 р., –40 % у 2016 р., –33,33 % у 2017 р., 100 % у 2018 р., 0 % у 2019 р., –50 % у 2020 р. Щодо стану притягнення підсудних до відповідальності (засудження), то тут динаміка була малоінформативною: –100 % у 2014, 2017 та 2020 роках та 200 % у 2019 р. В інші роки відповідні показники дорівнювали нулю.

За злочинами, відповідальність за які передбачена ст. 148 Кримінального кодексу України, було зареєстровано лише по одному злочину у 2013, 2014, 2016, 2018 роках та два у 2020 р. Показники в інші роки дорівнюють нулю.

За злочинами, відповідальність за які передбачена ст. 150 Кримінального кодексу України, динаміка реєстрації правопорушень була як негативною (–63,64 % у 2014 р., –50 % у 2015 р., –83,33 % у 2017 р., –43,75 % у 2019 р., –100 % у 2020 р.), так і позитивною (200 % у 2016 р., 1500 % у 2018 р.). Стан представлення звинувачень у суді продемонстрував неочевидну динаміку: 0 % у 2014 р., –100 % у 2015 р., –62,5 % у 2019 р., –100% у 2020 р.). Показник в інші роки дорівнюють нулю. Щодо стану притягнення підсудних до відповідальності (засудження), то тут динаміка була малоінформативною.

За злочинами, відповідальність за які передбачена ст. 150-1 Кримінального кодексу України, динаміка реєстрації правопорушень була здебільшого негативною або нейтральною (–84,91 % у 2015 р., –64,29 % у 2017 р., 0 % у 2019 р., 0 % у 2020 р., –42,86 % у 2021 р.), інколи позитивною (29,27 % у 2014 р., 75 % у 2016 р., 40 % у 2018 р.). Стан представлення звинувачень у суді також продемонстрував здебільшого негативну або нейтральну динаміку (–83,67 % у 2015 р., 0 % у 2016 р., –50 % у 2017 р., –20 % у 2019 р., –20 % у 2021 р.), інколи позитивною (44,11 % у 2014 р., 25 % у 2018 р., 25 % у 2020 р.). Щодо стану притягнення підсудних до відповідальності (засудження), то тут динаміка була також негативною (–58,33 % у 2014 р., –70 % у 2015 р., –25 % у 2017 р., –66,67 % у 2018 р., –50 % у 2019 р., –75 % у 2021 р.), проте позитивною у 2016 (166,67 %) та 2020 (300 %) роках .

За злочинами, відповідальність за які передбачена ст. 169 Кримінального кодексу України, було зареєстровано лише по 3 злочини у 2016 та 2017 роках, по 2 злочини у 2013, 2014, 2018, 2021 роках, по одному злочину у 2015, 2019 та 2020 роках. Решта показників неочевидні.

За злочинами, відповідальність за які передбачена ст. 301 Кримінального кодексу України, динаміка реєстрації правопорушень демонструє хвилеподібну форму: 12,44 % у 2014 р., –10,98 % у 2015 р., –9,69 % у 2016 р., 66,63 % у 2017 р., 8,06 % у 2018 р., –39,11 % у 2019 р., 13,83 % у 2020 р., 29,34 % у 2021 р. Стан представлення звинувачень у суді показав здебільшого позитивну динаміку: 8,88 % у 2014 р., –4,90 % у 2015 р., 90,09 % у 2017 р., 32,24 % у 2018 р., проте –22,91 % у 2016 р., –42,04 % у 2019 р., –1,39 % у 2020 р., –2,93 % у 2021 р. Щодо стану притягнення підсудних до відповідальності (засудження), то тут динаміка є здебільшого негативною: –15,81 % у 2015 р., –47,99 % у 2016 р., –14,19 % у 2017 р., –8,63 % у 2019 р., –19,69 % у 2020 р., проте 7,60 % у 2014 р., 4,51 % у 2018 р., 1,96 % у 2021 р.

За злочинами, відповідальність за які передбачена ст. 302 Кримінального кодексу України, динаміка реєстрації правопорушень здебільшого негативна: 21,53 % у 2014 р., –7,48 % у 2015 р., –27,44 % у 2016 р., –31,67 % у 2017 р., –3,86 % у 2018 р., 14,28 % у 2019 р., 36,33 % у 2020 р., 18,4 % у 2021 р. Стан представлення звинувачень у суді показав здебільшого негати-

вну або нейтральну динаміку: –43,42 % у 2016 р., 0 % у 2017 р., –7,07 % у 2018 р., –38,83 % у 2020 р., –17,46 % у 2021 р., проте 3,23 % у 2014 р., 9,38 % у 2015 р., 11,95 % у 2019 р. Щодо стану притягнення підсудних до відповідальності (засудження), то тут динаміка є здебільшого негативною: –4,23 % у 2015 р., –51,93 % у 2016 р., –8,05 % у 2017 р., –30 % у 2018 р., –21,43 % у 2019 р., –15,91 % у 2020 р., –21,6 % у 2021 р., проте 3,85 % у 2014 р.

За злочинами, відповідальність за які передбачена ст. 304 Кримінального кодексу України, динаміка реєстрації правопорушень переважно негативна: –21,46 % у 2014 р., –14,80 % у 2015 р., –38,55 % у 2016 р., –13,04 % у 2017 р., –16,43 % у 2018 р., –35,47 % у 2019 р., проте 5,96 % у 2020 р. Стан представлення звинувачень у суді показав переважно негативну або нейтральну динаміку: –23,79 % у 2014 р., –12,34 % у 2015 р., –40,99 % у 2016 р., –10,87 % у 2017 р., –15,35 % у 2018 р., –36,74 % у 2019 р., –24,82 % у 2021 р., проте 3,68 % у 2020 р. Щодо стану притягнення підсудних до відповідальності (засудження), то тут динаміка є здебільшого негативною: –42,31 % у 2014 р., –15 % у 2015 р., –47,06 % у 2016 р., – 43,33 % у 2018 р., 0 % у 2019 р., –29,41 % у 2020 р., проте 11,11 % у 2017 р., 8,33 % у 2021 р.

За злочинами, відповідальність за які передбачена ст. 447 Кримінального кодексу України, було зареєстровано лише по одному злочину у 2014, 2016, 2019 роках, у 2021 р. – 2 злочини. Показники в інші роки дорівнюють нулю.

Наведені тренди свідчать про позитивну динаміку у розслідуванні проваджень. Водночас існує негативний тренд щодо прийнятих судових рішень. Так, наприклад, щодо притягнення до відповідальності за злочини торгівлі людьми (ст. 149 Кримінального кодексу України), які кваліфікуються як тяжкі або особливо тяжкі та можуть передбачати покарання від 3 до 15 років позбавлення волі, з 2013 р. засуджується в середньому 32 особи на рік, із них лише до 11 осіб застосовується позбавлення волі на певний строк.

Вказана ситуація потребує:

– додаткового вивчення проблемних питань у сфері доказування таких злочинів у суді;

– налагодження взаємодії передусім між суддями та прокурорами;

– додаткового підвищення обізнаності суддів щодо механізму вчинення та документування злочинів торгівлі людьми із застосуванням інформаційних технологій, оскільки переважна частина зареєстрованих злочинів цього виду так чи інакше містить доказову інформацію в електронному вигляді.

Одержано 01.05.2022

UDC 621.3.01

YASHCHUK Inna Petrivna,
Doctor of Pedagogical Sciences, Professor,
Honored Worker of Science and Technology of Ukraine,
Acting Director of the Department of Education,
Science and Sports of the Ministry of Internal Affairs of Ukraine
https://orcid.org/0000-0003-4028-3327

CONTEMPORARY TASKS OF ENSURING THE SECURITY OF COMPUTER NETWORKS

Modernity can no longer be imagined without digital electronic devices designed to solve certain problems or provide the necessary services. With the development of innovations in this industry, devices are beginning to be networked in a complex structure of complex architecture to share the resulting resources and capacities. These networks can cover an unlimited number of participants, and due to new technologies, these participants can be significantly removed from each other, thereby increasing the actual physical size of the network.

It is obvious that such structures are the object of increased interest and close attention on the part of criminal elements, as they contain valuable personal information, and also provide various opportunities in the cyber sphere. Illegal and malicious use of these features is a crime and should be prevented.

There are a number of computer network protection mechanisms that are used in specific technical means and protection systems in various combinations and variations. The greatest effect is achieved with their systemic use in combination with other types of protection measures.

These mechanisms can be divided into the following categories.

Preventive one is aimed at preventing a security breach, for example, access restriction can be attributed to this category.

Purposes of their application:

– update and prevention of problematic situations;

– creation of barriers on the way of realization of threats;

– redundancy, separation of roles;

– use of access control means;

– access control to the premises, etc.

Detective tools allow one to detect violations in a timely manner, for example, they include mechanisms such as event registration and attack detection.

Purposes of application of detective mechanisms:

– identifying problematic situations and security breaches during or after they are identified;

– security monitoring;

– detection of network attacks;

– antivirus scanning;

– file checksum check;

– internal audit procedures, etc.

Adjustments allow for a reasonable period of time to solve problematic situations identified with the help of detective control mechanisms.

Purposes of application of the given protection mechanisms:

– system recovery in case of attacks;

– insurance of information security risks;

– security breach response;

– elimination of the last introduction of threats and minimization of damage;

– development, implementation and implementation of a disaster recovery plan (business continuity and recovery plan);

– data backup and recovery, etc.

Theoretically, a preventive approach to ensuring information security can be considered ideal, as it involves preventing the implementation of threats. But in practice, systems based on preventive measures can be too complex, which contradicts the basic principle of information security – the principle of reasonable sufficiency of protection.

Computer network security control belongs to the categories of preventive defense mechanisms. Its main purpose is to “reveal” weaknesses (vulnerabilities) in network protection in a timely manner and thereby help prevent possible attacks using it.

The process of monitoring network operation is usually divided into two stages: monitoring and analysis.

Network monitoring is a crucial process in which all network components such as routers, switches, firewalls, servers, and virtual machines are monitored for failures and performance and continuously evaluated to maintain and optimize their availability. One important aspect of network monitoring is that it must be proactive.

At *the monitoring stage*, a simpler procedure is performed – the procedure for collecting primary data on the operation of the network:

- statistics on the number of frames and packets of various protocols circulating in the network,

- the state of the ports of hubs, switches and routers, etc.

Next, the *analysis stage is performed*, which is understood as a more complex and intelligent process of comprehending the information collected during the monitoring stage, comparing it with data obtained earlier, and developing assumptions about the possible causes of slow or unreliable network operation.

Monitoring tasks are solved by software and hardware meters, testers, network analyzers, built-in monitoring tools for communication devices, as well as agents of control systems.

The task of analysis requires more active human participation and the use of such complex tools as expert systems, which accumulate the practical experience of many network specialists.

Received 01.05.2022

УДК 65.012.8+004

СОКУРЕНКО Валерій Васильович,
доктор юридичних наук, професор,
член-кореспондент Національної академії правових наук України,
заслужений юрист України,
ректор Харківського національного університету внутрішніх справ
https://orcid.org/0000-0001-8923-5639

АКТУАЛЬНІ ПИТАННЯ ПРОТИДІЇ ЗАГРОЗАМ БЕЗПЕКИ ІНФОРМАЦІЇ В УМОВАХ АГРЕСІЇ РОСІЙСЬКОЇ ФЕДЕРАЦІЇ

Іде вже дев'ятий рік війни Російської Федерації, яку вона веде проти України та всього цивілізованого світу. Стратегія агресора, як і класичних імперій, передбачає організацію збройного протистояння силами підкорених, яких не шкода і яких кидають у перших лініях фронтових атак. Це можна спостерігати на прикладі політики тотального знищення у жерлі війни звичайних «мобілізованих» громадян України з тимчасово окупованих частин Донецької та Луганської областей, залучення до бойових дій проти України військових зрадників з Автономної Республіки Крим, залучення до служби на боці агресора етнічних українців, що проживають на нинішній території Російської Федерації.

Агресивні дії Росії супроводжуються вчиненням великої кількості військових злочинів, частина з яких уже виявлена, але, впевнений, що це лише краплинка у вирі того жаху, який залишається прихованим за лінією окупованих територій.

Для полегшення здійснення військових операцій і прикриття вчинених злочинів агресор використовує нетрадиційне інформаційне та кіберсередовище.

У першому випадку це може стосуватися:

– проведення дезінформаційних компаній;

– вкидання фейків;

– несвідоме залучення українських засобів масової інформації до поширення недостовірної інформації з метою їх дискредитації та викликання негативного ставлення до України в цілому;

– створення псевдоукраїнських інформаційних ресурсів та донесення через них ворожих наративів;

– сіяння паніки серед громадян України;

– пропаганда.

В останньому випадку йдеться про ціле різноманіття методів донесення інформації з метою викривлення світогляду людини. Серед них виділяють «гнилий оселедець» (скандальні звинувачення, які постійно асоціюватимуться з особою), «перегорнута піраміда» (пріоритетне донесення інформації на початку матеріалу), «велика брехня» (коли неможливо повірити, що про таке можна брехати), «40 на 60» (60 % інформації на користь супротивника, 40 % – на користь суб'єкта інформаційного впливу), «абсолютна очевидність» (інформація доноситься як очевидний факт, що не потребує підтвердження).

У кіберпросторі дії агресора є також вельми різноманітними. Передусім це:

– виявлення фото- та відеознімків територій нанесення ударів у мережі Інтернет з метою коригування ворожого вогню;

– вербування, спілкування з колаборантами, інформаторами та зрадниками з числа громадян України, в тому числі віддалене отримання координат і фотознімків об'єктів критичної інфраструктури, додаткових маршрутів пересування в районі здійснення військових дій, інформації про рух військової техніки та важливих вантажів;

– ствоерння мереж ботоферм для вирішення різноманітних завдань;

– збирання інформації про об'єкти з різних мережних джерел;

– атаки на державні інфоресурси.

Описані небезпеки є не вичерпними та потребують належних заходів протидії. У рамках захисту від агресії в інформаційному просторі можна застосвувати різноманітні логічні, технічні та комбіновані методи. Логічні методи є найбільш тривіальними та передбачають критичний підхід до будь-яких відомостей, надання переваги раціональній складовій над емоційною під час здійснення аналізу, зіставлення даних із багатьох джерел з доброю репутацією, робота з першоджерелами. Серед технічних методів виділяють застосування різних програмних засобів залежно від поставлених завдань. Це може бути пошук першоджерела певних даних за допомогою інформаційно-пошукових систем, розпізнавання облич і предметів на фотознімках та відео, ототожнення об'єктів із різноманітних мультимедійних файлів, аналіз мультимедіа на предмет монтажу тощо. Комбіновані методи захситу в інформаційному просторі передбачають уміле поєднання описаних логічних і технічних методів у контексті конкретної ситуації.

Із точки зору протидії загрозам у кіберсфері вельми корисним виглядає підхід, викладений у імплементованих Україною міжнародних стандартах ISO/IEC 27-ї серії, які передбачають побудову на об'єктах інформаційної діяльності системи управління інформаційною безпекою.

В описаних станадартах комплексно викладаються питання:

– загальних проблем безпеки в інформаційних системах;

– розробки базової концепції та відповідних внутрішніх регулюючих нормативних документів щодо побудови та ефективного застосування політик безпеки;

– створення планів захисту, моніторингу та відновлення критичних інформаційних систем;

– важливості забезпечення безпеки не лише технічних, а й людських ресурсів;

– проведення аудиту, аналізу й оцінки потенційних загроз і ризиків інформаційних систем;

– безпечної взаємодії з розробниками/постачальниками інформаційних систем та програмного забезпечення;

– управління інцидентами інформаційної безпеки.

В умовах агресії Російської Федерації захист вітчизняного інформаційного та кіберпростору є одним із пріоритетів держави в цілому та правоохоронних органів зокрема. Використання ефективних рішень і захисних механізмів в описаній сфері дозволить побудувати надійний рубіж оборони України та суттєво вдосконалити національний сектор безпеки.

Одержано 07.04.2022

УДК 65.012.8
ШВЕЦЬ Дмитро Володимирович,
доктор юридичних наук, доцент,
заслужений працівник освіти України,
перший проректор Харківського національного
університету внутрішніх справ
https://orcid.org/0000-0002-1999-9956

РИЗИКИ ТОРГІВЛІ ЛЮДЬМИ В КОНТЕКСТІ ВІЙНИ РОСІЇ ПРОТИ УКРАЇНИ

Війна, розв'язана Російською Федерацією проти України, завдає шкоди всім сферам життя нашої Батьківщини. Жахливі злочини, які вчинюються окупантами, змусили світ здригнутися та по-іншому поглянути на режим В. Путіна, виступити з однозначним засудженням військових злочинів і злочинів проти людяності, що вчиняються його збоченими військами та наймитами.

Означені дії агресора потребують юридичного документування з метою подальшого притягнення винних до відповідальності. Одними із пріоритетних питань, які потребують прискіпливої уваги правоохоронних органів, є виявлення, фіксація та належне юридичне супроводження розслідування злочинів, пов'язаних із торгівлею людьми. У цьому контексті слід виділити декілька напрямів, що породжують суттєві ризики вчинення злочинів торгівлі людьми та інших супутніх правопорушень.

Передусім це різке збільшення кількості мігрантів, які виїжджають за кордон із території України. Оскільки виїзд чоловіків призовного віку переважно заборонений, жіноча половина роз'єднаних сімей може потрапити до трудової або сексуальної експлуатації.

Міжнародна організація з міграції, Агентство ООН з питань міграції застерігають, що випадки, пов'язані з торгівлею людьми, складно ідентифікувати під час масового переміщення людей, попередні повідомлення в Україні та за її межами свідчать про те, що торговці людьми готуються скористатися вразливістю тих, хто змушений покинути Україну. Міжнародна організація з міграції також звертає увагу на зростання випадків роз'єднання сімей, появу дітей, які переміщуються без супроводу або зазнали роз'єднання з родичами, а також імовірність випадків сексуального насильства, пов'язаного з конфліктом. Усе це становить серйозні ризики у сфері захисту, що пов'язані з торгівлею людьми. Втрата роботи і доходу внаслідок війни, обмежені можливості забезпечити головні потреби внутрішньо переміщених осіб, біженців і загалом постраждалого від війни населення призведуть до зростання ризиків [1].

У розрізі війни в Україні комісар Євросоюзу з внутрішніх справ І. Йоханссон зазначила про небезпеку потрапляння дітей до тенет торговців людьми: «Існує величезний ризик, що вразливими дітьми будуть торгувати, або вони стануть жертвами примусового усиновлення. Ми всі знаємо з досвіду, що, коли у нас є великі потоки міграції, завжди є люди, які отримують вигоду від ситуації та використовують вразливих жінок і дітей як жертв торгівлі людьми» [2].

Ще один напрям, про який не можна забувати, – це насильницьке та без згоди переміщення громадян України на територію країни-агресора та на окуповані території. Широко відомі випадки, коли громадян України з Донецької та Луганської областей без їхньої згоди відправляли до Ростовської, Бєлгородської, Владимирської, Пензенської областей та в Крим [3]. Із окупованих частин Харківської області виїзд дозволяють тільки в бік Білгородської області Російської Федерації. Багатьох українців вивезли до найвіддаленіших регіонів Росії, очевидно, щоб ускладнити їм повернення на територію України. Так, 8 квітня 2022 р. до Чебоксарів депортували 466 людей, з них 106 дітей, 308 маріупольців вивезено на Далекий Схід, у місто Находка Приморського краю [4].

Особливу категорію вивезених становлять діти. На російському телебаченні було продемонстровано сюжети, які засвідчують факт розміщення українських дітей у російських сім'ях із можливістю їх подальшого всиновлення. Не виключено, що в подальшому щодо них можуть учинятися інші категорії злочинів, у тому числі щодо примусового донорства (пропозиції щодо примусового донорства крові українських військовополонених для поранених окупантів лунали у Держдумі Росії), сексуальної експлуатації, створення дитячої порнографії, залучення до жебрацтва тощо.

Усі ці факти потребують ретельної правової оцінки, надання таким протиправним діянням належної кваліфікації. Чи є в таких діях ознаки геноциду, адже діти втрачатимуть українську ідентичність? Такі дії дещо нагадують практику підготовки яничарів, яких також виховували з українських дітей. Історія повторюється.

Наші ключові завдання – не допустити продовження цієї ганебної практики, притягнути винних до відповідальності та перемогти.

Список використаних джерел

1. Через війну Росії проти України зростають ризики торгівлі людьми, – МОМ // Організація Об'єднаних Націй Україна : сайт. 18.03.2022. URL: https://ukraine.un.org/uk/175247-cherez-viynu-rosiyi-proty-ukrayiny-zrostayut-ryzyky-torhivli-lyudmy-mom (дата звернення: 17.04.2022).

2. Орлова В. Через війну українські діти можуть стати жертвами торгівлі людьми – Єврокомісія // УНІАН : сайт. 21.03.2022. URL: https://www.unian.ua/war/cherez-viynu-ukrajinski-diti-mozhut-stati-zhertvami-torgivli-lyudmi-yevrokomisiya-novini-vtorgnennya-rosiji-v-ukrajinu-11753401.html (дата звернення: 17.04.2022).

3. «Ми вже шукаємо понад 16 тисяч людей» – Денісова про воєнні злочини, зниклих безвісти та вивезених у РФ // Суспільне : сайт. 26.04.2022. URL: https://suspilne.media/232328-mi-vze-sukaemo-ponad-16-tisac-ludej-denisova-pro-voenni-zlocini-zniklih-bezvisti-ta-vivezenih-u-rf/ (дата звернення: 27.04.2022).

4. Депутат Госдумы от ЛДПР Сергей Леонов выступил с инициативой, чтобы украинские военнопленные «в обязательном порядке» сдавали кровь для лечения мирного населения и российских военных, «пострадавших от действий ВСУ» // Telegram : соц. мережа. 21.04.2022. URL: https://t.me/FastFocus/16695 (дата звернення: 23.04.2022).

Одержано 29.04.2022

УДК 343.43+004

БАНДУРКА Олександр Маркович,
доктор юридичних наук, професор,
академік Національної академії правових наук України,
заслужений юрист України,
професор кафедри теорії та історії держави і права факультету № 1
Харківського національного університету внутрішніх справ
https://orcid.org/0000-0002-0240-5517

ПРІОРИТЕТНІ ТЕХНОЛОГІЇ ЦИФРОВІЗАЦІЇ ОРГАНІВ СИСТЕМИ МВС УКРАЇНИ

Цифрові технології відкривають унікальні перспективи для розвитку Міністерства внутрішніх справ України та органів системи МВС як частини сектору національної безпеки. Оптимізація єдиної інформаційної системи триває. Завдяки застосуванню новітніх технологій, що були використані при створенні та впровадженні ЄІС МВС, вдалося досягнути значних успіхів в економії бюджетних коштів шляхом мінімізації аутсорсингових контрактів на супроводження програмних продуктів, що використовуються в системі МВС, оскільки досягнуто можливостей їх самостійного розвитку та супроводження. Фактично передбачається

використання коштів, що раніше витрачалися на підтримку аналогових автоматизованих систем.

Моніторинг результатів реалізації завдань, визначених галузевою програмою інформатизації на 2018–2020 роки, підтвердив необхідність розроблення та застосування комбінованої стратегії з подальшої інформатизації органів системи МВС, в якій необхідно передбачити місце як довгостроковим заходам у масштабі в цілому на всю систему, так і короткостроковим швидким заходам, що більш релевантні для реалізації в окремих сегментах системи МВС, визначення критеріїв впливу чинників на розвиток інформатизації органів системи МВС, головних перешкод для користування цифровими технологіями та конкретними інструментами. Отже, є потреба в гнучких, реактивних трансферах прогресивних технологій та імплементації інноваційних методик інформатизації органів системи МВС із метою завершення як розпочатих проєктів, так і втілення проєктів, спрямованих на подолання нових викликів, що постають перед органами системи МВС [1].

Масштабні зміни, що відбуваються останнім часом у державі у сфері цифровізації, потребують переосмислення низки проєктів, які планувалося реалізувати в межах галузевої програми інформатизації, яка була розрахована на 2018–2020 роки. Серед цих проєктів: формування на рівні держави в цілому і регіонів зокрема комплексної автоматизованої багаторівневої системи забезпечення громадської безпеки, правопорядку і безпеки середовища проживання населення, що базується на сучасних підходах до моніторингу, прогнозування, запобігання вчиненню правопорушень, виникненню пригод і надзвичайних ситуацій та реагування на них, в умовах збереження високого рівня ризиків техногенного і природного характеру та триваючої тенденції до урбанізації як одного з важливих елементів створення стійкого соціально-економічного розвитку та зростання інвестиційної привабливості України; автоматизація планування та управління об'єднаними силами із забезпечення громадської безпеки та ліквідації надзвичайних ситуацій, а також подальше вдосконалення автоматизації міграційних процесів та управління кордонами; розбудова національних електронних інформаційних ресурсів у сфері забезпечення безпеки дорожнього руху, в тому числі модернізації Єдиного державного реєстру МВС та системи фіксації адміністративних правопорушень у сфері забезпечення безпеки дорожнього руху в автоматичному режимі щодо зареєстрованих транспортних засобів та їх власників [2]; подальша розбудова ІТ-інфраструктури органів системи МВС, у тому числі інфраструктури комунікацій; побудова комплексних систем захисту інформації інформаційно-телекомунікаційних систем з урахуванням вимог щодо кіберзахисту таких систем; подальша гармонізація нормативної бази, яка регулює процеси цифровізації органів системи МВС, осмислення і підготовка відповідних законодавчих ініціатив; запровадження обов'язковості цифрових компетенцій для працівників органів системи МВС із застосуванням підходу з урахуванням наскрізної (кросплатформеної) цифрової компетентності, тобто через використання цифрових технологій із супутнім розвитком цифрових навичок.

Галузева програма інформатизації системи Міністерства внутрішніх справ України та центральних органів виконавчої влади, діяльність яких спрямовується і координується Кабінетом Міністрів України через Міністра внутрішніх справ України, на 2021–2023 роки має фокусуватися на: розбудові публічних сервісів ЄІС МВС, упровадженні та модернізації національних електронних інформаційних ресурсів як складових ЄІС МВС, створенні інноваційної інфраструктури органів системи МВС, підвищенні довіри і безпеки при використанні ІКТ; створенні в новостворених функціональних підсистемах ЄІС МВС комплексних систем захисту інформації та вжитті заходів із забезпечення кіберзахисту цих систем; подальшій структуризації законодавчих та нормативно-правових документів сфери інформатизації органів системи МВС.

Список використаних джерел

1. Концепція програми інформатизації системи Міністерства внутрішніх справ України та центральних органів виконавчої влади, діяльність яких спрямовується і координується Кабінетом Міністрів України через Міністра внутрішніх справ України, на 2021–2023 роки : затв. Рішенням колегії МВС України від 22.04.2021 № 5км.

2. Цифрова трансформація інтеграції відомчих інформаційних ресурсів (ЄІС МВС) //

Цифрова держава : сайт. URL: https://plan2.diia.gov.ua/projects (дата звернення: 29.04.2022).

3. Деякі питання цифрової трансформації : Розпорядження Кабінету Міністрів України від 17.02.2021 № 365-р // База даних «Законодавство України» / Верховна Рада України. URL: https://zakon.rada.gov.ua/laws/show/365-2021-р (дата звернення: 29.04.2022).

Одержано 30.04.2022

УДК 004.04:004.67:004.77

БОРТНИК Сергій Миколайович,
доктор юридичних наук, доцент,
проректор Харківського національного університету внутрішніх справ
https://orcid.org/0000-0002-5281-6007

ОКРЕМІ АСПЕКТИ ПРОТИДІЇ ЛЕГАЛІЗАЦІЇ ДОХОДІВ, ОДЕРЖАНИХ У РЕЗУЛЬТАТІ ВЧИНЕННЯ КІБЕРЗЛОЧИНІВ

За останні десятиліття інтернет і в більш широкому сенсі кіберпростір вплинули на всі верстви суспільства. Наше повсякденне життя, основні права, соціальна взаємодія та економіка залежать від безперебійної роботи інформаційних і комунікаційних технологій. Відкритий та вільний кіберпростір сприяє політичній і соціальній інтеграції в усьому світі. Інтернет зруйнував бар'єри між країнами, спільнотами та громадянами, дав можливість взаємодіяти, обмінюватися інформацією та ідеями по всьому світу. Кіберпростір дав форум для свободи вираження думок і здійснення основних прав, а також розширив можливості людей у прагненні до більш демократичного та справедливого суспільства.

Щоб кіберпростір залишався відкритим і вільним, в інтернеті повинні застосовуватися ті самі норми, принципи та цінності, що існують в автономному режимі. Тому в кіберпросторі необхідно захищати основні права, демократію та верховенство закону від кіберзлочинності.

Поняття «кіберзлочинність» уперше з'явилося в американській, а потім і в іншій іноземній літературі на початку 1960-х років і означало порушення чужих прав та інтересів відносно автоматизованих систем обробки даних [1].

Згідно із Законом України «Про основні засади забезпечення кібербезпеки України» кіберзлочинність – це сукупність кіберзлочинів. Кіберзлочин (комп'ютерний злочин) – це суспільно небезпечне винне діяння у кіберпросторі та/або з його використанням, відповідальність за яке передбачена законом України про кримінальну відповідальність та/або яке визнано злочином міжнародними договорами України [2].

Найбільш поширеними способами відмивання злочинних доходів, які використовують у своїй діяльності кіберзлочинці, є:

– перерахування коштів на карткові та корпоративні рахунки фізичних осіб із подальшим зняттям готівкою, в тому числі через банкомати;

– переміщення коштів через рахунки фізичних та юридичних осіб з подальшим придбанням товарів та послуг через інтернет;

– переведення коштів в електронні гроші та подальше обготівковування або придбання товарів;

– обмін/розміщення коштів на електронних гаманцях [3].

Попередження кіберзлочинності базується на заходах, спрямованих на зниження ризику здійснення таких злочинів та нейтралізацію шкідливих наслідків для суспільства і приватного сектора. Ефективна протидія кіберзлочинам повинна поєднувати в собі комплекс правових (законодавчих), технічних, організаційних та інформаційних заходів [4].

Удосконалення нормативно-правового забезпечення у сфері попередження та протидії легалізації доходів, пов'язаних зі злочинами у сфері кіберзлочинності, можливе за такими напрямами:

– внесення змін до чинного Кримінального кодексу України щодо посилення відповідальності за злочини у сфері комп'ютерних та інформаційних технологій;

– визнання електронних документів та інших даних як доказової бази при розслідуванні кіберзлочинів;

– введення сертифікації електронних платіжних засобів;

– обов'язок банків встановити антискімингові пристрої на всіх банкоматах тощо.

Із метою попередження кіберзлочинів банківськими установами можуть упроваджуватися такі технічні й організаційні заходи:

– періодичний огляд банкоматів для виявлення незаконно встановлених пристроїв;

– вимоги щодо двофакторної/двоканальної аутентифікації;

– обов'язкове інформування клієнтів про кожну проведену операцію;

– підтвердження платежу в телефонному режимі тощо.

У зв'язку з цим значну користь у попередженні кіберзлочинності мають інформаційно-просвітницькі заходи щодо нових ризиків і загроз в інформаційних та комп'ютерних системах [5].

Таким чином, можна зробити висновок, що кіберзлочинність є порівняно новим видом суспільно небезпечних діянь, проте, на відміну від традиційних крадіжок і шахрайства, вона постійно вдосконалюється і «йде в ногу» з технологіями, що, у свою чергу, ускладнює виявлення та протидію зазначеним протиправним діям. Ефективний контроль за кіберзлочинністю вимагає більш інтенсивного міжнародного співробітництва, ніж існуючі заходи з боротьби з будь-якими іншими формами транснаціональної злочинності. Протидія кіберзлочинам поєднує в собі комплекс правових, технічних, організаційних та інформаційних заходів, при цьому роль кожного із цих заходів не може бути визначена пріоритетною чи другорядною. Ефективна протидія відмиванню злочинних доходів і зниження рівня злочинності в цій сфері можливі завдяки своєчасному виявленню фінансових операцій, що можуть бути пов'язані з відмиванням доходів, одержаних у сфері кіберзлочинності, та ефективному співробітництву між державним та приватним сектором.

Список використаних джерел

1. Міщук Н. Кіберзлочинність як загроза інформаційному суспільству. *Вісник Львівського університету. Серія економічна*. 2014. № 51. URL: http://publications.lnu.edu.ua/bulletins/index.php/economics/article/view/5886/5899 (дата звернення: 28.04.2022).

2. Про основні засади забезпечення кібербезпеки України : Закон України від 05.10.2017 № 2163-VIII // База даних (БД) «Законодавство України» / Верховна Рада (ВР) України. URL: https://zakon.rada.gov.ua/laws/show/2163-19 (дата звернення: 28.04.2022).

3. Схеми: Легалізація коштів від кіберзлочинів // Академія фінансового моніторингу : сайт. 05.04.2019. URL: https://finmonitoring.in.ua/sxemi-legalizaciya-koshtiv-vid-kiberzlochiniv/ (дата звернення: 28.04.2022).

4. Про затвердження Типологій легалізації (відмивання) доходів, одержаних злочинним шляхом, у 2013 році : Наказ Держ. служби фінансового моніторингу України від 25.12.2013 № 157 // БД «Законодавство України / ВР України. URL: https://zakon.rada.gov.ua/rada/show/v0157827-13 (дата звернення: 28.04.2022).

5. Департамент фінансових розслідувань // Державна служба фінансового моніторингу України : сайт. URL: http://www.sdfm.gov.ua/content/file/Site_docs/2013/20131230/tipolog2013.pdf (дата звернення: 28.04.2022).

Одержано 29.04.2022

УДК 342:343.346.8
БУРДІН Михайло Юрійович,
доктор юридичних наук, професор,
проректор Харківського національного університету внутрішніх справ
https://orcid.org/0000-0002-6748-3321

БЕЗПЕКА І КРИМІНАЛІСТИЧНА ЕКСПЕРТИЗА ІНТЕРНЕТУ РЕЧЕЙ: ПРОБЛЕМИ ТА АНАЛІЗ НАПРЯМІВ ПРОТИДІЇ КІБЕРЗЛОЧИННОСТІ

Інтернет речей (далі – IoT) передбачає повноцінні, підключені та розумні вузли, які взаємодіють автономно, пропонуючи всілякі послуги. Вузли IoT здатні надавати дані, отримувати доступ до хмарних ресурсів і авторизувати їх для збору та вилучення даних і прийняття рішень шляхом аналізу зібраних даних. Широке поширення, відкритість і відносно невисока обчислювальна потужність об'єктів IoT зробили їх ідеальною мішенню для кібератак. Більше того, оскільки багато вузлів IoT збирають і обробляють приватну інформацію, вони стають цінним джерелом даних для зловмисників. Тому безпека і, зокрема, здатність виявляти скомпрометовані вузли разом із збором і збереженням доказів атаки або зловмисної діяльності стають *актуальним завданням* успішного розгортання мереж IoT.

Питання безпеки, такі як конфіденційність, контроль доступу, безпечне спілкування та безпечне зберігання даних, стають серйозними проблемами в середовищі IoT. Швидке зростання пристроїв і сервісів IoT призвело до розгортання багатьох вразливих і незахищених вузлів. Більше того, звичайні архітектури безпеки, керовані користувачами, мало використовуються в об'єктних мережах IoT. Тому потрібні нові спеціалізовані інструменти, методи та процедури забезпечення безпеки мереж IoT і збір, збереження та аналіз залишкових доказів IoT середовищ. До основних проблем безпеки, які існують у середовищах IoT, належать такі.

Автентифікація. У домені IoT автентифікація дозволяє інтегрувати різні пристрої інтернету речей, які розгорнуті в різних контекстах. Процес автентифікації включає в себе автентифікацію однорангових маршрутизаторів, які беруть участь у передаванні даних, а також автентифікацію маршруту джерела даних. Ефективне розгортання ключів і керування ними є проблемою для автентифікації пристроїв IoT. Будь-яке генерування криптографічних ключів і обмін ключами не повинні спричиняти великих витрат на вузли інтернету речей.

Авторизація та контроль доступу. Авторизація передбачає специфікацію прав доступу до різних ресурсів під час керування доступом, при цьому кожен вузол IoT може підтримувати лише обмежені інструменти перевірки доступу.

Конфіденційність. Розгортання автономних об'єктів в IoT, які сприймають персональні дані людей, створює новий рівень загрози для приватності людей. Існуючі інструменти забезпечують конфіденційність, орієнтовану на користувача, і вимагають використання об'єктно орієнтованих моделей забезпечення конфіденційності.

Безпечна архітектура. Будь-яка архітектура інтернету речей повинна вирішувати не лише названі вище проблеми безпеки, але і ті, які виникають при розгортанні пристроїв IoT через програмно-визначені мережі та хмарну інфраструктуру

Проблеми криміналістики в середовищі IoT. У цьому напрямі коротко представляємо основні проблеми криміналістики в середовищах IoT.

Ідентифікація, збір і збереження доказів. Обшук і виїмка є важливим етапом будь-якої судово-комп'ютерної експертизи. Однак виявити наявність цих доказів у системі IoT є досить складним завданням, оскільки ці пристрої призначені для роботи автономно. Навіть у більшості випадків, коли ідентифіковано пристрій IoT, немає задокументованого методу чи надійного інструменту для збору залишкових доказів із пристрою судово обґрунтованим способом. Більше того, існують дуже обмежені методи створення криміналістичного образу такого пристрою IoT, які ігнорують етичні міркування під час збору доказів із пристроїв, що працюють у середовищі з багатьма орендарями. Збереження сцени є величезною проблемою

в середовищі IoT. У режимі реального часу й автономних взаємодій між різними вузлами дуже важко або взагалі неможливо визначити масштаби компромісу та межі місця злочину.

Аналіз доказів і кореляція. Більшість вузлів IoT не зберігають жодних метаданих, враховуючи тимчасову інформацію, що робить походження доказів проблемою для дослідника. За відсутності тимчасової інформації, такої як час зміни, доступу та створення, кореляція доказів, зібраних з різних пристрої IoT, практично неможлива. Крім технічних проблем, конфіденційність є основною проблемою, яку слід враховувати під час аналізу та співвіднесення зібраних даних. Більше того, величезному обсягу даних, який збирається в неоднорідних середовищах IoT, майже неможливо надати наскрізний аналіз залишкових доказів.

Всі джерела доказів щодо пристроїв на основі IoT можуть бути поділені на три групи: 1) докази, зібрані з розумних пристроїв і датчиків; 2) докази, зібрані з апаратного та програмного забезпечення, які забезпечують зв'язок між розумними пристроями і зовнішнім світом; 3) докази, зібрані з апаратного та програмного забезпечення, які знаходяться поза межами мережі, що досліджується. До останньої групи входять хмара, соціальні мережі, постачальники послуг інтернету та мобільних мереж, віртуальні онлайн-ідентифікації та інтернет.

Політики хмарної кібербезпеки повинні бути інтегровані з інфраструктурою інтернету речей, щоб швидко реагувати на будь-які підозрілі проблеми діяльності. Політику слід переглянути з точки зору доказів ідентифікації, цілісності, збереження та доступності даних.

Зараз судово-комп'ютерна експертиза і дослідники з кібербезпеки досліджують інтернет речей з точки зору комп'ютерного судового аналітика щодо зібрання даних, вилучення доказів, обробки та аналізу доказів. Докази можуть бути зібрані за допомогою стаціонарних датчиків, що вбудовані у фізичні об'єкти, хмарних сховищ та навіть журналів ISP. Практичне вивчення цієї нової галузі дозволить визначити методи для виконання цифрового криміналістичного аналізу в середовищі IoT.

Таким чином, швидкі темпи розвитку та характер середовищ IoT створюють різноманітні проблеми безпеки та криміналістики. Надані матеріали пропонують сучасний погляд на проблеми конфіденційності, безпеки та криміналістичної експертизи в середовищах інтернету речей, а також інноваційні рішення, які прокладають шлях до безпечного та надійного розгортання мереж IoT.

Одержано 19.04.2022

УДК 342:343.346.8
ГУСАРОВ Сергій Миколайович,
доктор юридичних наук, професор,
заслужений юрист України,
член-кореспондент Національної академії правових наук України,
професор кафедри адміністративного права та процесу факультету № 1
Харківського національного університету внутрішніх справ
https://orcid.org/0000-0002-8136-0694

ЩОДО РОЗРОБКИ ПОЛІТИКИ БЕЗПЕКИ ОРГАНІЗАЦІЇ

Для того, щоб забезпечити визначені нормативними документами та стандартами принципи управління та підтримку безпеки інформації в конкретній організації, потрібно розробити концептуальний набір правил поведінки, який буде регулювати найважливіші питання, що стосуються безпеки інформації в інформаційних системах. Цей набір правил описує властивості системи, яка потребує захисту, та має назву «Політика безпеки». Політка безпеки формується як окремий документ. Цей документ ухвалюється керівництвом організації та обов'язково доводиться до відома персоналу й інших зацікавлених суб'єктів під підпис. Як правило, політика безпеки затверджується окремим наказом по організації, який на-

лежним чином реєструється. У цьому ж наказі доцільно прописати відповідальність за порушення вимог політики безпеки.

У нормативних документах поняття «політика безпеки» можна зустріти в Загальних вимогах до кіберзахисту об'єктів критичної інфраструктури, затверджених Постановою Кабінету Міністрів України від 19 червня 2019 р. № 518. З урахуванням зазначеного документа *політику безпеки* можна визначити як політику, що визначає підхід підприємства, установи та організації до інформаційної безпеки, вимоги, правила, обмеження, рекомендації, що регламентують порядок дотримання та забезпечення інформаційної безпеки. Політика безпеки є якісним (або якісно-кількісним) описом властивостей захищеності, вираженим у термінах, що описують систему. Саме особливості роботи з інформаційною системою організації складають більшу частину наповнення політики безпеки.

Методичною основою для створення та розробки політики безпеки є стандарти:

– ДСТУ ISO/IEC 27001:2015 «Інформаційні технології. Методи захисту. Системи управління інформаційною безпекою. Вимоги»;

– ДСТУ ISO/IEC 27002:2015 «Інформаційні технології. Методи захисту. Звід практик щодо заходів інформаційної безпеки».

Форма представлення політики безпеки може бути різною. В окремих випадках її представляють власною назвою, в інших позначають як інструкцію або правила. З точки зору управління безпекою інформації організації, це не повинно мати принципового значення.

Політики безпеки можуть охоплювати:

– всю інформаційну діяльність організації (саме такий вид політики безпеки описаний у стандартах ISO/IEC 27-ї серії);

– конкретну комп'ютерну систему або мережу організації. У цьому випадку часто говорять про вибір однієї з таких політик безпеки, як дискреційна, мандатна, рольова.

Типовими розділами політики безпеки можуть бути:

– вступ або загальні положення;

– терміни та скорочення;

– мета політики;

– сфера застосування;

– предмет документа й опис дій;

– ролі та відповідальність;

– перегляд політики.

У деяких випадках окремим розділом може подаватися перелік взаємопов'язаних документів.

В обов'язковому порядку слід ознайомити з правилами політики безпеки персонал організації, зібрати відповідні розписки. Для підтримання політики безпеки на належному рівні та виконання її всіма працівниками організації потрібно передбачити систему відповідного навчання персоналу, а також порядок і терміни оновлення політики безпеки організації.

Одержано 30.04.2022

УДК 351:343.431

КОБКО Євген Васильович,
кандидат юридичних наук, доцент,
доцент кафедри публічного управління та адміністрування
Національної академії внутрішніх справ
https://orcid.org/0000-0002-3121-0823

НАПРЯМИ ВДОСКОНАЛЕННЯ ПРАВОВОГО РЕГУЛЮВАННЯ ВЗАЄМОДІЇ СУБ'ЄКТІВ ЗАБЕЗПЕЧЕННЯ НАЦІОНАЛЬНОЇ БЕЗПЕКИ

Забезпечення національної безпеки в Україні, особливо в сучасних умовах, є складним процесом, ефективність реалізації якого залежить від того, наскільки уповноважені суб'єкти

будуть якісно та ефективно виконувати покладені на них обов'язки у відповідній сфері. Разом із тим, безспірним є той факт, що жоден із окреслених нами в рамках даного наукового дослідження не може самостійно вирішувати проблеми у сфері національної безпеки, а тому важливим завданням законодавця є створити необхідні правові та організаційні умови для їх взаємодії.

Спробою вирішити вказане у даному науковому дослідженні проблемне питання було у рішенні Ради національної безпеки і оборони України від 20 серпня 2021 року «Про запровадження національної системи стійкості», яка визначає мету, основні принципи, напрями, механізми і строки запровадження та функціонування національної системи стійкості, спрямованої на забезпечення здатності держави і суспільства своєчасно ідентифікувати загрози, виявляти вразливості та оцінювати ризики національній безпеці, запобігати або мінімізувати їх негативні впливи, ефективно реагувати та швидко і повномасштабно відновлюватися після виникнення загроз або настання надзвичайних та кризових ситуацій усіх видів, включаючи загрози гібридного типу, але не обмежуючись ними [1].

Вказану вище концепцію передбачається реалізувати протягом 2021-2025 років. За строками реалізації завдання поділяються на короткострокові (першочергові) (до 2-х років) та середньострокові (3-5 років). Основними короткостроковими (першочерговими) завданнями є: розроблення та прийняття законодавчих, інших нормативно-правових актів з питань забезпечення національної стійкості; аналіз наявних спроможностей щодо ресурсного, кадрового та фінансового забезпечення функціонування національної системи стійкості, визначення відповідних потреб та шляхів їх забезпечення; визначення органів, відповідальних за координацію діяльності суб'єктів забезпечення національної стійкості на державному, регіональному та місцевому рівнях; налагодження ефективної координації та взаємодії суб'єктів забезпечення національної стійкості [1].

Основними інституційними проблемами, які потребують розв'язання на етапі запровадження національної системи стійкості, є: невизначеність інституційної моделі забезпечення національної стійкості; відсутність органів державної влади, відповідальних за координацію взаємодії державних та недержавних структур у сфері забезпечення національної стійкості на державному, регіональному та місцевому рівнях, у тому числі управління ризиками та забезпечення відповідних спроможностей, обґрунтування та формування необхідних резервів, ідентифікацію загроз національній безпеці та аналізування ризиків, формування і ведення національного реєстру ризиків, а також їх обробку; недосконалість механізмів організації і координації дій на національному рівні у сфері кризового менеджменту; відсутність механізмів і постійних форматів міжвідомчої взаємодії з питань забезпечення національної стійкості на державному, регіональному і місцевому рівнях; технічна, інженерна та матеріальна застарілість резервних пунктів управління органів державної влади; недостатній рівень забезпечення готовності до реагування та взаємодії органів державної влади і громадян в умовах виникнення загроз і настання кризових ситуацій, підтримання функціонування базових елементів національної системи стійкості; відсутність методик прогнозування, запобігання та реагування на ризики та кризові ситуації на різних етапах їх розвитку, а також планів відновлення сталого функціонування, з урахуванням потенційних каскадних ефектів [1].

Незважаючи на всі позитивні зміни, які запропоновані до запровадження «Концепцією забезпечення національної системи стійкості», всіх проблем, пов'язаних із взаємодією та координацією суб'єктів забезпечення національної безпеки в Україні. З огляду на зазначене вище, ми пропонуємо розробити новий підзаконний нормативно-правовий акт: «Положення про взаємодію та координацію суб'єктів забезпечення національної безпеки», в якому необхідно:

– по-перше, визначати уповноважений орган, який буде відповідати за координацію суб'єктів забезпечення національної безпеки, зокрема: а) розкрити його правовий статус; б) встановити межі його впливу на суспільні відносини у даному напрямку; в) визначити межі відповідальності уповноваженого суб'єкта координації;

– по-друге, окреслити коло суб'єктів забезпечення національної безпеки, а також встановити межі їх компетенції щоб уникнути дублювання завдань та функцій, які вони виконують у відповідній сфері;

– по-третє, закріпити форми та методи взаємодії відповідних суб'єктів;

– по-четверте, окреслити джерела фінансування спільної діяльності органів та їх посадових осіб під час здійснення спільної діяльності.

Список використаних джерел

1. Про рішення Ради національної безпеки і оборони України від 20 серпня 2021 року "Про запровадження національної системи стійкості" / Указ Президента України від 27.09.2021 № 479/2021 URL: https://zakon.rada.gov.ua/laws/show/479/2021/conv#Text (дата звернення: 17.03.2022).

Одержано 27.04.2022

УДК 343

НАЗАРЕНКО Ігор Віталійович,
кандидат юридичних наук,
декан факультету № 4
Харківського національного університету внутрішніх справ

ЩОДО НОРМАТИВНО-ПРАВОВОЇ БАЗИ КІБЕРБЕЗПЕКИ В УКРАЇНІ

У Законі України «Про основні засади забезпечення кібербезпеки України» від 05.10.2017 **кібербезпека** визначається як захищеність життєво важливих інтересів людини і громадянина, суспільства та держави під час використання кіберпростору, за якої забезпечуються сталий розвиток інформаційного суспільства та цифрового комунікативного середовища, своєчасне виявлення, запобігання і нейтралізація реальних і потенційних загроз національній безпеці України у кіберпросторі.

Актуальні загрози кібербезпеці та шляхи їх блокування викладено у підзаконних актах. Наприклад, ***Стратегія кібербезпеки України*** – це документ довгострокового планування,
що визначає загрози кібербезпеці України, пріоритети та напрями забезпечення кібербезпеки України з метою створення умов для безпечного функціонування кіберпростору, його використання в інтересах особи, суспільства і держави. Більш докладно структуру вказаного документа зображено на рис. 1.

Об'єктами кібербезпеки є:

1) конституційні права і свободи людини і громадянина;
2) суспільство, сталий розвиток інформаційного суспільства та цифрового комунікативного середовища;
3) держава, її конституційний лад, суверенітет, територіальна цілісність і недоторканність;
4) національні інтереси в усіх сферах життєдіяльності особи, суспільства та держави;
5) об'єкти критичної інфраструктури.

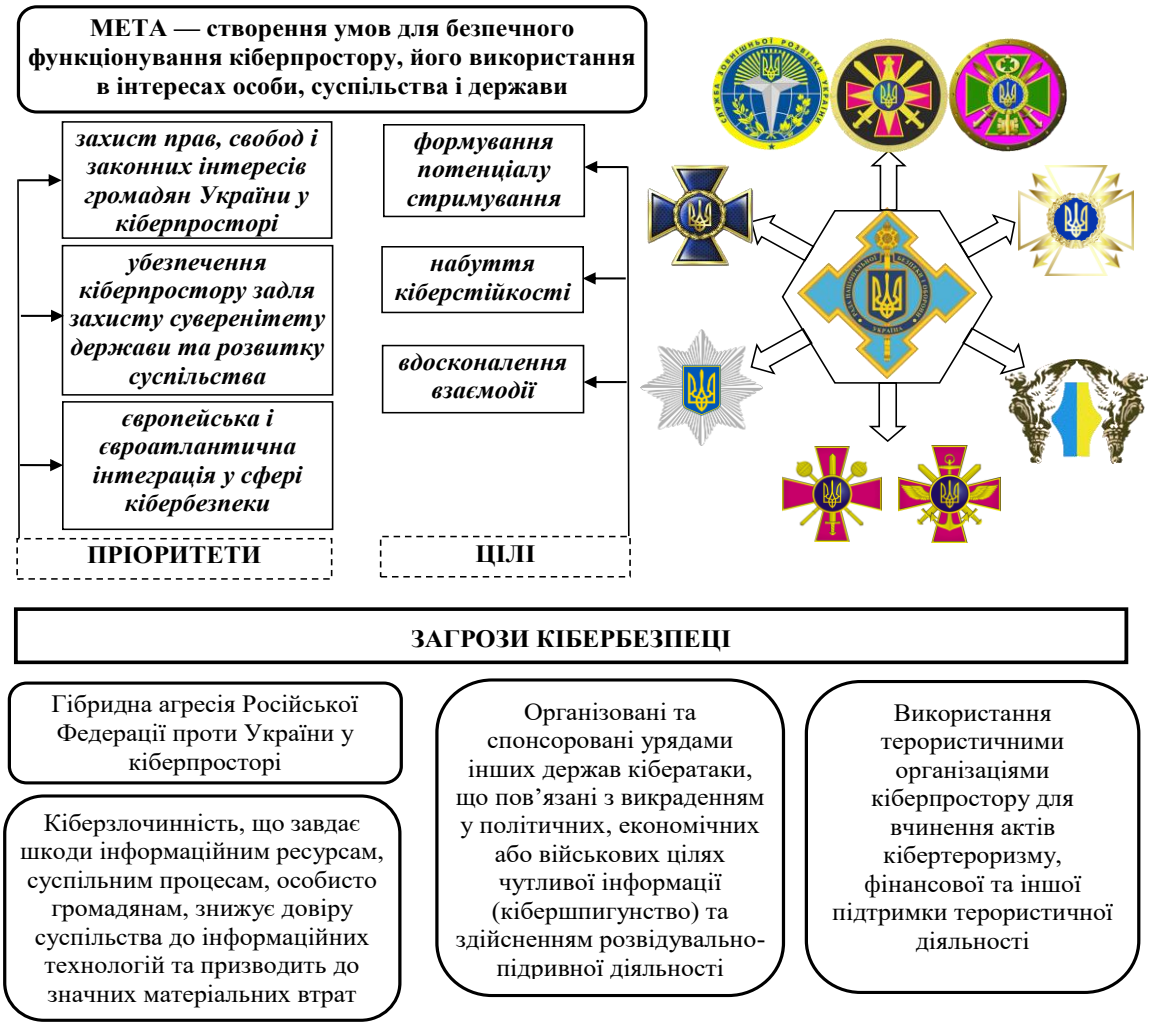

Рис. 1. Основні елементи стратегії кібербезпеки України

Цікавим нововведенням Стратегії кібербезпеки стало запровадження відповідних маркованих літерно-числовими ідентифікаторами стратегічних цілей (табл. 1).

Таблиця 1

Потенціал та стратегічні цілі кібербезпеки

Потенціал / **Цілі**	Стримування **(С)**	Кіберстійкість **(К)**	Удосконалення взаємодії **(В)**
1	*Дієва кібероборона*	*Національна кіберготовність та надійний кіберзахист*	*Зміцнення системи координації*
2	*Ефективна протидія розвідувально-підривній діяльності у кіберпросторі та кібертероризму*	*Професійне вдосконалення, кіберобізнане суспільство та науково-технічне забезпечення кібербезпеки*	*Формування нової моделі відносин у сфері кібербезпеки*
3	*Ефективна протидія кіберзлочинності*	*Безпечні цифрові послуги*	*Прагматичне міжнародне співробітництво*
4	*Розвиток асиметричних інструментів стримування*		

Для досягнення виділених цілей передбачено виконання цілої низки *завдань*.

Крім розглянутих документів, існує ціла низка відповідних методичних рекомендацій, які хоча і не є обов'язковими до виконання, проте можуть бути використані під час побудови системи кіберзахисту. Так, 06 жовтня 2021 року Адміністрація Держспецзв'язку наказом № 601 затвердила методичні рекомендації щодо підвищення рівня кіберзахисту критичної інформаційної інфраструктури. Рекомендації розроблені з урахуванням Настанови для підвищення кібербезпеки критичної інфраструктури (Framework for Improving Critical Infrastructure Cybersecurity), виданої у 2014 році та оновленої у 2018 році Національним інститутом стандартів та технології Сполучених Штатів Америки (National Institute of Standards and Technology).

Одержано 01.05.2022

УДК 343.431

ОНИЩЕНКО Юрій Миколайович,
кандидат наук з державного управління, доцент,
доцент кафедри кібербезпеки та DATA-технологій факультету № 6
Харківського національного університету внутрішніх справ
https://orcid.org/0000-0002-7755-3071;
БАБИЧ Олександр Юрійович,
курсант 2 курсу факультету № 4
Харківського національного університету внутрішніх справ

РИЗИКИ, ПОВ'ЯЗАНІ З ТОРГІВЛЕЮ ЛЮДЬМИ, В УМОВАХ МІГРАЦІЇ УКРАЇНЦІВ ДО КРАЇН ЄС

На сьогоднішній день торгівля людьми постає як гостра проблема світового масштабу, це явище створює загрози безпеці у багатьох країнах світу та існує досить тривалий проміжок часу. Зазначена проблема не обійшла стороною і нашу державу, так згідно з проведеним опитування Міжнародної організації з міграції за період 2019-2021 рр. від торгівлі людьми постраждало 46 тисяч українців у тому числі дітей [1]. Торгівля людьми була досить важливою проблемою і раніше, але військові конфлікти та війни значно посилюють ризики пов'язані з торгівлею людьми. Це обумовлено збільшенням потоку біженців, які шукають прихисток у країнах Європейського Союзу. Люди масово приїжджають на вокзали міст країн Європи, де одразу починають шукати місце для ночівлі, роботу та захист. Через відсутність будь-якого плану, щодо поїздки найчастіше біженці звертаються до волонтерів та просто доброзичливих людей. Злочинні структури досить часто користуються страхом та невпевненістю людей, які опинились в незнайомій країні далеко від своєї домівки. Розгубленість, залякання та відсутність нормального правового захисту таких людей робить їх легкою мішенню для злочинної діяльності. Найчастіше злочинні формування використовують біженців як практично безоплатну робочу силу, забираючи у них документи та примушуючи працювати на себе або третіх осіб.

Наразі через війну в Україні люди масово їдуть до країн Європи, зокрема Польщі та Німеччини, у яких умови прийняття біженців найбільш сприятливі серед усіх інших. Так, за даними на початок травня 2022 року з України виїхало 6 мільйонів осіб [2]. Така кількість людей створює хаос на вокзалах, чим користуються злочинці.

Міжнародні гуманітарні організації б'ють на сполох через збільшення ризиків торгівлі людьми [3]. Вони намагаються цьому протистояти, привертаючи увагу правоохоронних структур. Поліція Берліну вже звернула на це увагу і почала попереджати про загрозу на своїх сторінках у соціальних мережах [4]. Вже зараз існують факти спроб використання українських жінок з метою сексуальної експлуатації. Так, у польському місті Люблін жінкам про-

понували прихисток під виглядом волонтерів, а натомість заманювали у «невідомі автомобілі» [5]. Досить небезпечною для наших громадян є ситуація у Німеччині, де активно працюють злочинні угрупування, що займаються торгівлею людьми [6]. Як заявляє активістка Хушке Мау: «Торговці людьми і сутенери знають, що біженці можуть принести їм багато грошей» [6].

Нажаль, від проблем торгівлі людьми потерпають і діти. Існують ситуації, коли діти самостійно без супроводу перетинали кордон держави [7]. Такі діти є найменш захищеними від злочинної діяльності, та практично не здатні самостійно захиститись від посягань на свої права, у тому числі пов'язаних з торгівлею людьми. Крім цього на тимчасового окупованих територіях війська росії незаконно вивозять дітей на свою територію після чого інформації щодо місця їх знаходження, умов проживання тощо немає, що фактично є легалізованим на державному рівні викраденням людини [8].

До первинних ознак вербування з боку злочинців, що займаються торгівлею людьми, можна віднести наступне: неофіційне працевлаштування, розмите формулювання у трудовому договорі, однакові або лише позитивні відгуки, відсутність відповідних сертифікатів щодо посередництва у працевлаштуванні, відмова надання документів, гіперболізовані заробітні плати або умови проживання, постійна зміна умов та прохання віддати паспорт [9].

Отже, на сьогоднішній день проблема торгівлі людьми носить особливо важливий характер, адже війна з росією призвела до масового потоку біженців до країн Європи. Ці люди часто, тікаючи від війни, опиняються в містах країн заходу без реальної допомоги та захисту, що робить останніх легкими мішенями для злочинців, які можуть оманою або силою затягнути людину у рабство.

Вберегтись від торгівлі людьми можливо за допомогою активізації відповідної інформаційної кампанії, збільшення кількості тренінгів з особами, які найбільш вразливі для злочинців з торгівлі людьми; перевірки осіб, які пропонують роботу/прихисток тощо через знайомих, офіційні органи; використання біженцями виключно офіційних джерел інформації, які пройшли перевірку. У випадках підозри – одразу звертатись до правоохоронних органів, прикордонної служби, працівників посольств та консульств. Також не варто передавати свої ідентифікуючі документи третім особам, погоджуватись на неофіційне працевлаштування.

Список використаних джерел

1. Через війну Росії проти України зростають ризики торгівлі людьми, - МОМ // Організація об'єднаних націй Україна : вебсайт. 18.03.2022. URL: https://ukraine.un.org/uk/175247-cherez-viynu-rosiyi-proty-ukrayiny-zrostayut-ryzyky-torhivli-lyudmy-mom (дата звернення: 25.04.2022).

2. Кількість біженців з України перевищила 6 мільйонів – ООН // Українська правда : вебсайт. 12.05.2022. URL: https://www.pravda.com.ua/news/2022/05/12/7345788/ (дата звернення: 17.05.2022).

3. Гуманітарні організації б'ють на сполох через ризик торгівлі людьми! Як не наражати себе на небезпеку? // EU NEIGHBOURS east : вебсайт. 22.03.2022. URL: https://euneighbourseast.eu/uk/news-and-stories/latest-news/gumanitarni-organizacziyi-byut-na-spoloh-cherez-ryzyk-torgivli-lyudmy-yak-ne-narazhaty-sebe-na-nebezpeku/ (дата звернення: 14.05.2022).

4. Warning notice of the Federal Police in Ukrainian and Russian language // Twitter : вебсайт. 08.03.2022. URL: https://twitter.com/bpol_b/status/1501226336483905540?s=20&t=47EYtCeILGebfdo0Uf5v-Q (дата звернення: 24.04.2022).

5. Уповноважений закликає європейські країни вжити заходів для недопущення потрапляння громадян України в ситуації торгівлі людьми // Уповноважений Верховної Ради України з прав людини : вебсайт. 25.03.2022. URL: https://www.ombudsman.gov.ua/news_details/upovnovazhenij-zaklikaye-yevropejski-krayini-vzhiti-zahodiv-dlya-nedopushchennya-potraplyannya-gromadyan-ukrayini-v-situaciyi-torgivli-lyudmi (дата звернення: 27.04.2022).

6. German police warn Ukraine refugees of human traffickers // Deutshe Welle : вебсайт. 10.03.2022. URL: https://www.dw.com/en/german-police-warn-ukraine-refugees-of-human-

traffickers/a-61086922 (дата звернення: 28.03.2022).

7. Діти, які тікають від війни в Україні, наражаються на підвищений ризик торгівлі людьми та експлуатації – ЮНІСЕФ // ЮНІСЕФ Україна : вебсайт. 20.03.2022. URL: https://www.unicef.org/ukraine/press-releases/children-fleeing-war-ukraine-heightened-risk-trafficking-and-exploitation (дата звернення: 24.04.2022).

8. Уповноважений: викрадених в Україні дітей рашисти влаштовують у свої сім'ї // Уповноважений Верховної Ради України з прав людини : вебсайт. 23.04.2022. URL: https://www.ombudsman.gov.ua/news_details/upovnovazhenij-vikradenih-v-ukrayini-ditej-rashisti-vlashtovuyut-u-svoyi-simyi (дата звернення: 25.04.2022).

9. Торгівля людьми – це не міф, це реальність! Через війну Росії проти України зростають ризики торгівлі людьми // Східне міжрегіональне управління Державної служби України з питань праці : вебсайт. 28.04.2022. URL: https://smu.dsp.gov.ua/news/torhivlia-liudmy-tse-ne-mif-tse-realnist-cherez-viinu-rosii-proty-ukrainy-zrostaiut-ryzyky-torhivli-liudmy/ (дата звернення: 29.04.2022).

Одержано 01.05.2022

РОЗДІЛ 2.
КРИМІНАЛЬНО-ПРАВОВІ, ПРОЦЕСУАЛЬНІ ТА КРИМІНАЛІСТИЧНІ АСПЕКТИ ПРОТИДІЇ КІБЕРЗЛОЧИННОСТІ ТА ТОРГІВЛІ ЛЮДЬМИ

УДК 343.9:[004.738.5:316.613.434]
КАЗНАЧЕЄВА Дар'я Володимирівна,
кандидат юридичних наук, доцент,
доцент кафедри кримінального права і кримінології факультету № 1
Харківського національного університету внутрішніх справ;
ДОРОШ Анастасія Олександрівна,
курсантка 4 курсу факультету № 2
Харківського національного університету внутрішніх справ

ВІКТИМНІСТЬ У КІБЕРПРОСТОРІ

Розвиток сучасного суспільства в світовому масштабі завжди визначається глобальними викликами сучасності. Серед них особливе місце займають виклики, пов'язані з розвитком і впровадженням цифрових технологій в різні сфери життєдіяльності людини і сучасного соціуму, які породжують не тільки позитивні зміни, але і певні загрози для його членів. Поступ людства до інформаційного суспільства, діджиталізацція економіки, культури та й побутового життя передбачає здійснення частини звичних практик у цифровому просторі (кіберпросторі): спілкування із близьким і віддаленим соціальним оточенням, а відтак набуття соціального досвіду із відповідним засвоєнням соціальних норм, цінностей і розбудовою стосунків; пошук інформації для забезпечення предметної діяльності, ведення поточних справ і забезпечення повсякденних потреб (фінансово-економічні, соціокультурні, громадсько-політичні аспекти людської діяльності також все більше набувають «оцифрованого» характеру).

На сьогодні людство переживає швидкий перехід різних сфер життєдіяльності до мережі «Інтернет», як то обіг безготівкових грошових коштів, неконтрольовані державою фінансові взаєморозрахунки у віртуальній (цифровий) валюті, кібершахрайство, кібербулінг тощо. За даними проведених досліджень Інтернетом регулярно користуються близька 71% українців і ця кількість постійно зростає [1].

Погоджуємось із думкою, що у масовій свідомості вже давно констатується розрив між технологіями, зокрема й інформаційними, та гуманітарною сферою, соціальним розвитком, і при цьому спостерігається неспіврозмірне, загрозливе випередження темпів розвитку перших [2, с.137].

Разом з тим зазначену динаміку злочинності загострило і введення в Україні з березня 2020 року особливих карантинних умов, викликаних пандемією COVID-19. Зазначений режим обмежив права громадян, перш за все, на свободу пересування. Тому багато хто з них був змушений залишатися в місцях проживання (перебування) та виконувати вимоги суворої самоізоляції. Вплив пандемії COVID-19 на економічну діяльність та соціальну поведінку спричинив стрімку трансформацію і організацію значного сегмента суспільних відносин у дистанційному режимі з широким використанням електронних сервісів та інформаційно-комунікаційних систем.

Можна спостерігати тенденцію до стрімкого зростання комп'ютерної злочинності, в першу чергу, фінансових шахрайств з використанням соціальної інженерії- вішинг, а також фішінга- жертвами яких ставали, в основному, клієнти банків. Активно використовувалася експлуатація теми протидії COVID-19 під виглядом шкідливих розсилок, посилилось залучення нових учасників до діяльності злочинних спільнот, упровадження нових технологій, цифрових послуг та механізмів електронної взаємодії громадян з державою, що здійснюється безсистемно в частині заходів з кібербезпеки та без належної оцінки ризиків. За даними звіту

Європолу щодо оцінки зареєстрованих злочинів режим карантину особливо позначився на зростанні кіберзлочинності, торгівлі контрафактними та неякісними товарами, а також різних видів шахрайства і схем, пов'язаних з організованою злочинністю [3].

Аналіз статистичних даних, а також наукових публікацій у нашій державі також підтверджують зазначену тенденцію. Так, наприклад, *«у вересні 2021 року працівники кіберполіції Херсонщини виявили протиправну діяльність трьох чоловіків, які видаючи себе за працівників служби безпеки банку випитували у громадян реквізити їхніх банківських карток та відомості для доступу до онлайн-банкінгу. Надалі через додаток онлайн-банкінгу фігуранти переказували гроші з карток потерпілих на підконтрольний рахунок» [4].*

В той же час *«у вересні 2021 року співробітники управління протидії кіберзлочинам м. Києва викрили правопорушника, який купував на анонімних форумах у мережі DarkNet бази авторизаційних даних користувачів різних програм лояльності відомих платіжних систем та компаній. За допомогою власноруч написаних скриптів із застосуванням автоматизованої системи, перевіряв їх відповідність до існуючих облікових записів громадян. Надалі - авторизувався в особистих кабінетах користувачів та привласнював гроші з їхніх бонусних рахунків. За попередніми підрахунками, у такий спосіб чоловік ошукав понад сотню осіб» [5].*

Можна зазначити, що такі особливості цифровізації суспільства, як 1) змагальний характер розвитку засобів кібербезпеки в умовах швидких прогресуючих змін інформаційно-комунікаційних технологій, зокрема хмарних та квантових обчислень, 5G-мереж, великих даних, Інтернету речей, штучного інтелекту, а також 2) стрімка віртуалізація реальності, 3) інформаційна соціалізація, 4) зниження емоційного інтелекту, породжують певні загрози суспільству і державі в цілому.

Саме для запобігання та протидії кіберзлочинності у 2001 р. у Будапешті була прийнята Конвенція про кіберзлочинність, яка була ратифікована Верховною Радою України із застереженнями і заявами Законом № 2824-IV від 07.09.2005 р. Крім того, в Україні прийнято Закон «Про основні засади забезпечення кібербезпеки України» № 2163-VIII від 5 жовтня 2017 р. Однак, швидко змінюваний цифровий світ потребує формування більш збалансованої та ефективної національної системи кібербезпеки, яка зможе гнучко адаптуватися до змін безпекового середовища, гарантуючи громадянам України безпечне функціонування національного сегмента кіберпростору, передбачивши нові можливості для цифровізації всіх сфер суспільного життя. Саме для виконання цих завдань у серпні 2021 року Указом Президента України № 447/2021 затверджено Стратегію кібербезпеки України.

Наведені вище аргументи, на нашу думку, свідчать про необхідність та доцільність не тільки вивчення кіберзлочинності, а й «корпусу» її жертв.

На сьогодні немає єдиної думки щодо визначення та предмету віктимології. Однак можна цілком погодитись із думкою О.М. Джужи, «…що особливе значення для кримінологічної науки має розвиток кримінологічної віктимології як комплексної міждисциплінарної галузі, що досліджує проблему жертви злочину з позиції кримінального, кримінально-процесуального, кримінально-виконавчого права, криміналістики та кримінології» [6, с. 134].

З іншого боку, як справедливо зауважують О.М. Литвинов та Ю.В. Орлов, розмаїття ситуацій, що виникають під час вчинення злочинів, з очевидністю свідчить про необхідність вивчення жертви злочину. В її структурі віктимологічно значущою може виявитись будь-яка з безлічі людських властивостей: від анатомічних та біологічних до психологічних та соціальних. І однозначно не можна сказати, які дії потерпілого здатні спровокувати вчинення злочину. Тому дійсно особу, яка вчиняє злочин, потерпілого та особливості ситуації вчинення злочину варто розглядати як дві частини одного цілого - системи механізму злочинної поведінки [2, с. 164-165].

На нашу думку, проблема вивчення жертв протиправних посягань, що вчиняються у кіберпросторі, є однією із фундаментальних для сучасної науки з певних причин.

По-перше, на сьогодні взагалі недостатньо досліджень та даних щодо зазначеної категорії потерпілих, також треба наголосити, що за даними ООН близька 80 % потерпілих взагалі не звертаються до правоохоронних органів [8, с. 25].

По-друге, розвиток цифрових технологій та їх стрімка розповсюдженість серед населення значно підвищує кількість потерпілих від зазначеної категорії злочинних посягань.

По-третє, вивчення жертв протиправних посягань, що вчиняються у кіберпросторі буде сприяти виявленню масштабів цього явища та допоможе розробити заходи профілактики останньому.

В рамках дослідження ми вирішили провести анкетування молоді, а саме курсантів та студентів нашого університету у віці від 18 до 22 років у кількості 290 респондентів щодо їх досвіду у мережі Інтернет, а також випадків індивідуальної віктимізації у цій сфері. Із загальної кількості опитаних 65% склали особи чоловічої статі, 35% - жіночої.

Так, на питання «Як часто Ви користуєтесь мережею Інтернет?» - 99% респондентів відповіли, що підключаються до Інтернету кожен день. А 91% - щоденно користуються соціальними мережами.

Щодо випадків передачі персональних даних, а саме реквізитів документів, адрес, номерів телефонів або адрес електронної пошти стверджено відповіли 87% опитаних (див. табл. 1.).

Таблиця 1

Структура передачі конфіденційної інформації в мережі Інтернет

Ресурс	% від загальної кількості респондентів
Державні послуги	65 %
Веб банкінг	79 %
Онлайн магазини	53 %
Запис до медзакладів	41 %
Сайти перевізників (наприклад, Укрзалізниця)	67 %
Реєстрація на різних тематичних порталах	38 %
Сайти оголошень (наприклад, OLX)	27 %

На запитання «Чи траплялись по відношенню до Вас неправомірні діяння у мережі Інтернет?» - 72 % респондентів відповіли, що так. Після проведеного опитування було виокремлено основні кібер загрози, або можна сказати різні форми віктимізуючих діянь (див. табл. 2.).

Таблиця 2

Структура віктимізації в мережі Інтернет

Вид діяння	% від загальної кількості респондентів
злом почтової скрині аба акаунту у соцмережі	36 %
розповсюдження від мого імені неправдивої інформації	24 %
привласнення грошей інтернет-аферистами	4 %
пропозиція продажу неіснуючих товарів на платформах оголошень або у соцмережах	38 %
телефонні шахрайства або їх спроба	78 %
відвідування фішингових ресурсів, схожих на популярні Інтернет-магазини, банківські установи або організації	12 %
пропозиція переходу за сумнівними посиланнями	81 %
здійснення ризикованих онлайн-платежів	13 %
образи, спроби приниження	21 %
непристойні пропозиції, відправка інтимних фото	17 %
оформлення без моєї згоди платних інтернет підписок або спроба оформити	31 %

Результати дослідження свідчать, що близька 72% респондентів – осіб молодого віку, що кожен день відвідують мережу Інтернет, зіштовхувались із протиправними діяннями по відношенню до себе, або їх спробами в Інтернеті. Окрім цього опитування дає змогу прийти до висновку, що особи стикалися не з однією, а з декількома кіберзагрозами. Також ми приходимо до висновку про великий рівень латентності протиправних посягань, що вчиняються у кіберпросторі. Цифри офіційної статистики явно не відображають повний спектр таких діянь. У зв'язку із цим, сьогодні особливо відчувається потреба у детальній розробці важливих питань, пов'язаних із віктимологічною характеристикою та запобіганням протиправним посяганням у кіберпросторі.

Також важливим тригером віктимізації молоді, особливо неповнолітніх в мережі Інтернет є прояви кібербулінгу, масштаби якого зростають кожен день, як зростає і рівень комунікації серед підлітків виключно у соціальних мережах та віртуальному просторі. Однак зазначене питання потребує окремого вивчення.

У підсумку слід підкреслити, що цілковите залучення населення до процесів цифровізації суспільства буде сприяти активізації їх віктимної поведінки, що, в свою чергу, вимагає від суб'єктів державної влади, громадських організацій, оперативних заходів віктимологічної профілактики кіберзлочинів, спрямованої, насамперед, на індивідуальне виховання неповнолітніх, підвищення рівня правосвідомості та технічної освіти в сфері кібербезпеки.

Список використаних джерел

1. Майже 23 млн. українців регулярно користуються Інтернетом. URL:https://mind.ua/news/20204323-majzhe-23-mln-ukrayinciv-regulyarno-koristuyutsya-internetom-doslidzhennya (дата звернення 19.10.2021).

2. Литвинов О.М., Орлов Ю.В. Нариси з кримінології постмодерну. Х. 2019. 278 с.

3. Report Serious Organised Crime (SOCTA/OCTA). URL:https://www.europol.europa.eu/activities-services/main-reports/european-union-serious-and-organised-crime-threat-assessment (дата звернення 19.10.2021).

4. На Херсонщині поліцейські оголосили підозру організаторам шахрайського call-центру URL: https://cyberpolice.gov.ua/news/na-xersonshhyni-policzejski-ogolosyly-pidozru-organizatoram-shaxrajskogo-call-czentru-1108/ (дата звернення 19.10.2021).

5. Кіберполіція викрила киянина у привласненні грошей громадян через несанкціоноване втручання в роботу платіжних систем URL:https://cyberpolice.gov.ua/news/kiberpolicziya-vykryla-kyyanyna-u-pryvlasnenni-groshej-gromadyan-cherez-nesankczionovane-vtruchannya-v-robotu-platizhnyx-system-4009/ (дата звернення 19.10.2021).

6. Джужа О.М. Віктимологія на захист прав і законних інтересів жертв злочину. Право України. 2002. №2. С. 134.

7. Джужа О. М. Запобігання злочинам: кримінологовіктимологічна парадигма. Київ. 2015. 331 с.

8. Всестороннее исследование проблемы киберпреступности : проект / С. Малби, Р. Мейс, А. Холтерхоф [и др.]. Вена, 2013. 360 с.

9. Литвинов О.М., Орлов Ю.В. Кримінологія «свого» часу: наукові розвідки. Харків. 2021. 316 с.

Одержано 01.05.2022

УДК 351.745.7
МОВЧАН Анатолій Васильович,
доктор юридичних наук, професор,
професор кафедри оперативно-розшукової діяльності
Львівського державного університету внутрішніх справ
https://orcid.org/0000-0002-6997-6517;
ЖУКОВСЬКИЙ Ігор В'ячеславович,
аспірант кафедри оперативно-розшукової діяльності
Львівського державного університету внутрішніх справ
https://orcid.org/0000-0002-1121-6582

ВИКОРИСТАННЯ ІНФОРМАЦІЙНИХ СИСТЕМ ГЕНЕРАЛЬНОГО СЕКРЕТАРІАТУ ІНТЕРПОЛУ У ПРОТИДІЇ ТОРГІВЛІ ЛЮДЬМИ

Використання інформаційних систем Генерального секретаріату Інтерполу є однією із форм міжнародного поліцейського співробітництва. Банки даних Інтерполу використовуються з метою забезпечення всебічної взаємодії правоохоронних органів держав-членів Інтерполу. Зокрема, з банків даних Інтерполу з використанням інформаційної системи Інтерполу може бути отримано: інформацію про осіб; інформацію про транспортні засоби, які перебувають у розшуку; інформацію про плавзасоби, які перебувають у розшуку; інформацію про викрадені, втрачені, підроблені, недійсні документи, що підтверджують громадянство, посвідчують особу чи її спеціальний статус; інформацію про твори мистецтва / культурні цінності; інформацію про вогнепальну зброю; сліди рук, вилучені з місць вчинення злочину; дактилоскопічну карту; ДНК-профілі; зображення дітей, які зазнали сексуальної експлуатації; інші дані [1].

Крім того, Генеральний секретаріат за допомогою системи I-24/7 надає доступ до банку даних циркулярних повідомлень Інтерполу, у якому міститься інформація про усі зазначені циркулярні повідомлення в електронному вигляді. Департамент міжнародного поліцейського співробітництва Національної поліції на підставі отриманого від правоохоронного органу України запиту чи звернення забезпечує використання інформаційної системи Інтерполу шляхом надсилання запиту про публікацію Генеральним секретаріатом Інтерполу оповіщень.

Повідомлення публікується лише в тому випадку, якщо воно відповідає Статуту Інтерполу та всім умовам для обробки інформації, визначеним Правилами обробки даних, що забезпечує законність і якість інформації та захист персональних даних. Повідомлення не буде опубліковано, якщо воно порушує статтю 3 Статуту Інтерполу, яка забороняє Організації здійснювати будь-яке втручання або діяльність політичного, військового, релігійного чи расового характеру. Правовою підставою для «повідомлення з червоним кутом» є ордер на арешт або ухвала суду, видана судовими органами відповідної країни. Будь-яка особа, на яку поширюється повідомлення Інтерполу, повинна вважатися невинною, доки не буде доведено її вину [2].

Прикладом успішної взаємодії правоохоронних органів за підтримки штаб-квартири Генерального секретаріату Інтерполу у протидії торгівлі людьми є затримання в рамках поліцейської спецоперації Джона Хабету в Найробі 16 грудня 2021 року. Спеціалізований підрозділ Інтерполу з питань незаконного ввезення мігрантів і торгівлі людьми визначив Хабету як високопріоритетну ціль ще у жовтні 2020 року, коли країни-члени попередили Інтерпол про глобальну контрабандну діяльність Хабети, про що негайно повідомили НЦБ Інтерполу Нідерландів. Хабету ймовірно брав участь принаймні в чотирьох різних операціях з контрабандного ввезення груп громадян Еритреї до Європи, використовуючи маршрути з Азії.

Використовуючи захищену глобальну поліцейську комунікаційну мережу I-24/7, Інтерпол координував зусилля країн-учасниць, що спрямовувались на руйнування контрабандної мережі, надаючи можливість країнам обмінюватися кримінальною розвідкою та аналізом щодо Хабети та те, як він організував трансконтинентальні контрабандні операції.

10 грудня 2021 року НЦБ Інтерполу Нідерландів повідомило НЦБ Інтерполу Кенії про присутність втікача в Найробі. Того ж дня було опубліковано червоне повідомлення Інтерполу – міжнародне попередження про втікача – про контрабанду людей та використання підроблених документів для здійснення трансконтинентальних контрабандних операцій, що спричинило спостереження та арешт підозрюваного в столиці Кенії. Це розслідування було підтримано Регіональним оперативним центром на підтримку Хартумського процесу та Ініціативи Африканського союзу (АС) Африканського Рогу (ROCK) та Європолом.

Крім того, у рамках міжнародного поліцейського співробітництва в липні 2021 року, в ході операції Інтерполу Liberterra, було заарештовано 286 підозрюваних членів транснаціональних злочинних груп, які займалися торгівлею людьми та незаконним переміщенням мігрантів. У квітні 2021 року, в ході операції Weka, правоохоронні органи Африки та Європи врятували майже 500 жертв торгівлі людьми та ідентифікували близько 760 нелегальних мігрантів на території 24 країн походження, транзиту та призначення. Обидві операції активізували співробітництво регіональних правоохоронних органів щодо контрабанди людей і викликали пов'язані поліцейські розслідування на всіх континентах щодо таких цілей, як Хабету [3].

Отже, використання інформаційних систем Генерального секретаріату Інтерполу є запорукою проведення успішних операцій правоохоронних органів країн-членів Інтерполу у протидії торгівлі людьми і незаконній міграції.

Список використаних джерел

1. Офіційний вебсайт Інтерполу URL: https://www.interpol.int/ (дата звернення: 15.03.2022).

2. Про затвердження Інструкції про порядок використання правоохоронними органами України інформаційної системи Міжнародної організації кримінальної поліції – Інтерпол: наказ МВС, Офісу Генерального прокурора, НАБУ, СБУ, ДБР, Мінфіна, Мінюста від 17 серпня 2020 р. № 613/380/93/228/414/510/2801/5.

3. People smuggling sting operation: Kenya-Netherlands cooperation lands renowned fugitive in jail. URL: https://www.interpol.int/News-and-Events/News/2021/People-smuggling-sting-operation-Kenya-Netherlands-cooperation-lands-renowned-fugitive-in-jail (дата звернення: 20.03.2022).

Одержано 30.04.2022

УДК 519.7:537.8

МОЖАЄВ Михайло Олександрович,
доктор технічних наук,
доцент кафедри кібербезпеки та DATA-технологій факультету № 6
Харківського національного університету внутрішніх справ
https://orcid.org/0000-0003-1566-9260
ЄВСТРАТ Дмитро Іванович,
кандидат технічних наук, доцент,
доцент кафедри інформаційних систем
факультету інформаційних технологій
Харківського національного економічного університету ім. Семена Кузнеця
https://orcid.org/0000-0001-8393-6063

ОСОБЛИВОСТІ СИНТЕЗУ ІНФОРМАЦІЙНОЇ СИСТЕМИ СУДОВОЇ ЕКСПЕРТИЗИ

На даний момент у сучасному світі функціонує колосальна кількість готових до використання інформаційно-обчислювальних ресурсів, створених у різний час. Для їхньої розробки використовувалися різні підходи. Майже завжди при розробці новішої інформаційної системи можна знайти і застосувати вже готові за своїми функціями, вже готові компоненти. Головним завданням таких інформаційно-обчислювальних ресурсів є насамперед полегшений доступ до віддалених ресурсів та контроль спільного використання цих ресурсів

(комп'ютерів, файлів, даних у базі даних (БД). Саме до таких ресурсів належать різноманітні розподілені інформаційні системи (РІС).

Розподілений характер інформаційних систем судової експертизи та значимість інформації, що обробляється, пред'являють підвищені вимоги як до структури самої системи, так і до якості передачі між різними підсистемами. Подолання цих проблем було присвячено велику кількість досліджень [1–3].

Отже, вдосконалення існуючих систем передачі та проектування нових телекомунікаційних систем є важливим чинником підвищення якості обслуговування всієї ІС судової експертизи.

Метою даної доповіді є аналіз існуючих моделей та типів інформаційних систем судової експертизи.

Для вирішення цього завдання необхідно вирішити наукове завдання: Проаналізувати різні інформаційні системи судової експертизи та завдання, які вони вирішують.

Відомо, що різноманітна за формою та змістом судово-експертна діяльність неможлива без використання найрізноманітніших джерел інформації. Це – документи у різних інформаційних системах, зокрема і БД. При доборі інформації дотримуються принципи достовірності, актуальності, необхідної достатності та повноти. До принципів створення інформаційних систем належать простота, відкритість, інтерактивність, структурність, інтегрованість, захищеність та інше.

Експертні системи – це напрямок досліджень у галузі штучного інтелекту зі створення обчислювальних систем, які вміють приймати рішення, схожі на рішення експертів у заданій предметній області [4]. Функціонування БД у судовій експертизі ґрунтується на принципах оперативної поповнюваності та актуальності, достатньої швидкодії при пошуку та обробці даних, відповідності відповідей пошуковим запитам, а також забезпечення захисту інформації. При дослідженні обстановки місця надзвичайної ситуації (НС), аналізі речових доказів, а також вивченні слідчої чи оперативної ситуації використовуються системний підхід, теорія ігор, масового обслуговування, нечітких множин тощо. Об'єктивність експертизи за такого інформаційного забезпечення реалізується повною мірою.

Використання БД у судовій експертизі передбачає збирання, накопичення, зберігання, переробку та аналіз інформації. При зборі інформації, як правило, застосовується спеціальне обладнання, сканери, цифрові фотоапарати та відеокамери, звукозаписні пристрої. У ряді випадків досі не вдається цифрувати інформацію, що використовується в експертизі. Нині є багато довідково-інформаційних фондів. Переважно вони засновані на БД і є автоматизовані інформаційно-пошукові системи. Судово-експертні установи використовують довідково-інформаційні фонди, побудовані стосовно конкретних родів експертиз, а також з різних об'єктів або методів дослідження. Проте вони реалізовані як автоматизованих інформаційно-пошукових систем з урахуванням БД, і є частиною системи криміналістичної реєстрації. Ця система включає підсистеми, які називаються криміналістичними обліками.

Список використаних джерел

1. Lamport L. Distributin. URL: http://research.microsoft.com/enus/um/people/lamport/pubs/distributed-system.txt (reference date: 06.11.2016).

2. Tanenbaum E., Van-Steen M. Distributed Systems. The principles and paradigms. SPb.: Peter, 2003. 877 p.

3. Radchenko G.I. Distributed Computing. Chelyabinsk: Photographer, 2012. 184 p.

4. Mozhaiev M., Melashchenko O., Roh V. Usatenko M. (2020), Means of improving the quality of service of the computer network of the forensic information system. *Innovate Technologies and Scientific Solutions for Industries*, No. 2 (12), pp. 57-65. DOI: https://doi.org/10.30837/2522-9818.2020.12.057.

Одержано 25.04.2022

УДК 519.7:537.8
МОЖАЄВ Михайло Олександрович,
доктор технічних наук,
доцент кафедри кібербезпеки та DATA-технологій факультету № 6
Харківського національного університету внутрішніх справ
https://orcid.org/ 0000-0003-1566-9260
ПЕРЕСІЧАНСЬКИЙ Валерій Миколайович,
доцент кафедри кібербезпеки та DATA-технологій факультету № 6
Харківського національного університету внутрішніх справ
https://orcid.org/0000-0002-0130-9339

АНАЛІЗ МЕТОДИК СУДОВИХ ЕКСПЕРТИЗ ЦИФРОВИХ ФОТОЗОБРАЖЕНЬ І ВИЗНАЧЕННЯ НАПРЯМІВ ДОСЛІДЖЕННЯ

За прийнятою класифікацією методики проведення судових експертиз дослідження цифрових фотозображень належить до спеціальностей: 6.1 «Дослідження фотозображень та технічних засобів їх виготовлення» та 7.1 «Технічне дослідження матеріалів та засобів відеозвукозапису» [1].

Найбільше близькою до зазначених досліджень зареєстрованою методикою судової експертизи цифрових зображень на сьогодні є Методика досліджень цифрових фотозображень та технічних засобів їх виготовлення [2].

Її метою є визначення автентичності цифрових фотографій.

Методика містить такі загальні етапи:

– підготовче дослідження;
– аналітичне дослідження;
– порівняльне дослідження;
– синтез результатів дослідження;
– формулювання висновків.

Об’єктами дослідження за методикою є:

– цифрові фотозображення – фотознімки в конкретний момент часу;
– окремі кадри цифрових відеозаписів у певний проміжок часу;
– технічні засоби фотографування – цифрові фотокамери;
– технічні засоби відеозапису – цифрові відеокамери (відео реєстратори тощо).

Порівняльними об’єктами дослідження за методикою є:

– цифрові фотозображення, отримані в результаті експертних і слідчих експериментів;
– цифрові фотозображення з чітко визначеними способами та умовами отримання.

У цілому методика відповідає завданням судової експертизи цифрових зображень. Докладно висвітлено загальну схему досліджень, порядок дій експерта при попередньому дослідженні, дії при візуальному аналізі та аналізі метаданих у межах аналітичного дослідження. Однак слід зауважити, що ефективність візуального аналізу цілком залежить від кваліфікації та стану зору експерта й містить значний суб’єктивний фактор. Аналіз метаданих є ефективним лише в разі примітивних підробок, бо EXIF-дані фотографії можуть бути легко відредаговані існуючими EXIF-редакторами.

Проте за методикою, використання різних методів (ELA, PCA, wavelet та ін.) у межах розширеного аналізу зображень означено лише концептуально без конкретних рекомендацій щодо обмежень їх використання та запобігання отримання експертом хибного висновку – визначення ознак фотомонтажу або ретушування за відсутності таких (помилка першого роду), або визначення їх відсутності в редагованому зображенні (помилка другого роду). Це змушує експертів застосовувати означені та інші методи на свій розсуд, з урахуванням свого досвіду, що призводить до протилежних висновків різних експертів за одним і тим самим провадженням.

Так, результати за методом ELA, що рекомендований цією методикою до застосування для виявлення ознак фотопідробок значною мірою залежать від завданих параметрів (настройок).

Також особливістю методу ELA, яку треба прийняти до уваги, є те, що шумова картина створюється шляхом порівняння досліджуваного зображення з його стиснутим jpeg-аналогом. Параметри стискання аналога (параметр jpegQ) і масштабування шуму (nL) (рівень втрат аналога) задаються експертом і потребують детального обґрунтування. Також потребує обґрунтування принципове питання допустимості використання в судовій експертизі самого принципу ELA: порівняння досліджуваного зображення із зображенням спотвореним експертом. Багато аналогічних питань виникає також і при використанні інших методів комп'ютерного дослідження фотопідробок.

Враховуючи наведене, методика досліджень, що розглядається [2], на наш погляд, потребує удосконалення методики комп'ютерного аналізу зображень у рамках аналітичного дослідження (розширеного).

В основу методики [3] дослідження зображень щодо встановлення ознак зміни змісту фотозображень засобами редагування покладено явище пошкодження (спотворення) природного шумового фону зображення, притаманного йому внаслідок наявності шуму чутливих елементів цифрових фотокамер. Спотворення шумового фону виникає в певних випадках (фотомонтаж, ретушування та ін.) у відповідних зонах зображення в разі застосування до нього засобів цифрового редагування.

Список використаних джерел

1. Реєстр методик проведення судових експертиз URL: http://rmpse.minjust.gov.ua/page/38 (дата звернення: 10.02.2022).

2. Розробка методики досліджень цифрових фотозображень та технічних засобів їх виготовлення / Є. В. Тимко та ін. Звіт про НДР : КНДІСЕ, 2013. 121 с.

3. Бобрицкий С. М. Черный С. В. Методические аспекты комплексного исследования с целью выявления признаков монтажа в цифровой фотографии. *Теорія та практика судової експертизи і криміналістики*. 2010. Вип. 10.С. 633–639.

Одержано 19.04.2022

УДК 004.8:004.9:343.98

МОЖАЄВ Олександр Олександрович,
доктор технічних наук, професор,
професор кафедри кібербезпеки та DATA-технологій факультету № 6
Харківського національного університету внутрішніх справ
https://orcid.org/0000-0002-1412-2696;
ЯКИМЕНКО Ігор В'ячеславович,
студент 3 курсу факультету № 6
Харківського національного університету внутрішніх справ

АНАЛІЗ ДОСЛІДЖЕННЯ ФАКТІВ ЗНИЩЕННЯ ІНФОРМАЦІЇ НА ЦИФРОВИХ НОСІЯХ

Одним із основних завдань, що вирішуються в межах комп'ютерно-технічної експертизи, є встановлення фактів знищення інформації. Органи досудового розслідування все частіше ставлять на вирішення питання «Чи піддавався досліджуваний накопичувач певним процедурам з метою знищення інформації?». Не зважаючи на наявність зазначеного питання у Науково-методичних рекомендаціях з питань підготовки та призначення судових експертиз та експертних досліджень, затвердженої наказом Міністерства юстиції України від 8 жовтня 1998 року № 53/5 (зі змінами та доповненнями) для його вирішення повністю відсутня мето-

дична база і питання вирішується виключно на основі спеціальних знань кожного експерта, що стикається з даною проблемою [1-4].

У більшості обчислювальних систем (ОС) в якості основного енергонезалежного носія інформації використовується накопичувач на жорсткому магнітному диску (НЖМД). У цій доповіді розглядається визначення фактів знищення інформації у цифрових носіях для уніфікації підходів визначення ознак знищення інформації та їх інтерпретації.

Варто один раз записати інформацію на жорсткому диску і видалити її з магнітної пам'яті диска буде дуже складно. Тому, здавалося б, нешкідливий акт списання старого комп'ютера або передача його в іншу організацію - найбільш простий шлях несанкціонованого отримання інформації з обмеженим доступом.

Крім тієї конфіденційної інформації, про яку знають користувачі (бухгалтерської, фінансової, особистої, перспективних розробках), на ПК може зберігатися безліч інших конфіденційних даних, які не завжди відомі оператору. Додатки та операційні системи зберігають паролі, ключі шифрування і інші дані з обмеженим доступом в різних місцях, включаючи файли конфігурації і тимчасові файли. Операційні системи довільним чином записують вміст оперативної пам'яті в файл підкачки на диску, що не дає можливості дізнатися, що з цих даних дійсно збережено на носії.

Тому дослідження фактів знищення інформації на цифрових носіях є безумовно **актуальною науковою задачею**, вирішення якої є **метою** доповіді.

В доповіді наведено аналіз методів відновлення інформації, вилученої з жорстких магнітних дисків. Для цього було проаналізовано основні фізичні основи магнітного запису сигналів та технічні методи їх реалізації. Було проведено аналіз принципів роботи накопичувачів на жорстких магнітних дисках та особливості їх застосування.

У подальшому в роботі було проведено аналіз існуючих методів знищення інформації з магнітних носіїв інформації серед яких можливо виділити:

• програмні методи - засновані на використанні стандартних команд управління НЖМД;

• апаратні методи - реалізуються за допомогою спеціального обладнання, що впливає на магнітні диски НЖМД.

За способом впливу апаратні методи класифікуються на кілька підгруп:

• методи, перебудовують доменну структуру магнітного носія без руйнування його конструкції;

• методи, пов'язані з руйнуванням конструкції носія.

Таким чином, були розглянуті існуючи методи знищення інформації з магнітних носіїв інформації.

У подальшому в роботі було створено програмне забезпечення для накопичення статистичних даних з накопичувачів, що дозволило забезпечити більш надійні результати експертних криміналістичних досліджень та покращити якість висновків комп'ютерно-технічної експертизи.

Список використаних джерел

1. Методологія наукових досліджень / М. Л. Черчик. Луцьк, 2013. URL: http://elib.lutsk-ntu.com.ua/book/fb/pesp/2012/12-31 (дата звернення: 10.01.2022).

2. Методика дослідження інформації на цифрових носіях / С. М. Бобрицький, О. В. Чишкала, О. В. Селезньова та ін. Х. : ХНДІСЕ, 2011. 44 с.

3. Клименко Н.І. Судова експертологія: Курс лекцій: Навч. посіб. для студ. юрид. спец. вищ. навч. закл. К.: Видавничий Дім «ІнЮре», 2007. 528 с.

4. Моїсєєв О.М., Перепічка О.І. Самоконтроль в експертному дослідженні // Криминалистика и судебная экспертиза: Междуведомственный научно-методический сборник. Вып. 58, ч. 1. К: Министерство юстиции Украины, 2013. С. 131-137.

Одержано 19.04.2022

РОЗДІЛ 3.
ВИКОРИСТАННЯ ІНФОРМАЦІЙНИХ ТЕХНОЛОГІЙ І ТЕХНІЧНИХ ЗАСОБІВ У ПРОТИДІЇ КІБЕРЗЛОЧИННОСТІ ТА ТОРГІВЛІ ЛЮДЬМИ

УДК 004.04:004.67:004.77
БРУСАКОВА Оксана Валеріївна,
доктор юридичних наук, доцент,
декан факультету № 6
Харківського національного університету внутрішніх справ
https://orcid.org/ 0000-0001-8616-0424;
МОЖАЄВ Олександр Олександрович,
доктор технічних наук, професор,
професор кафедри кібербезпеки та DATA-технологій факультету № 6
Харківського національного університету внутрішніх справ
https://orcid.org/0000-0002-1412-2696

КЛАСИФІКАЦІЯ КІБЕРЗАГРОЗ ТА СЦЕНАРІЇВ КІБЕРАТАК НА СИСТЕМИ БПЛА

В даний час використання БПЛА має важливе значення, що й підтвердили останні події в Україні. Це у свою чергу змушує до активного протиборства сторін, які широко використовують ці системи. Одним із видів цього протиборства є створення кіберзагроз для систем БПЛА.

Основні види кіберзагроз найчастіше спрямовані на ураження центру управління польотом БПЛА, дестабілізацію радіоканалу БПЛА або виведення з ладу безпосередньо БПЛА.

Загрози, спрямовані на ураження центру управління польотом БПЛА або Sensor Spoofing, спрямовані на бортові контролери, які залежать від зовнішнього середовища. Прикладами таких контролерів є GPS-приймачі, датчики зору, радари, гідролокатори, лідари та інфрачервоні датчики. Зловмисник може відправити помилкові дані по каналах GPS або вивести з ладу будь-який датчик польоту.

Загрози, спрямовані на дестабілізацію радіоканалу БПЛА або Wireless Attack проходять з використанням зловмисником бездротових каналів зв'язку для зміни даних на борту автопілота БПЛА. Найгіршим сценарієм для цієї атаки є ситуація, коли зловмисник зможе зламати шифрування каналу зв'язку. Як тільки це станеться, зловмиснику стає відомим протокол зв'язку, і він може отримати повний контроль над БПЛА. Іншою можливістю є атака переповнення буфера, що ушкоджує деякі дані на борту або ініціює якусь подію. Слід зазначити, що атаки, спрямовані на дестабілізацію радіоканалу БПЛА є найнебезпечнішими, оскільки зловмисник може проводити свої деструктивні дії здалеку під час виконання БПЛА польотного завдання.

Загрози безпосереднього виведення БПЛА з ладу або Hardware Attack можуть відбуватися щоразу, коли зловмисник має прямий доступ до будь-якого компонента автопілота БПЛА.

Потім зловмисник може пошкодити дані, що зберігаються на борту автопілота або встановити додаткові компоненти, які можуть пошкодити потік даних. Ці типи атак можуть бути здійснені під час обслуговування та зберігання БПЛА або при виготовленні та доставці. Зловмисник може підключитися безпосередньо до автопілота БПЛА і пошкодити його або перепрограмувати, якщо має засоби, або замінити або додати компоненти, які дадуть йому контроль над БПЛА та/або зібраними тактичними даними. Апаратні атаки можуть вплинути на живучість БПЛА, поставити під загрозу управління БПЛА та компрометувати тактичні дані, зібрані БПЛА.

Наведені різновиди кіберзагроз можуть бути використані дослідниками у процесі моделювання та розробки сценаріїв кібератак, що демонструють уразливості систем управління та функціонування БПЛА.

Одержано 25.04.2022

УДК 004.056.53
ВОРОПАЄВА Анна Олександрівна,
кандидат технічних наук, доцент,
доцент кафедри протидії кіберзлочинності факультету № 4
Харківського національного університету внутрішніх справ
https://orcid.org/0000-0002-7382-5471;
ГРИЩЕНКО Денис Олександрович,
старшій викладач кафедри протидії кіберзлочинності факультету № 4
Харківського національного університету внутрішніх справ
https://orcid.org/0000-0001-5066-7389

ДОСЛІДЖЕННЯ ІНФОРМАЦІЙНИХ РЕСУРСІВ ТЕРИТОРІАЛЬНИХ ГРОМАД ДОНЕЦЬКОЇ ОБЛАСТІ

Важливим інструментом комунікації уряду з населенням є веб портали обласних та районних адміністрацій, територіальних громад, міських та сільських рад. Варто відмітити, що наявність сайту державної установи є обов'язковою вимогою. Сьогодні на функціонування веб-порталу покладаються представницькі, інформаційні та контрольні функції діяльності відповідних установ.

Під час дослідження стану інформатизації Донецької області були оцінені сайти 13 об'єднаних територіальних громад [1]. Якість сайтів є інтегральною характеристикою яка включає широкий спектр властивостей продукту і визначає міру задоволення потреб користувача. На якість сайту впливає велика кількість показників. Умовно їх є три основні категорії , які характеризують дизайн або візуальне наповнення, функціональність або технічне наповнення та контент або інформаційне наповнення [2]. Оцінка проводилась з дотриманням принципів неупередженості, доцільності, повномасштабності з використанням комплексного підходу. У 2018 році Програма розвитку ООН в Україні провела експертне дослідження «Оцінка впровадження та використання інструментів електронного урядування Донецькою обласною державною адміністрацією та органами місцевого самоврядування Донецької області». Одним із вимірів оцінки було обрано інформаційну наповненість офіційних вебсайтів органів місцевого самоврядування [3]. За базис для поточного дослідження вирішено було прийняти методологію та критерії з вказаного вище джерела та оцінювались наступні напрями: загальна інформація, рекомендована до представлення на сайті, актуальність та динамічність стрічки новин (критерії оцінювання: історія громади; символіка громади; стратегія розвитку; депутатський склад; інформація про комунальні підприємства (для міських громад), посилання на ресурси); рекомендовані до розміщення документи (перевірялась можливість повнотекстового перегляду та, у разі необхідності, завантаження за наступними критеріями: звіти голови громади; протоколи засідань; рішення рад та виконкомів; плани закупівель); зручність та доступність веб-контенту (включаючи інклюзивні верстви населення за критеріями: структурованість; зорова інклюзивність; можливість перекладу сайту на інші мови);рівень доступу до публічної інформації (повнота представлення інформації згідно норм; форма запиту на доступ до публічної інформації; алгоритм подачі заяви на доступ; аналітика обробки запитів). Результати оцінки веб ресурсів ОТГ Донецької обл. зведено до таблиці 1.

Таблиця 1

Назва ОТГ	Загальна інформація							Документи				Зручність та доступність			Публічна інформація			
	1	2	3	4	5	6	7	1	2	3	4	1	2	3	1	2	3	4
Андріївська сільська ОТГ	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+
Бахмутська міська ОТГ	+	+	+	+	+	+	+	+	+	+	+	+	+	-	+	+	+	+
Вугледарська міська ОТГ	+	+	+	+	+	+	-	+	+	+	+	+	+	+	-	+	-	+
Званівська сільська ОТГ	+	+	+	+	+	+	+	+	+		+	+	+	+	+	-	+	+
Іллінівська сільська ОТГа	-	+	+	+	+	+	+	+	+	+	+	+	+	+	+	-	-	-
Криворізька сільська ОТГ	+	+	-	+	+	+	+	+	+	+	-	+	+	+	+	-	-	-
Лиманська міська ОТГ	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	-
Миколаївська міська ОТГ	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	-	+
Олександрівська селищна ОТГ	+	+	+	+	+	+	+	-	+	+	+	+	+	+	+	+	-	-
Сіверська міська ОТГ	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+
Соледарська міська ОТГ	+	+	+	+	+	+	+	+	+	+	+	+	-	+	+	+	+	+
Черкаська селищна ОТГ	-	-	-	+	+	+	+	+	+	+	+	+	+	+	+	-	-	-
Шахівська сільська ОТГ	-	-	+	+	+	+	+	+	+	+	+	+	+	+	+	-	-	-

Шкала експертизи складається з трьох рівнів, позначених кольорами: зелений (є переконливі свідчення високого рівня критерію), жовтий (свідчення високого рівня критерію не є очевидними), червоний (є переконливі свідчення щодо проблем із обраним критерієм (наприклад, його відсутність). Варто відмітити, що на сайтах перевірялася лише наявність доступу до інформації та послуг, а не їх якість.

За результатами проведеної оцінки сайтів територіальних громад можна зробити наступні висновки: сайти мають базову необхідну інформативну наповнюваність відповідно до перелічених напрямів дослідження: загальна інформація, новини громади, документи, зручність та доступність контенту, доступ до публічної інформації. Існуючі недоліки, виявлені під час аналізу, мають несистематичний характер та можуть бути пояснені відсутністю кваліфікованих технічних спеціалістів, які б мали постійно працювати над контентом сайтів для ефективної комунікації із мешканцями громад.

Список використаних джерел

1. Воропаєва А.О. Актуальність та передумови дослідження стану та перспектив інформатизаії громад Донецької області / Наукові досягнення та відкриття сучасної молоді: матеріали міжнародної науково-практичної конференції, 28 квітня 2021 року. Покровськ: ДВНЗ «ДонНТУ»,2021. 216 с.

2. Метод оцінювання якості сайтів / В. П. Ткаченко та ін. // Полиграфические, мультимедийные и WEB-технологии (PMW-2016) : тез. докл. 1-й Междунар. науч.-техн. конф., 16–20 мая 2016 г. Харьков : ХНУРЭ, 2016. Т. 1. С. 96–98.

3. Оцінка впровадження та використання інструментів електронного урядування Донецькою обласною державною адміністрацією та органами місцевого самоврядування Донецької області: UNDP Україна. URL: https://www.ua.undp.org/content/ukraine/uk/home/library/democratic_governance/egov-donetsk.html. (дата звернення: 17.04.2022).

Одержано 18.04.2022

УДК 004.056
ГЕЛЬДТ Станіслав Володимирович,
курсант 2 курсу факультету № 4
Харківського національного університету внутрішніх справ;
ОНИЩЕНКО Юрій Миколайович,
кандидат наук з державного управління, доцент,
доцент кафедри кібербезпеки та DATA-технологій факультету № 6
Харківського національного університету внутрішніх справ
https://orcid.org/0000-0002-7755-3071;

АНАЛІЗ ЛОГ-ФАЙЛІВ ДЛЯ ПРОТИДІЇ КІБЕРАТАКАМ

Згідно з даними Державної служби спеціального зв'язку та захисту інформації, за період війни вже сталося майже втричі більше різного роду хакерських атак, ніж за аналогічний період минулого року [1]. Це вплинуло на роботу таких сайтів та порталів, як: Приват24, Ощадбанк, Дія, Міністерство оборони України, ЗСУ [2]. Мета скоординованих нападів – порушення роботи державних та військових органів, підрив довіри населення до державних інституцій. Таким чином, влада понесла колосальні збитки у вигляді злитих конфіденціальних даних багатьох українців.

Головною задачею цифрової країни є безпека приватної інформації, тому найбільш важливо вміти якомога швидше реагувати на кіберінциденти. Одним із найкращих методів виявлення слідів втручання у систему є перевірка та аналіз певних файлів.

Лог-файл – це створений комп'ютером файл даних, який містить інформацію про моделі використання, дії та операції в програмі, сервері чи іншому пристрої [3]. Проаналізувавши сучасні операційні системи, можна прийти до висновку, що операційна система Linux ефективно налаштована на створення та зберігання файлів журналів. Linux створює безперервну часову шкалу подій, які відбуваються в системі, включаючи кожну подію, пов'язану з сервером, ядром і запущеними програмами. Linux поділяє події на чотири різні категорії:

- журнали додатків;
- журнали подій;
- журнали обслуговування;
- системні журнали.

Щоб зрозуміти важливість інформації та способи її обробки, пропонується розібрати один з лог-файлів сервера Apache. Apache – відкритий вебсервер Інтернет для UNIX-подібних, Microsoft Windows, Novell NetWare та інших операційних систем [4]. Файл знаходиться за абсолютним шляхом – /var/log/apache2/access.log. Завжди має певну структуру, а саме:

– IP-адреса хоста, який запросив сторінку;
– дата, час та GMT;
– сторінка, яку запросив хост;
– версія протоколу;
– код стану;
– розмір файлу в байтах;
– сторінка, з якої посилається хост;
– агент користувача, ідентифікований браузером [5].

Завдяки структурі, файл можна аналізувати за допомогою утиліти cut. Наприклад, команда нижче виведе лише IP-адреси з лог-файлу:

cut –d' ' –f 1 /var/log/apache2/access.log

Параметр –d вказується для визначення роздільника тексту, -f для номера стовпця.

Для виводу інформації щодо вебсторінок, які відвідувала певна IP-адреса, використовується утиліта awk:

awk '$1 == "192.168.0.3" {print $0}' /var/log/apache2/access.log | cut –d' ' –f 7

Awk – це мова програмування, призначена для сканування та обробки зразків [6]. В команді вище '192.168.0.3' – тестова IP-адреса, яку ми маємо проаналізувати.

Якщо хост зайшов на кожну сторінку лише по 1 разу, це може вказувати на вебсканер або клонування сайту. Website Crawler – програма, що є складовою частиною пошукової системи та призначена для обходу сторінок інтернету з метою занесення інформації про них до бази даних.

awk '$9 == "404" {print $0}' /var/log/apache2/access.log | cut –d' ' –f 1

За допомогою цієї команди можна проаналізувати IP-адреси, яким повернувся статус 404 (Not Found). Якщо хост виводиться забагато разів, є сенс перевірити які саме сторінки він відвідував. Web Directory Enumeration – атака методом застосування грубої сили на приховані файли та каталоги шляхом послідовного відвідування сторінок, визначених у списку спеціального словника [7].

awk '$1 == "192.168.0.3" {print $0}' /var/log/apache2/access.log | cut –d' ' –f 12

Команда, наведена вище, аналізує агента користувача, ідентифікованого браузером. Таким чином, можна побачити нестандартні браузери та боти, які не являються прямим користувачами.

tail –f /var/log/apache2/access.log | egrep –line-buffered 'HTTP/. 404' | cut –d' ' –f4-7*

Утиліта tail з параметром –f аналізує лог-файл в режимі реального часу. Утиліта egrep знаходить збіг з рядком *'HTTP/.* 404'* та виводить в термінал дату, час, тип запиту та сторінку.

Файли журналу та Системні журнали є невід'ємною частиною захисту системи на основі перегляду та аналізу. Лише однією командою, адміністратор може контролювати кожен запит користувача та швидко реагувати на певні аномалії. Завдяки автоматизації процесів за допомогою утиліти mail, нестандартні строки можуть бути відправлені на електрону пошту та проаналізовані в короткий період часу.

Список використаних джерел

1. За час війни кількість хакерських атак в Україні зросла втричі // Економічна правда : вебсайт. URL: https://www.epravda.com.ua/news/2022/04/3/685157/ (дата звернення: 21.04.2022).

2. Масована DDoS-атака на ПриватБанк та Ощадбанк. Сайт Міноборони не відкривається // Ліга.Tech : вебсайт. URL: https://tech.liga.net/ua/ukraine/article/massirovannaya-ddos-ataka-na-privatbank-i-oschadbank-sayt-minoborony-ne-otkryvaetsya (дата звернення: 21.04.2022).

3. DevOps and Security Glossary Terms // Log File : вебсайт. URL: https://www.sumologic.com/glossary/log-file/ (дата звернення: 21.04.2022).

4. Apache HTTP Server // Wikipedia : вебсайт. URL: https://uk.wikipedia.org/wiki/Apache_HTTP_Server (дата звернення: 21.04.2022).

5. Bash-скрипты // Хабр : вебсайт. URL: https://habr.com/ru/company/ruvds/blog/325522/ (дата звернення: 21.04.2022).

6. AWK // Wikipedia : вебсайт. URL: https://uk.wikipedia.org/wiki/AWK (дата звернення: 21.04.2022).

7. Web Directory Enumeration // Gitbooks : вебсайт. URL: https://www.epravda.com.ua/news/2022/04/3/685157/ (дата звернення: 21.04.2022).

Одержано 01.05.2022

УДК 343.1:65.012.8+004
КАЛАНЧА Андрій Андрійович,
курсант 1 курсу факультету № 4
Харківського національного університету внутрішніх справ;
КЛІМУШИН Петро Сергійович,
кандидат технічних наук, доцент,
доцент кафедри інформаційних технологій і кібербезпеки факультету № 4
Харківського національного університету внутрішніх справ
https://orcid.org/0000-0002-1020-9399

АНАЛІЗ МЕРЕЖЕВОГО ТРАФІКУ ЯК СПОСІБ ПРОТИДІЇ КІБЕРЗЛОЧИННОСТІ

На сьогодні спостерігається стрімкий зріст об'єму мережевого трафіку, що провокує ускладнення його структури. Аналіз мережевого трафіку набуває все більшу актуальність у зв'язку з розвитком мережевих технологій, впровадженням великої кількості нових мережевих протоколів, збільшенням обсягу мережевих даних. Практичне застосування моніторингу мережі забезпечує: виявлення проблем в роботі мережі; запобігання мережевих атак; визначення класифікації трафіку. Моніторинг трафіку також необхідний, щоб більш ефективно діагностувати, оптимізувати пропускну здатність каналів передачі даних, контролювати якість зв'язку та вирішувати проблеми в сфері протидії кіберзлочинності.

Метою роботи є визначення інструментів аналізу мережевого трафіку та порівняльна оцінка їх можливостей в протидії кіберзлочинності.

У кіберполіції для розслідування злочинів необхідні знання з форензики (комп'ютерна криміналістика, розслідування кіберзлочинів), аналізаторів мережевого траіфіку (сніферів), методів атак та криптографії. Моніторинг мережі складне завдання, що вимагає великих сил та витрат, яке є невід'ємною складовою повсякденного життя мережевих адміністраторів-провайдерів мережі. Проте левову частку від успішності цих розслідувань грає саме провайдер, оскільки у нього міститься вся інформація про дії злочинця у мережі. Провайдери мають доступ до такої інформації: усі відвідані сайти з протоколом http/https; завантажені дані; трафік і дані з месенджерів. Ключовим моментом є, на теперішній час, відсутність безпосередньої комунікації між провайдерами та кіберполіцією. Тож досить часто доводиться власноруч перехоплювати трафік та слідкувати за мережевою активністю підозрюваного.

Сьогодні на ринку є інструменти моніторингу як платні так і безкоштовні. І хоча кожен інструмент побудований на основних принципах збору мережевого трафіку, вони значно відрізняються за своєю шириною та глибиною.

TCPDump це інструмент дослідження пакетів з відкритим кодом, сумісний на платформах Unix та Linux, більш легкий і портативний інструмент для сніфу пакетів і тому мережеві адміністратори використовують його для доступу до мережевих пристроїв з віддаленого місця. Обмеженнями TCPDump є: відсутність візуального захоплення даних; застосовування для аналізу протоколів лише на основі TCP; пакети, заблоковані брандмауером, не відображаються.

Colasoft це інструмент аналізатора протоколів із закритим кодом, що використовується для усунення несправностей, порушень та моніторингу трафіку в мережі. Він забезпечує: простоту використання; глибокий аналіз пакетів у режимі реального часу та надійний поглиблений, криміналістичний аналіз протоколів; має особливість відкриття декількох графічних інтерфейсів та можливість генерування різноманітних звітів. Є деякі обмеження Colasoft: це дорогий додаток, що працює лише на платформі операційної системи Microsoft Windows [1].

Wireshark є проектом програмного забезпечення з відкритим вихідним кодом і випущено під загальною суспільною ліцензією GNU (GPL), доступній для UNIX і Windows і надає наступні функції: знімає пакетні дані в реальному часі з мережевого інтерфейсу; відкриває файли, що містять пакетні дані; імпортує пакети з текстових файлів; відображає пакети з дуже детальною інформацією про протокол; зберігає зібрані пакетні дані; експортує пакети; фільтрує пакети та виконує пошук пакетів за багатьма критеріями; створює різноманітні ста-

тистичні дані. Обмеження Wireshark: потребує найкращого розуміння форматів протоколів; знання мови у форматі байтів; не є автоматизованим інструментом та не підтримує моніторинг в тривалому часі [2].

Для порівняння наданих інструментів мережевого аналізу слідує використовувати таки параметри, як тип вихідного коду, кількість підтримуваних протоколів, підтримувана операційна система, вартість, форми декодування тощо.

Colasoft має функції аналізу більш візуального пояснення зі статистикою захоплених пакетів, відображенням більшої кількості інформації про протоколи та користувацькі програми з графіками та матричним поданням для всіх підключених кінцевих точок. Colasoft, у порівнянні з Wireshark, забезпечує більшу мережеву безпеку. Проте, він охоплює лише 300 протоколів, що дуже менше порівняно з Wireshark, який підтримує 1100 протоколів. TCPDump - це дуже портативний і економічний пакет.

Таким чином, аналіз інструментів моніторингу мережевого трафіку показав, що Wireshark, Colasoft є досить ефективними інструментами в протидії кіберзлочинності, а завдяки своїй доступності Wireshark надає для кіберполіції широкі можливості аналізу множини протоколів, що прискорить розслідування протиправних діянь в кіберпросторі.

Список використаних джерел

1. Горбовський А. І., Войтович О. П. Дослідження безпеки у інтернеті речей // Матеріали XLVI науково-технічної конференції підрозділів ВНТУ, Вінниця, 22-24 березня 2017 р. URL: http://ir.lib.vntu.edu.ua/bitstream/handle/123456789/17277/2805.pdf?sequence=3 (дата звернення: 23.04.2021).

2. Smarter Security For Your Everything, Atmel Has You Covered // Microchip : вебсайт. 2019. URL: https://www.microchip.com/design-centers/security-ics (дата звернення: 23.04.2021).

3. Асангханва Ю., Ий Р., Сыров А. Повышение уровня безопасности граничных узлов интернета вещей с помощью микросхем ATECC608A компании microchip. *Электроника НТБ*. 2019. № 7 (00188). С. 60-64.

Одержано 18.04.2022

УДК 343.1:65.012.8+004

КАЛАНЧА Андрій Андрійович,
курсант 1 курсу факультету № 4
Харківського національного університету внутрішніх справ;
СВІТЛИЧНИЙ Віталій Анатолійович,
кандидат технічних наук, доцент,
доцент кафедри протидії кіберзлочинності факультету № 4
Харківського національного університету внутрішніх справ
https://orcid.org/0000-0003-3381-3350

АНАЛІЗ МЕРЕЖЕВОГО ТРАФІКУ ЯК СПОСІБ ПРОТИДІЇ ЗЛОЧИННОСТІ

Дедалі більше люди використовують Інтернет та техніку в повсякденному житті: розумні холодильники аналізують термін придатності продуктів, нагадують, що потрібно придбати в магазині; розумні чайники самі вмикаються за вашої присутності поряд, а жалюзі зачиняються в темну пору доби. У кожного «розумного» пристрою є доступ до Всесвітньої мережі, а кожен такий девайс має власну IP-/MAC-адресу, що дозволяє власнику керувати ними дистанційно. Проте постає запитання, чи залишається ця інформація лише на цьому пристрої, та чи не протікає вона у чиїсь злі руки?

Великі корпорації типу Google чи Amazon вже вирішили за Вас, що б Ви хотіли придбати, яке місце Ви б хотіли відвідати для прогулянки чи затишної вечері зі своєю другою половинкою [1].

Боротьба за анонімність та приватність також не вічна, оскільки «Корпорації Зла» вигадують дедалі жорстокіші способи вашої деанонімізації. Як приклад – двохфакторна авторизація Google-аккаунтів, яка наполягає на використанні вашого мобільного телефону в якості підтвердження власника, чи реєстрація gmail-пошти, яка вимагає у користувача реєстрацію з номером телефону (яку не можна пропустити). Лякає те, що відмовитися від цих сервісів, які намагаються викрасти вашу інформацію стає складніше, тож уникати їх, чи лягти під каток доксингу – вибір особисто кожного.

У провайдера міститься вся інформація про ваші запити в пошуковій стрічці браузера, усі завантажені та передані файли та документи, а також кому ви і коли писали, а у великих українських компаніях спеціалісти з кібербезпеки постійно грають з балансом принципів конфіденційності, цілісності та доступності, щоб дані не потрапили у відкритий доступ.

Якщо упустити незаконну діяльність «Корпорацій зла» (шпигунство, продаж даних користувачів), то основну загрозу в мережі Інтернет становлять grey-/black-hat хакери, вішинг-/смішинг-/фішинг-шахраї та script-kiddy (хакери, що не мають, власне, досвіду в створенні власних скриптів, а лише використовують такі, що створені досвідченими хакерами).

Щоб детальніше розібратися з проблемою, звернемося до законодавства України. Кіберзлочин - суспільно небезпечне винне діяння у кіберпросторі та/або з його використанням, відповідальність за яке передбачена законом України про кримінальну відповідальність та/або яке визнано злочином міжнародними договорами України, де кіберпростір - середовище, яке надає можливості для здійснення комунікацій та/або реалізації суспільних відносин, утворене в результаті функціонування сумісних комунікаційних систем та забезпечення електронних комунікацій з використанням мережі Інтернет та/або інших глобальних мереж передачі даних. Особи, винні у порушенні законодавства у сферах національної безпеки, електронних комунікацій та захисту інформації, якщо кіберпростір є місцем та/або способом здійснення кримінального правопорушення, іншого винного діяння, відповідальність за яке передбачена цивільним, адміністративним, кримінальним законодавством, несуть відповідальність згідно із законом [2].

У кіберполіції для розслідування злочинів необхідні знання з форензики, мережевих концепцій, методів атак та криптографії. Проте левову частку від успішності цих розслідувань грає саме провайдер, оскільки у нього міститься вся інформація про дії злочинця у Всесвітній мережі.

Провайдери мають доступ до такої інформації:

1) усі відвідані сайти з протоколом http/https;

2) завантажені дані;

3) трафік і дані з месенджерів (за умови, що в них не використовується шифрування);

Ключовим моментом є, на теперішній час, відсутність безпосередньої комунікації між провайдерами та кіберполіцією. Тож досить часто доводиться власноруч перехоплювати трафік та слідкувати за мережевою активністю підозрюваного.

Наразі доступним інструментом для здійснення аналізу трафіку є рішення від Джеральда Комбса –Wireshark [3].

Wireshark у реальному часі перехоплює мережеві пакети та зберігає їх. Ці дані потім використовують з метою вивчення трафіку, відновлення інформації, аналізу роботи мережі, виявлення атак. Це альтернатива та доповнення до стандартної утиліти tcpdump, з графічним інтерфейсом, фільтрами та ширшими можливостями.

Він здатен розшифровувати SSL/TLS трафік, показувати вміст пакетів, пошук пакетів по вмісту, трафік з телефенів, телевізорів та інших побутових пристроїв, інспектувати потоки TCP і UDP [4].

Висновки. Отже, у час залежності пристроїв від Інтернету, на мою думку, аналіз мережевого трафіку за допомогою програмного забезпечення Wireshark є досить ефективним методом попередження та протидії кіберзлочинності, а завдяки своїй доступності та наявності зручного графічного інтерфейсу значно спрощує власну експлуатацію. Та є надія, що в майбутньому кіберполіції нададуть доступ до безпосереднього трафіку від провайдера, що прискорить розслідування протиправних діянь в рази.

Список використаних джерел

1. Як Google шпигує за користувачами. КДБ і не снилось // Економічна правда : вебсайт. URL: https://www.epravda.com.ua/rus/publications/2019/07/2/649257/ (дата звернення: 17.04.2022).

2. Про основні засади забезпечення кібербезпеки України: закон України від 15.12.2021 № 2163-VIII, // База даних «Законодавство України» / Верховна Рада України. URL: https://zakon.rada.gov.ua/laws/show/2163-19#Text (дата звернення: 17.04.2022).

3. Офіційний сайт програмного забезпечення Wireshark // вебсайт. URL: https://www.wireshark.org/ (дата звернення: 17.04.2022).

4. Wireshark для всіх // вебсайт. URL: https://habr.com/ru/company/vdsina/blog/562110/ (дата звернення: 17.04.2022).

Одержано 17.04.2022

УДК 343.1:65.012.8+004

КЛІМУШИН Петро Сергійович,
кандидат технічних наук, доцент,
доцент кафедри інформаційних технологій і кібербезпеки факультету № 4
Харківського національного університету внутрішніх справ
https://orcid.org/0000-0002-1020-9399;
СПАСІБОВ Дмитро Вікторович,
кандидат технічних наук,
начальник відділу технічного захисту інформації
Департаменту технічного супроводження Харківської міської ради

СИМЕТРИЧНА АВТЕНТИФІКАЦІЯ: ПОТЕНЦІЙНЕ ЗАСТОСУВАННЯ АПАРАТНО ЗАХИЩЕНИХ МІКРОСХЕМ ДЛЯ ЗАБЕЗПЕЧЕННЯ БЕЗПЕКИ ІНТЕРНЕТУ РЕЧЕЙ

Інтернет речей (Internet of Things – IoT) – це мережа, що складається із взаємозв'язаних фізичних об'єктів (пристроїв), які мають вбудовані мікроконтролери, датчики, а також програмне забезпечення, що дозволяє здійснювати передачу і обмін даними між ними за протоколами зв'язку.

Метою роботи є дослідження способів застосування криптографічних мікросхем для забезпечення безпечної автентентифікації вузлів інтернет речей з використанням процедур симетричної криптографії.

Автентифікація може бути виконана двома основними способами - симетричним і асиметричним. Основна відмінність між ними полягає в тому, яким чином використовуються таємні ключі. Якщо і на стороні хоста, і на стороні клієнта застосовується один і той же ключ, то автентифікація – симетрична. Якщо ж використовується математично пов'язана пара відкритого і таємного ключів, то автентифікація асиметрична.

До основних переваг апаратних засобів реалізації стандарту симетричного блочного шифрування (Advanced Encryption Standard – AES) для захисту IoT відносять [1]:

1) наявність апаратного вбудованого генератора випадкових чисел, який забезпечує генерацію більш надійних криптографічних ключів;

2) зберігання криптографічних ключів та виконання криптографічних процедур над даними здійснюються в захищеної криптографічної мікросхемі;

3) виконання функції спеціалізованого мікропроцесора для виконання криптографічних перетворень, що розвантажує центральний процесор комп'ютера;

4) гарантування цілісності реалізації алгоритмів криптографічних перетворень;

5) підвищення швидкості шифрування/дешифрування даних.

Використання криптографічних акселераторів підвищує швидкодію шифрування за алгоритмом AES порівняно з його програмною реалізацією у 8/16-бітових мікроконтролерах в 10-20 разів, а у 32-бітових мікроконтролерах – до 150 разів. При цьому швидкодія хеш-алгоритмів SHA-256 з апаратною реалізацією у 32-бітових мікроконтролерах зростає в 100 разів, а для хеш-алгоритмів HMAC – до 500 разів [2].

В роботі проаналізовано потенційні застосування криптографічних мікросхем сімейства CryptoAuthentication в безпеки інтернет речей з використанням процедур симетричної криптографії [4]. Аналіз основних симетричних схем автентифікації показав, що: 1) схема автентифікації зі зберіганням таємного ключа на стороні хоста забезпечує швидкий процес симетричної автентифікації, але вимагає захищеного зберігання таємного ключа на стороні хоста; 2) схема автентифікації без зберігання таємного ключа на стороні хоста, тобто без криптографічної мікросхеми на стороні хоста, забезпечує швидкий процес симетричної автентіфикації, але має відносно невисоку криптостійкість, так як взаємодія в системі виконується без випадкової складової в криптографічних перетвореннях; 3) для підвищення криптостійкості схеми п. 2 доцільне введення в систему взаємодії випадкової складової в криптографічних перетвореннях та використання додаткових процедур хешування з проміжним ключем.

Завантаження оригіналу мікропрограмного забезпечення в системі реалізується за допомогою таємних ключів шифрування та автентифікації, які зберігаються постійно в захищеної енергонезалежної пам’яті криптографічних мікросхем на стороні клієнта і хоста. При цьому сеансові ключі шифрування коду мікропрограми або її розшифрування формується відповідно на стороні клієнта і хоста. Цей підхід дозволяє створювати унікальні завантаження оригіналу коду мікропрограм (додатку) шляхом недопущення отримання криптоаналітиками її образів і алгоритмів.

Особливістю схеми обміну симетричними сеансовими ключами шифрування повідомлень є: 1) виконання на основі генерування випадкового числа на стороні хоста та використання таємного ключа, що зберігається на стороні хоста і клієнта; 2) сеансовий ключ визначається як результат хешування випадкового числа з таємним ключем та виділення певної частини з дайджесту, отриманого за результатом хешування; 3) для забезпечення захищеності передавання сеансового ключа на сторону клієнта виконується за рахунок шифрування деяких даних сеансовим ключем; 4) виділення сеансового ключа на стороні клієнта здійснюється за тією ж самою що на стороні хоста на основі випадкового числа та таємного ключа.

Для захищеного зберігання даних використовується шифрування швидким симетричним алгоритмом AES. При цьому сеансовий ключ шифрування для цієї операції формується шляхом хешування деякої початкової послідовності (випадково число) і таємного ключа, який надійно і безпечно зберігається на стороні шифрування. Передування конфіденційних даних можливо в мережі в зашифрованому файлі.

Для безпечного зберігання системних паролів потрібно зберігати їх в захищеної енергонезалежної пам’яті криптологічної мікросхеми, оскільки мікропрограма стандартного мікроконтролера може бути зламана. При цьому, порівняння паролів, що вводиться в мікроконтролер, з еталонним, що зберігається в пам’яті криптологічної мікросхеми доцільно виконувати у захищеному середовище як порівнювання результатів хешування цих паролів з певним випадковим числом.

Таким чином, застосування апаратно захищених мікросхем для забезпечення безпеки інтернет речей базується на зберіганні ключів в зашифрованому вигляді та в захищеному обладнанні і виконанні операцій зашифровування і розшифрування даних відбувається в захищеному середовищі.

Список використаних джерел

1. Петренко А.Б., Шматок О.С., Агеєнко Є.О. Аналіз часових атак на апаратний шифратор персонального засобу криптографічного захисту інформації ШИПКА. Наукоємні технології. 2014, № 2 (22), С. 187–191.

2. Совин Я.Р., Наконечний Ю.М., Опірський І.Р., Стахів М.Ю. Аналіз апаратної підтримки криптографії у пристроях інтернету речей. Ukrainian Scientific Journal of Information

Security, 2018, Vol. 24, Issue 1, pp. 36–48.

3. Klimushin P., Solianyk T., Kolisnyk T., Mozhaev O.. Potential application of hardware protected symmetric authentication microcircuitsto ensure the securityof internet of things. *Advanced Information Systems*. 2021. Vol. 5, No. 3, pp. 103–111.

Одержано 17.04.2022

УДК 004.056.5

КОБЗЕВ Ігор Володимирович,
кандидат технічних наук, доцент,
доцент Харківського національного університету ім. В. Н. Каразіна
https://orcid.org/0000-0002-7182-5814;
ГОРЕЛОВ Юрій Петрович,
кандидат технічних наук, доцент,
доцент кафедри кібербезпеки та DATA-технологій факультету № 6
Харківського національного університету внутрішніх справ
https://orcid.org/0000-0002-0330-5008

ДЕЯКІ АСПЕКТИ РЕАЛІЗАЦІЇ ДИСТАНЦІЙНОГО НАВЧАННЯ В УМОВАХ ВІЙНИ

В умовах військових дій технологія дистанційного навчання (ДН) виявилась єдиною освітньою технологією, яка дозволила ВНЗ продовжувати надання освітніх послуг здобувачам вищої та середньої освяти.

Поєднання освітніх та інформаційних технологій забезпечує можливість швидкого, досить дешевого поширення навчальної інформації, її адресної доставки на необмежену відстань у будь-який час та активізації роботи багатьох закладів освіти з продовження навчального процесу. Особливого поширення використання ДН набуло під час епідемії COVID-19. Це дозволило багатьом ВНЗ відпрацювати багато питань з впровадження та використання ДН у навчальному процесі. З початком воєнних дій ці ВНЗ вже виявились готовими до використання ДН як основної форми навчання.

ВНЗ використовують різноманітні LMS, серед яких найбільш популярні: Moodle, TrainingWare, Claroline LMS та ін.

Технології ДН дозволили не тільки реалізувати швидкий та зручний доступ до навчального матеріалу, але й застосовувати технології спільної творчої діяльності (метод проектів), проблемні ролеві ігри, кейс-методи, автоматизовані та відкриті форми контролю, як автоматизовані, так і відкриті види контролю та ін.

Але ситуація під час війни має декілька відмінностей у порівнянні з ситуацією під час карантину:

– нестабільність або повна відсутність доступу до Інтернету;
– неможливість виходу до мережі у певні моменти або інтервали часу;
– психологічний стан студентів.

Це має вплив на вибір методів ДН та його організацію. Так, майже неможливим є використання синхронних форм навчання, які вимагають присутності кількох студентів у LMS у певний час (відеолекції, тести з обмеженнями у часі, групові заняття та ін.) або виконання завдань з привязкою у часі.

У цих умовах раціональнім є використання асинхронних методів, що дозволяють студентам вивчати матеріал та виконувати завдання без врахування фактору часу або географічного місця знаходження студента.

У якості навчальних матеріалів доцільно використовувати текстові лекції або заздалегідь записані відео занять. Слід обмежити випадки, коли у студентів під час опрацювання навчального матеріалу виникає необхідність використовувати додаткові джерела, які складно знайти в мережі.

Не варто обмежувати доступ до навчального матеріалу певними проміжками часу. Під час організації тестування необхідно передбачити можливість використання декількох спроб проходження тестів.

Окремою проблемою є мотиваційні фактори, які необхідно також врахувати під час використання ДН. Практика показує, що активність студентів в умовах воєнних дій може різко знижуватися, тому важно мати з ними постійний контакт та забезпечувати психологічну підтримку.

Також гостро стає питання забезпечення інформаційної безпеки під час навчання. До інформаційних загроз можна віднести: неавторизований доступ до цифрового контенту; порушення цілісності і неадекватність навчальних ресурсів; порушення нормального функціонування служб і сервісів; порушення безпеки процедур тестування.

Одержано 30.04.2022

УДК 004.7

КОЛІСНИК Тетяна Петрівна,
кандидат педагогічних наук, доцент,
доцент кафедри протидії кіберзлочинності факультету № 4
Харківського національного університету внутрішніх справ
https://orcid.org/0000-0002-74428136

ЦИФРОВА ТРАНСФОРМАЦІЯ СИСТЕМИ МІНІСТЕРСТВА ВНУТРІШНІХ СПРАВ УКРАЇНИ НА ПЕРІОД ДО 2023 РОКУ

Наказом МВС України від 22 квітня 2021 року № 301 затверджено Концепцію програми інформатизації системи МВС України та центральних органів виконавчої влади (ЦОВВ), діяльність яких спрямовується і координується Кабінетом Міністрів України через Міністра внутрішніх справ України, на 2021-2023 роки. Метою впровадження галузевої програми інформатизації на період 2021 – 2023 років є продовження позитивних напрацювань Програми з гармонізації можливостей органів системи МВС із питання розвитку цифрової інфраструктури системи МВС, спільне створення нових форматів розв'язання поточних завдань і закладення механізмів та ділових моделей для успішного подолання майбутніх викликів перед системою МВС, обумовлених впливом комплексу соціально-демографічних, економічних, політичних, правових, психологічних і технологічних чинників. Результатом реалізації цієї галузевої програми має стати формування політики, розроблення низки стратегічних документів, які визначатимуть візію, чітке бачення подальшої цифрової трансформації органів системи МВС, розроблення стратегічного майстер-плану досягнення цієї візії з відповідними показниками змін (KPIs), плану реалізації галузевої програми та проведення моніторингу щодо оцінки успішності процесів цифрової трансформації.

Інтеграція цифрових технологій у процеси діяльності органів системи МВС має стати пріоритетом державної політики при створенні єдиної стійкої функціональної системи внутрішніх справ як частини сектору національної безпеки.

Нова галузева програма інформатизації системи МВС та ЦОВВ зосереджена на розбудові публічних сервісів єдиної інформаційної системи МВС, упровадженні та модернізації національних електронних інформаційних ресурсів як складових ЄІС МВС, створенні інноваційної інфраструктури органів системи МВС, підвищенні довіри і безпеки при використанні ІКТ, створенні в новостворених функціональних підсистемах ЄІС МВС [1] комплексних систем захисту інформації та вжитті заходів із забезпечення кіберзахисту цих систем, подальшій структуризації законодавчих та нормативно-правових документів сфери інформатизації органів системи МВС.

Дзеркалом стану модернізації та оптимізації діяльності органів системи МВС за допомогою цифрових технологій повинна стати цифрова екосистема – Концепція, що свідчить

про наступну фазу цифровізації органів системи МВС, де вперед виходять такі технології, як аналітика великих даних (Big Data), предиктивна аналітика, хмарні обчислення, бездротові комунікації, дистанційне управління та обслуговування, інтеграція систем управління та загалом передбачає ефективне функціонування органів системи МВС у цифровій інфраструктурі країни [2].

Реалізація галузевих проектів інформатизації закріплена у розпорядженні Кабінету Міністрів України від 17 лютого 2021 р. № 365-р [3], яким схвалено наступні проекти цифрової трансформації системи Міністерства внутрішніх справ України на період до 2023 року: Безпечна країна; Система 112; Модернізація електронних інформаційних ресурсів у сфері безпеки дорожнього руху; Єдиний реєстр зброї; Реєстр відомостей про статус особи у кримінальному провадженні та судимості; Єдиний сервіс ідентифікації фізичних осіб; Єдиний Державний реєстр територіальних громад; Система планування та управління об'єднаними силами із забезпечення громадської безпеки та ліквідації надзвичайних ситуацій; Модернізація загальнодержавної автоматизованої системи централізованого оповіщення; Територіальна автоматизована система централізованого оповіщення; Єдина база сил цивільного захисту; Модернізація підсистеми Реєстрації місця проживання Єдиної інформаційно-аналітичної системи управління міграційними процесами в Україні; Створення підсистеми Статистики та аналітики Єдиної інформаційно-аналітичної системи управління міграційними процесами в Україні; Поліцейські послуги (My Pol); Розвиток сервісів для осіб, що перетинають державний кордон; Автоматизація ділових процесів працівників прикордонної служби.

Під час реалізації галузевої програми інформатизації упродовж 2021 – 2023 років плануються запровадження та подальший розвиток електронних сервісів у найбільш актуальних сферах життєдіяльності суспільства, зокрема у сфері розбудови єдиного середовища електронної ідентифікації та автентифікації фізичних осіб, єдиного адресного простору, синхронізації даних реєстрів територіальних громад тощо.

Список використаних джерел

1. Про затвердження Положення про Єдину Інформаційну Систему Міністерства внутрішніх справ та переліку її пріоритетних інформаційних ресурсів: Постанова КМУ від 14.11.2018 № 1024 // База даних «Законодавство України» / Верховна Рада України. URL: https://zakon.rada.gov.ua/laws/show/1024-2018-%D0%BF (дата звернення: 12.04.2022).

2. Концепція програми інформатизації системи Міністерства внутрішніх справ України та центральних органів виконавчої влади, діяльність яких спрямовується і координується Кабінетом Міністрів України через Міністра внутрішніх справ України, на 2021-2023 роки: Рішення колегії Міністерства внутрішніх справ України від 22 квітня 2021 року № 5 км.

3. Деякі питання цифрової трансформації: Розпорядження КМУ від 17 лютого 2021 року № 365-р // База даних «Законодавство України» / Верховна Рада України. URL: https://zakon.rada.gov.ua/laws/show/365-2021-%D1%80#Text (дата звернення: 12.04.2022).

Одержано 13.04.2022

UDC 004.49
LIQIANG Zhang,
Intermediate Grade of Experimenter, Teacher of College of Computer Science Neijiang Normal University Neijiang (China);
SEMENOV Serhii,
Doctor of Science, Professor, Professor of the Department of Cybersecurity and Information Technology, Kharkiv National Economic University

DEVELOPMENT OF A NEURAL NETWORK ARCHITECTURE FOR SOLVING THE PROBLEM OF SUPPORTING DECISION MAKING ON SOFTWARE SECURITY

After performing one of the important steps - extraction of security features, which is usually performed without a teacher, the second important step is the choice of a reasonably small number of features that concentrate the most significant information about the input (classified) data. Despite the fact that an artificial neural network can independently carry out classification, it is recommended to supplement it with a training scheme with a teacher to improve performance.

It is also recommended that the artificial neural network be able to scale as new security features or sets of security requirements are added. All vector elements F_{sec} must be normalized with respect to the range of possible values of the chosen neuron model.

On fig. 1. a model of an artificial neural network is presented that corresponds to the general scheme of the method for supporting decision making on software security.

To solve the problem, one hidden layer of neurons is enough [1, 2]. To build the final model of an artificial neural network, it is necessary to determine the number of neurons in the hidden layer, i.e. calculate its power.

To estimate the number of neurons in the hidden layers of homogeneous neural networks, you can use the formula for estimating the required number of synaptic weights L_w (in a multilayer network with sigmoidal transfer functions) [3]:

$$\frac{mN}{1+\log_2 N} \le L_w \le m\left(\frac{N}{m}+1\right)(m+n+1)+m, \qquad (1)$$

where n – размерность входного вектора;
m – dimension of the input vector;
N – number of training sample elements.

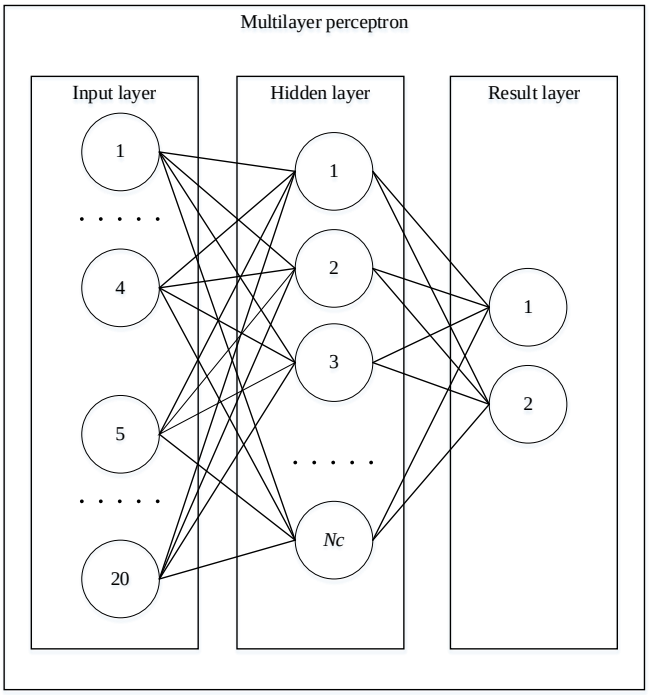

Fig. 1. Artificial neural network model

Having estimated the required number of weights, we can calculate the number of neurons in the hidden layers. For a neural network with one hidden layer, the calculation is carried out according to the formula (2) [4].

$$L = \frac{L_w}{n+m}. \tag{2}$$

The dependence of the number of neurons in the hidden layers of the network on the number of weight connections is shown in Fig.2.

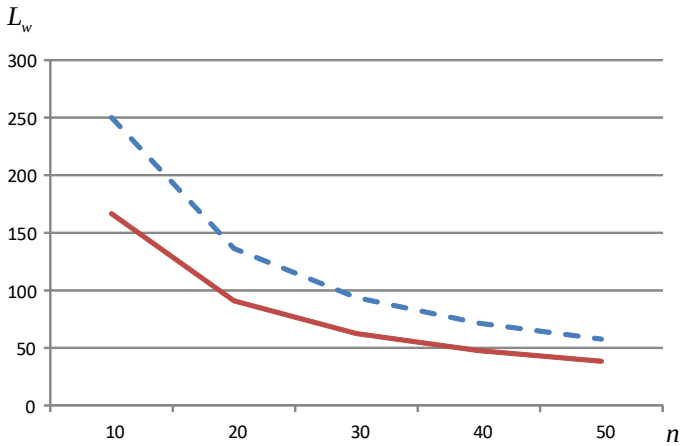

Fig. 2. Dependence of the number of neurons in the hidden layers of the network on the number of weight connections

It should be noted that the number of neurons in an artificial neural network should not be less than the number of classes, and since the exact number of classes may not be known in advance, the

number of neurons is set with a certain margin. "Superfluous" neurons, whose weights will change chaotically during the learning process, can be removed at the end of this process.

Literature

1. Semenov, S. ., Liqiang, Z., Weiling, C., & Davydov, V. (2021). Development a mathematical model for the software security testing first stage. Eastern-European Journal of Enterprise Technologies, 3(2 (111), 24–34. https://doi.org/10.15587/1729-4061.2021.233417.

2. Zongyuan Zhao, Shuxiang Xu, Byeong Ho Kang, Mir Md Jahangir Kabir, Yunling Liu, Rainer Wasinger, Investigation and improvement of multi-layer perceptron neural networks for credit scoring, Expert Systems with Applications, Volume 42, Issue 7, 2015, Pages 3508-3516, ISSN 0957-4174, https://doi.org/10.1016/j.eswa.2014.12.006.

3. . W. Zaki et al., "A Novel Sigmoid Function Approximation Suitable for Neural Networks on FPGA," 2019 15th International Computer Engineering Conference (ICENCO), 2019, pp. 95-99, doi: 10.1109/ICENCO48310.2019.9027479.

4. Kleyko D., Rosato A., Paxon F. E., Panella M., Sommer F. T. Perceptron Theory for Predicting the Accuracy of Neural Networks https://arxiv.org/pdf/2012.07881.pdf.

Одержано 14.04.2022

УДК 65.012.8+004

МАНЖАЙ Олександр Володимирович,
кандидат юридичних наук, доцент,
завідувач кафедри протидії кіберзлочинності факультету № 4
Харківського національного університету внутрішніх справ
https://orcid.org/0000-0001-5435-5921
МАНЖАЙ Ірина Андріївна,
завідувач навчального відділу Харківського університету

СУЧАСНІ ТЕНДЕНЦІЇ У ВІТЧИЗНЯНОМУ СЕКТОРІ ЗАБЕЗПЕЧЕННЯ БЕЗПЕКИ ІНФОРМАЦІЇ

У новому українському законодавстві на теперішній час формується розуміння термінології у сфері безпеки інформації, яке дещо відрізняється від класичного. Серед іншого це пов’язано з низкою серйозних викликів в інформаційному просторі держави, які посилилися у 2014 році і тривають донині. Водночас, залишені старі нормативні документи, продовжуючи класичні традиції формування безпеки інформації, можуть утворювати деяку плутанину та неузгодженість. Серед іншого це стосується таких категорій як «інформаційна безпека» та «кібербезпека».

Ще не так давно термін «інформаційна безпека» був узагальнюючим до тієї ж «кібербезпеки» та/або «захисту інформації». Саме такий стан речей випливає із все ще чинного Закону України, яким визначено основні засади розвитку інформаційного суспільства в Україні на 2007–2015 роки. Зокрема у п. 13 розділу ІІІ цього закону зазначено, що під ***інформаційною безпекою*** розуміється стан захищеності життєво важливих інтересів людини, суспільства і держави, за якого запобігається нанесення шкоди через: неповноту, невчасність і невірогідність інформації, що використовується; негативний інформаційний вплив; негативні наслідки застосування інформаційних технологій; несанкціоноване розповсюдження, використання і порушення цілісності, конфіденційності та доступності інформації.

Водночас прийняття нової Доктрини інформаційної безпеки засвідчило, що у вищих органах державної влади інформаційна безпека асоціюється радше з протидією дезінформації, забезпеченням безпеки інформаційного простору, як середовища впливу на світосприйняття людини, але аж ніяк не з кібербезпекою чи технічним захистом інформації.

У розумінні значення «кібербезпеки» також досі не простежується єдиного підходу. Так, у 2015 році запровадження нової спеціальності 125 «Кібербезпека» розпочало процес об’єднання дещо різних за змістом напрямів підготовки: «Системи технічного захисту інфор-

мації», «Безпека інформаційних та комунікаційних систем», «Управління інформаційною безпекою». Водночас на законодавчому рівні кібербезпека стосується переважно безпеки у кіберпросторі та аж ніяк не охоплює технічний захист інформації фізичних об'єктів. Отже, питання змісту термінології у сфері безпеки інформації наразі лишається відкритим.

Паралельно зі зміною підходів до розуміння термінологічного апарату у сфері безпеки в Україні простежується новий підхід до побудови системи безпеки на об'єктах інформаційної діяльності. Так, у 2020 р. на законодавчому рівні було запроваджено альтернативу досі монопольній комплексній системі захисту інформації (КСЗІ), а саме унормовано порядок впровадження системи управління інформаційною безпекою (СУІБ).

Відповідно до ч. 4 ст. 8 Закону України «Про захист інформації в інформаційно-телекомунікаційних системах» від 05.07.1994 державні інформаційні ресурси та інформація з обмеженим доступом, крім державної таємниці, службової інформації та державних і єдиних реєстрів, створення та забезпечення функціонування яких визначено законами, можуть оброблятися в системі ***без*** *застосування комплексної системи захисту інформації* у разі виконання **всіх** таких умов:

– підтвердження відповідності *системи управління інформаційною безпекою* за результатами процедури з оцінки відповідності національним стандартам України щодо систем управління інформаційною безпекою, яка проведена *органом з оцінки відповідності*, акредитованим національним органом України з акредитації чи національним органом з акредитації іншої держави, якщо і національний орган України з акредитації, і національний орган з акредитації такої держави є членами міжнародної або регіональної організації з акредитації та/або уклали з такою організацією угоду про взаємне визнання щодо оцінки відповідності;

– використання для захисту інформації в системі *засобів криптографічного захисту інформації, які мають позитивний експертний висновок* за результатами державної експертизи у сфері криптографічного захисту інформації;

– жоден з елементів системи не може бути *розташований на територіях* України, на яких органи державної влади України тимчасово не здійснюють своїх повноважень, на територіях держав, визнаних Верховною Радою України державами-агресорами, на територіях держав, щодо яких застосовані санкції відповідно до Закону України «Про санкції», та на територіях держав, які входять до митних союзів з такими державами;

– *виконання особливих вимог*, встановлених Кабінетом Міністрів України до забезпечення захисту інформації в системах залежно від категорії державних інформаційних ресурсів або інформації з обмеженим доступом (вимога щодо захисту якої встановлена законом, що обробляються.

Етапи побудови СУІБ дещо відрізняються від аналогічного процесу щодо КСЗІ. У загальному вигляді їх можна представити так:

– *визначення сфери дії* СУІБ;

– *попередня перевірка відповідності* системи безпеки організації вимогам стандарту ДСТУ ISO/IEC 27001:2015 Інформаційні технології. Методи захисту. Системи управління інформаційною безпекою. Вимоги. На цьому етапі можуть бути застосовані й інші стандарти, у тому числі ДСТУ ISO/IEC 27004:2018 Інформаційні технології. Методи захисту. Системи керування інформаційною безпекою. Моніторинг, вимірювання, аналізування та оцінювання;

– *оцінка ризиків*, де основою для вибору відповідної методики є стандарт ДСТУ ISO/IEC 27005:2019 Інформаційні технології. Методи захисту. Управління ризиками інформаційної безпеки;

– *опис процедур та їх документування*. На цьому етапі описуються процеси у сфері управління та забезпечення безпеки, які потрібно виконати, а також формується відповідна документація;

– *впровадження процедур та відповідної документації*;

– *дослідна експлуатація* СУІБ;

– *сертифікація*, яка проводиться у формі аудиту, за результатами якого організація має отримати сертифікат про відповідність СУІБ вимогам ДСТУ ISO/IEC 27001:2015.

Отже, нормативно-правова база кібернетичної та інформаційної безпеки на теперішній час перебуває в процесі становлення. Для убезпечення державних ресурсів в інформаційних системах можуть бути створені або комплексна система захисту інформації, або система управління інформаційною безпекою. Вимоги до обох видів систем та порядок їх побудови є недостатньо визначеними на законодавчому рівні та потребують удосконалення. СУІБ є певною альтернативою КСЗІ, її запровадження обумовлене тенденціями у світових процесах з безпеки. Проте в Україні СУІБ є досить новим механізмом і на законодавчому рівні унормований лише в червні 2020 року.

Одержано 07.04.2022

УДК 65.012.8+004
МОГІЛЕВСЬКИЙ Леонід Володимирович,
доктор юридичних наук, професор,
заслужений юрист України,
проректор Харківського національного університету внутрішніх справ
https://orcid.org/0000-0002-6994-6086

ІНСТРУМЕНТИ ВИЯВЛЕННЯ НЕПРАВДИВИХ ПОВІДОМЛЕНЬ

Для перевірки повідомлень та інших матеріалів на предмет їх актуальності та достовірності можуть бути використані різні аналітичні методи. Для полегшення цього процесу також варто застосовувати і низку технічних рішень. Серед подібних інструментів можна виділити розширення Fake Profile Detector (Deepfake, GAN) – інструмент, який працює у браузерах на базі Chrome або Chromium і дає змогу ідентифікувати заображення, створені з використанням штучного інтелекту (рис. 1). Саме тому, якщо обличчя реальної людини додано до іншого зображення, воно теж визначатиметься як справжнє. Розширення доступне за посиланням https: //chrome.google.com/webstore/detail/fake-profile-detectordee/jbpcgcnnhmjmajjkgdaogpgefbnokpcc/related?hl=en-US.

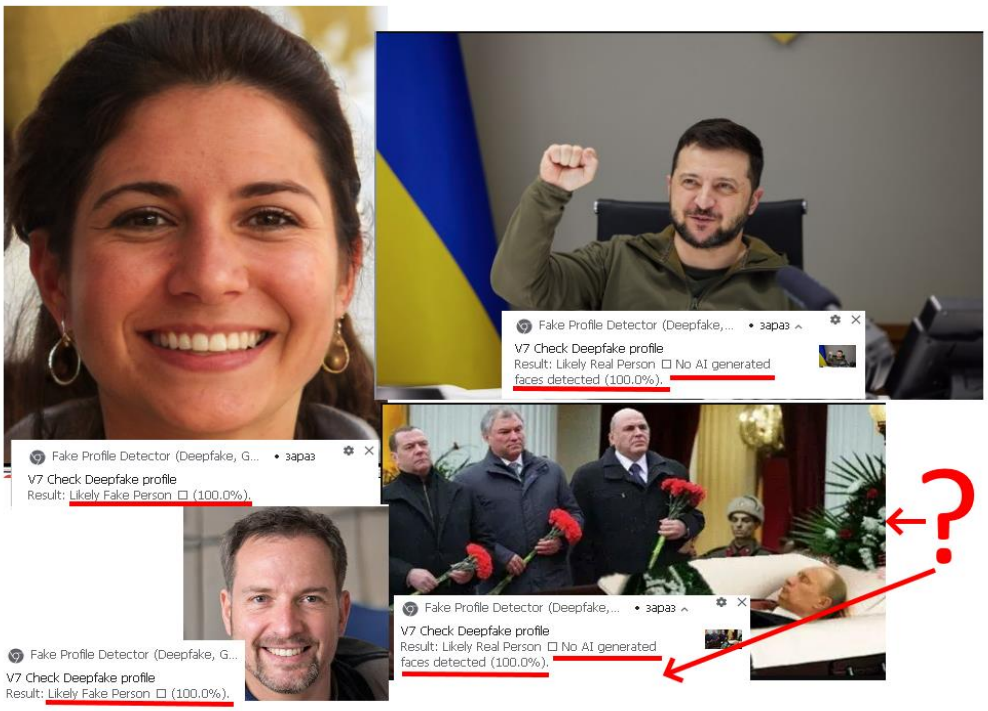

Рис. 1. Результат роботи розширення з виявлення діпфейків

Зображення можуть не мати ознак маніпуляцій, проте використовуватися в неправдивих повідомленнях у різних контекстах. Для того, щоб знайти першоджерело відповідних малюнків, можна використовувати розширення Who stole my pictures (рис. 2).

Завантажити описане розширення можна за адресами:

– для браузеру «Chrome» (https://chrome.google.com/webstore/detail/who-stole-my-pictures/mcdbnfhkikiofkkicppioekloflmaibd);

– для браузеру «Firefox» (https://addons.mozilla.org/ru/firefox/addon/who-stole-my-pictures/).

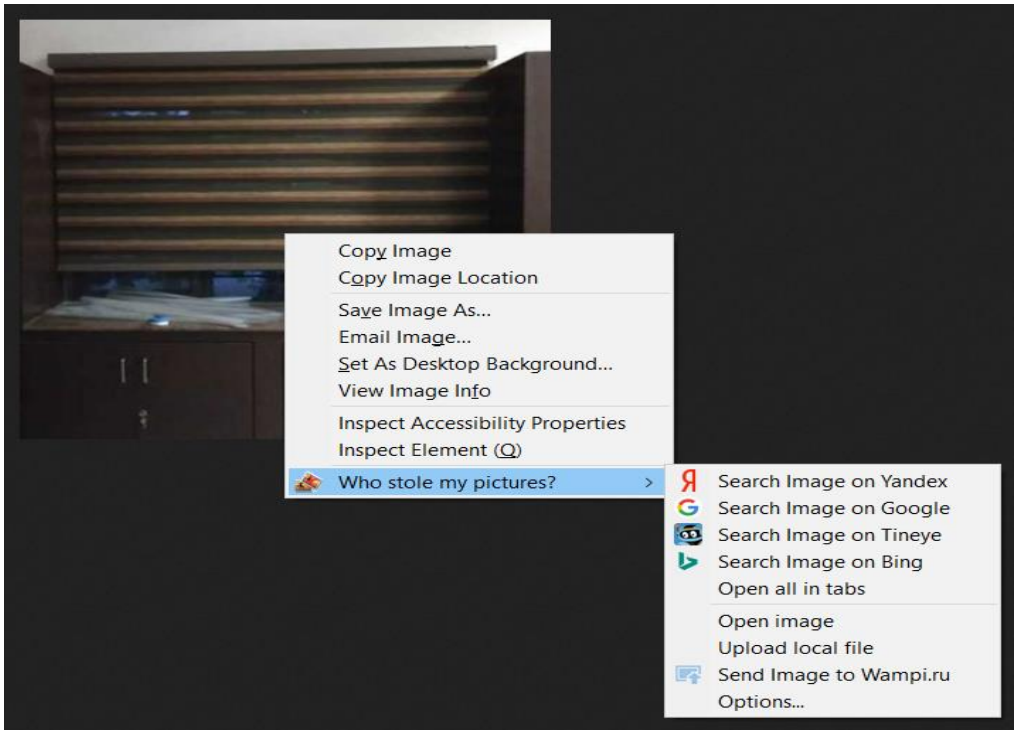

Рис. 2. Використання розширення для пошуку зображень

Велика кількість інструментів розпізнавання фейків доступні на сайтах stopfake.org, snopes.com, factcheck.org, truthorfiction.com.

Найбільш складним і часовитратним, проте достатньо ефективним методом протидії неправдивим повідомленням є підвищення аналітичних здібностей суспільства, навчання методам критичного аналізу повідомлень, убезпечення від інформаційних диверсій. Усе наведене дає підстави говорити про необхідність активізації в нашій країні зусиль із розбудови ефективної структури інформаційного протиборства.

Одержано 29.04.2022

УДК 004.04:004.67:004.77
МОЖАЄВ Олександр Олександрович,
доктор технічних наук, професор,
професор кафедри кібербезпеки та DATA-технологій факультету № 6
Харківського національного університету внутрішніх справ
https://orcid.org/0000-0002-1412-2696;
РОГ Вікторія Євгенівна,
старший викладач кафедри протидії кіберзлочинності факультету № 4
Харківського національного університету внутрішніх справ
https://orcid.org/0000-0002-7443-5125

УДОСКОНАЛЕННЯ МАТЕМАТИЧНОЇ МОДЕЛІ ОПТИЧНИХ КАНАЛІВ ПЕРЕДАЧІ ІНФОРМАЦІЇ

Інформаційні системи (ІС) відіграють значну роль в системі судових експертиз. Використання ІС дозволяє істотно підвищити якість виконуваних експертиз за рахунок зниження людського фактора. Для забезпечення надійного та оперативного обміну первинними даними, службової інформації, результатами експертизи необхідним є підвищення якості обслуговування (QoS) телекомунікаційною мережею інформаційної системи судової експертизи. Тому телекомунікаційна мережа ІС судової експертизи повинна забезпечувати дотримання жорстких вимог по підтримці параметрів якості обслуговування (QoS) [1-4], що в підсумку дозволить всій інформаційній системі вирішити поставлені перед нею завдання.

Забезпечення підвищення якості передачі даних можна досягти застосуванням повністю оптичних технологій, що актуально в даний час і для досліджуваної мережі ІС судової експертизи. Але навіть незначні зміни протоколів передачі та обробки інформації на фізичному рівні можуть призвести до суттєвих змін на всіх вищих рівнях класичної моделі OSI ISO. Причому такі зміни можуть інтегрально зростати в міру переходу на більш високий рівень моделі.

Таким чином, перед дослідниками стоїть досить важлива і актуальна задача забезпечення контролю за станом передачі інформації на фізичному рівні в оптичних каналах зв’язку.

Для опису процесу передачі інформації в неоднорідному нелінійному середовищі, яким можна вважати і оптичне середовище передачі інформації, перспективно скористатися формалізмом континуальних інтегралів (КІ) Фейман, які можуть дозволити проводити оцінку імовірнісних характеристик даних.

Використання КІ надає можливість провести аналіз результатів, які отримані при використанні альтернативних методів досліджень. Відмінною особливістю континуальних інтегралів є можливість знаходжень точних рішень, за умови їх існування. Застосування КІ дозволяє отримати максимальний результат у разі модифікації стандартної теорії збурень, з огляду на те, що використовуваний математичний апарат дозволяє здійснювати відповідні налаштування і визначати спосіб її конкретної реалізації.

Сувора математична теорія і коректне визначення, в даний час, отримані лише для частини безлічі КІ. Але в рамках теорії збурень, використовуючи КІ спеціального випадку - гаусового, формалізм КІ є достатньо суворим, і отримані результати не потребують додаткового обґрунтування

При вирішенні завдань дифракції в хвильовій теорії світла, метод континуальних інтегралів використовувався в теорії поширення хвиль в випадково-неоднорідних середовищах, а в подальшому отримав природний розвиток в атмосферній оптиці.

Перевагою методу КІ є легкість включення в дослідження анізотропії, регулярної рефракції, неоднорідності по одній або декількох координатах.

Застосовуючи КІ, стало можливим проаналізувати випадок насичених флуктуацій, коли нормована дисперсія інтенсивності зі збільшенням довжини траси поширення досягає свого максимуму.

Пропонована доповідь присвячена визначенню можливості використання формалізму КІ для моделювання процесу поширення сигналу в оптичному каналі зв'язку за рахунок дослідження просторово-часових і просторово-частотних кореляцій поля хвилі. Таке завдання є надзвичайно складним через труднощі отримання виразів для просторово-часових моментів довільного порядку. Одним із прийнятних рішень такого завдання є пошук або висновок рівнянь, які можна вирішити чисельне.

Список використаних джерел

1. Кучук Г. А. Рубан І. В., Давікоза О. П. Концептуальний підхід до синтезу структури інформаційно-телекомунікаційної мережі. *Системи обробки інформації : збірник наукових праць*. Х.: ХУПС, 2013. – Вип. 7 (114). – С. 106 – 112.

2. Lemeshko, O., Yevdokymenko, M., Yeremenko, O. (2019), "Model of data traffic QoS fast rerouting in infocommunication networks", *Innovative Technologies and Scientific Solutions for Industries*, No. 3 (9), P. 127–134.DOI: https://doi.org/10.30837/2522-9818.2019.9.127.

3. Zykov, I., Kuchuk, N., Shmatkov, S. (2018), "Architecture synthesis of the computer system of transaction control e-learning", *Advanced Information Systems*, Vol. 2, No. 3, P. 60–66. DOI: https://doi.org/10.20998/2522-9052.2018.3.10.

4. Mozhaev, O., Kuchuk, H., Kuchuk, N., Mozhaev, M., Lohvynenco, M. (2017), "Multiservise network security metric", *IEEE Advanced information and communication technologies-2017, Proc. of the 2th Int. Conf. Lviv, 2017*, P. 133–136.

Одержано 19.04.2022

УДК 343.1+004

НОСОВ Віталій Вікторович,
кандидат технічних наук, доцент,
професор кафедри протидії кіберзлочинності факультету № 4
Харківського національного університету внутрішніх справ
https://orcid.org/0000-0002-7848-6448

ДЕЯКІ АСПЕКТИ УПРАВЛІННЯ РЕСУРСАМИ СУІБ

Системним рішенням у боротьбі із кіберзлочинністю на рівні організацій є побудова і впровадження визначеної системи захисту інформації.

Наразі Закон України «Про захист інформації в інформаційно-комунікаційних системах» [ст. 8, 1] дозволяє для організацій, які оброблюють державні інформаційні ресурси або інформацію з обмеженим доступом, крім державної таємниці, службової інформації та державних і єдиних реєстрів, застосувати з підтвердженою відповідністю або комплексну системи захисту інформації, або систему управління інформаційною безпекою (СУІБ). СУІБ повинна відповідати вимогам стандарту України «ДСТУ ISO/IEC 27001:2015 Інформаційні технології. Методи захисту. Системи управління інформаційною безпекою. Вимоги» [2].

Вимоги ДСТУ ISO/IEC 27001 серед іншого передбачають визначення ризиків інформаційної безпеки організації, їх оцінку, прийняття рішення щодо обробки (зниження) неприйнятних ризиків, обробки ризиків та їх моніторинг, використовуючи політику та процедури, що визначені в СУІБ. В Додатку А ДСТУ ISO/IEC 27001 наведені типові заходи інформаційної безпеки, що дозволяють знижувати ризики інформаційної безпеки організації і серед яких зазначена необхідність управління ресурсами СУІБ.

Під ресурсами СУІБ розуміється все, що має цінність для організації: люди, активи, інформація, тощо, які повинні враховуватися для забезпечення ефективного управління інформаційною безпекою. З метою забезпечення належного рівня захисту інформації відповідно до її важливості для організації потрібно з урахуванням критичності й чутливості для неавторизованого розкриття чи модифікації інформації здійснити її класифікацію та маркування,

що передбачає розробку та впровадження належної сукупності відповідних процедур маркування й оброблення інформації згідно зі схемою класифікації, прийнятою організацією.

З практичної точки зору для інформації, що не становить державної таємниці і не є службовою, в організації можна застосувати класифікацію, маркування і відповідну її обробку як у Протоколі світлофора (Traffic Light Protocol, TLP) [3] міжнародної спільноти з реагування на інциденти комп'ютерної безпеки FIRST [4].

З урахуванням критичності й чутливості для неавторизованого розкриття чи модифікації інформації встановлюється чотири категорії інформації, які позначаються кольоровими мітками: червоний, жовтий, зелений, білий, з наступним порядком доступу:

– **червоний**. Інформація для поширення і доступу тільки для зазначеної особи або осіб;

– **жовтий**. Інформація для поширення і доступу тільки серед працівників організації;

– **зелений**. Інформація для поширення і доступу в межах відомства (міністерства) для установ, або визначеної групи компаній для недержавних організацій;

– **білий**. Інформація не має обмежень у поширенні і доступу.

Класифікацію і нанесення міток здійснюють особи, які несуть адміністративну відповідальність за створення, розробку, зберігання, використання та управління відповідною інформацією.

Така класифікація інформації із відповідними позначеннями дозволить включити в ресурси СУІБ так звану технологічну інформацію (логіни, паролі, ґеші паролів, переліки доменів, мережні налаштування, події в журналах аудиту, тощо), що значно підсилить адміністративну відповідальність користувачів інформаційно-комунікаційних систем організації.

Список використаних джерел

1. Про захист інформації в інформаційно-комунікаційних системах: Закон України від 05.07.1994 № 80/94-ВР, редакція від 01.01.2022 // База даних «Законодавство України»/Верховна Рада України. URL: https://zakon.rada.gov.ua/laws/show/80/94-%D0%B2%D1%80#top (дата звернення: 23.04.2022).

2. ДСТУ ISO/IEC 27001:2015 Інформаційні технології. Методи захисту. Системи управління інформаційною безпекою. Вимоги. ДП «УкрНДНЦ», 2016. 22 с.

3. TRAFFIC LIGHT PROTOCOL (TLP). FIRST Standards Definitions and Usage Guidance — Version 1.0. URL: https://www.first.org/tlp/docs/tlp-v1.pdf (дата звернення: 23.11.2022).

4. FIRST Organization. URL: https://www.first.org/about/organization (дата звернення: 23.04.2022).

Одержано 11.04.2022

УДК 004.056.5

СВІТЛИЧНИЙ Віталій Анатолійович,
кандидат технічних наук, доцент,
доцент кафедри протидії кіберзлочинності факультету № 4
Харківського національного університету внутрішніх справ
https://orcid.org/0000-0003-3381-3350

ДЕЯКІ ОСОБЛИВОСТІ КІБЕРАТАК ЗА ДОПОМОГОЮ АДРЕСНОГО ФІШИНГУ, КЛОН-ФІШИНГУ ТА УЕЙЛІНГУ

Фішинг є одним з найбільш ефективних методів, які використовуються хакерами для крадіжки облікових даних. Тобто фішинг - це набір методик, які використовують хакери, щоб стягнути особисту інформацію, наприклад, якийсь логін з паролем або дані кредитних карток. Ці техніки відрізняються від інших варіантів злому підходом до взаємодії з жертвою. Використання вірусів або DOS-атака найчастіше спрямовані на програмне забезпечення. Фішинг же зав'язаний на контакті з живою людиною, яка через відсутність навичок роботи з

комп'ютером або банальної наївності, сам підставиться під хакера і видасть йому щось конфіденційне.

Існує безліч способів зіграти на почуттях людей. Всі вони використовуються для того, щоб зробити психологічну атаку на жертв і обдурити їх, наприклад:

– заманити жертву безкоштовними пропозиціями, оскільки любителі «халявного» завжди знайдуться;

– використовувати шум, що виникає на ажіотажі якоїсь теми;

– запросити жертву скачати квитки на тести або захід через електронні сервіси та ін.

Внаслідок такої атаки жертва відкриває доступ вірусу на комп'ютер та втрачає особисті дані.

Методи фішингових атак. Більшість фішингових атак починаються з електронного листа, який виглядає так, ніби його надіслав цілком законне джерело, проте наступні способи атаки та проникнення можуть бути різними. Деякі способи досить прості і полягають у тому, щоб обманом змусити користувача натиснути на посилання та ввести конфіденційну інформацію, інші ж більш витончені, наприклад, запуск виконуваного файлу, який імітує корисний процес і отримує доступ до комп'ютера та мережі жертви, щоб непомітно запустити там шкідливу програму.

Зазвичай під час атаки фішингу для обману жертви використовується відразу кілька прийомів. Наприклад, нерідко хакери використовують маніпуляції з посиланнями та підробку веб-сайтів, що в комбінації надає їхнім діям максимальної переконливості. Перше, що ви бачите при отриманні фішингового електронного листа, це то що посилання виглядає цілком правдоподібно, та веде на сайт, який ви часто використовуєтеєі, та не викликає підозр, наприклад: Facebook, Amazon або YouTube, а також повідомлення, що під різними приводами закликає вас перейти за посиланням. Це повідомлення буде пропонувати користувачам ввести конфіденційну інформацію, стверджуючи, що з їх обліковим записом або замовленням виникла проблема, яку необхідно вирішити. Саме на цьому етапі в гру вступає наступний прийом - підробка веб-сайтів.

Хоча на перший погляд, посилання може виглядати зовсім як легітимний веб-сайт, скажімо, «amazon.com», при уважному розгляді можна виявити *невеликі невідповідності або нестиковки,* що розкривають справжню природу посилання. Створення таких шахрайських доменів, близьких за написанням до відомих сайтів, називається тайпсквоттінгом. Ці шкідливі сайти у всьому максимально схожі на реальні сторінки, і користувачі, що нічого не підозрюють, можуть ввести на них свої облікові дані. Хакери отримують можливість ввести вкрадені дані на цьому сайті.

Також хакери часто прикріплюють файл, що не викликає підозр, або додають посилання, при натисканні на яке буде таємно завантажено шкідливе програмне забезпечення, яке впровадиться в систему жертви. Ці атаки часто впроваджують шкідливу програму, що маскується під справжній файл. Працюючи у фоновому режимі, така програма переміщатиметься в мережі користувача з метою крадіжки конфіденційної інформації, такої як банківські рахунки, номери соціального страхування, облікові дані користувачів та багато іншого. Іноді шкідливе програмне забезпечення включає програму-вимагач, яка пробирається через мережу жертви, шифруючи та переміщуючи конфіденційні дані для зберігання з метою викупу.

Типи фішингових атак. Найбільш популярний метод атаки полягає у створенні максимально широкого охоплення. Хакери розсилають стандартні електронні листи від імені відомих сайтів максимально можливої кількості адресатів, сподіваючись, що хтось клюне на їхні хитрощі. Це ефективний, але не єдиний спосіб упіймати жертву на гачок.

Деякі кіберзлочинці для досягнення своїх цілей використовують більш точні методи, наприклад адресний (цільовий) фішинг, клон - фішинг та уейлінг.

Адресний фішинг та whaling (уейлінг). Як і у звичайних фішингових атаках, в адресному (цільовому) фішингу та уейлінг для обману жертв використовуються електронні листи з надійних джерел. Однак замість масового розсилання безлічі одержувачів адресний фішинг націлений на конкретних осіб або видає себе за особу, яка викликає довіру, для крадіжки облікових даних або інформації.

Подібно до адресного фішингу, уейлінг (дослівно - «полювання на китів») спрямований на конкретну високопоставлену особу. Мисливці на китів прагнуть видати себе за вище керівництво, наприклад генерального директора, фінансового директора або начальника відділу кадрів, щоб переконати членів організації розкрити конфіденційну інформацію, що представляє для них цінність.

Щоб уейлінг увінчався успіхом, хакери повинні набагато краще вивчити свою жертву в порівнянні зі звичайним фішингом, щоб виглядати якомога достовірніше. Кіберзлочинці розраховують скористатися авторитетом керівника, за якого себе видають, щоб переконати співробітників або інших керівників не перевіряти і не ставити під сумнів їхні запити.

Клон-фішинг не такий винахідливий, як адресний фішинг або уейлінг, але від цього не менш ефективний. Цьому методу атаки притаманні всі основні елементи шахрайства фішингу, а різниця полягає в тому, що замість того, щоб видати себе за користувача або організацію з конкретним запитом, хакери копіюють реальний електронний лист, який раніше було відправлено легітимною організацією. Потім вони використовують маніпуляції з посиланнями для заміни реального посилання з вихідного електронного листа та перенаправлення жертви на шахрайський сайт. Там хакери обманом намагаються змусити користувачів ввести облікові дані, які потім використовуватимуть на реальному сайті для того, щоб потрапити до обліку жертви.

В умовах воєнного стану в Україні, кількість інтернет-покупок досягла небачених масштабів, а отже, у шахраїв додалося роботи. У такий період, коли всі масово купують ліки або речі які тимчасово відсутні в аптеках або магазинах, кількість таких шахраїв зростає у геометричній прогресії.

Тому люди, що стають жертвами хакерів, сприяє тому факту, що інструменти для фішингових атак змінюються і стають витонченими.

Підроблені ресурси часто неможливо відрізнити від справжніх, вони мають безпечні адреси і майже працюють по **https,** причому з справжніми сертифікатами.

Найбільше фішинг може бути «успішним» при використанні мобільних девайсів. Через свої технічні особливості на планшетах та смартфонах розпізнати підроблений сайт набагато складніше, ніж на ноутбуку чи ПК. При цьому важливо розуміти, що дієвого захисту від фішингу немає, жодна платформа і загроза є універсальною для будь-якого пристрою.

Одержано 12.04.2022

УДК 004.056

СОЛЯНИК Тетяна Миколаївна,
кандидат технічних наук, доцент,
доцент кафедри протидії кіберзлочинності факультету № 4
Харківського національного університету внутрішніх справ
https://orcid.org/0000-0003-3695-0019

ОРГАНІЗАЦІЯ ВИЯВЛЕННЯ ВТОРГНЕНЬ У ЛОКАЛЬНІЙ МЕРЕЖІ ПІДПРИЄМСТВА

В наш час неможливо собі уявити жодного підприємства без корпоративної мережі, яка використовується для вирішення багатьох задач: звичайне поширення інформації, централізоване зберігання та доступ до великих обсягів даних, спільна робота над складним проектом тощо.

Одночасно зі зростанням попиту на такі корпоративні мережі, удосконаленням методів та засобів їх побудови та підтримки, на достатньо високому рівні залишаються злочинні можливості шахраїв з метою отримати доступ до таких корпоративних мереж у пошуках різної інформації.

З метою захисту цієї інформації доцільно використовувати комплексний багаторівневий захист, загальна структура якого включає наступні складові:

– політику безпеки мережі організації;
– систему захисту хостів в мережі;
– мережний аудит;
– захист на основі маршрутизаторів;
– міжмережні екрани;
– систему виявлення вторгнень;
– план реагування на виявлені атаки.

Одна з найважливіших компонент цього захисту – це виявлення вторгнень в комп'ютерну мережу, що є темою проведеного дослідження.

Підвищення ефективності захисту інформації в корпоративних мережах шляхом вибору та налаштування відповідної системи виявлення вторгнень на підприємстві є одним з прикладів протидії кіберзлочинності.

Аналіз процесу реалізації атаки на мережу виявив 3 основні етапи її скоєння: пошук інформації, реалізація та завершення. Спроба доступу до атакованого вузла відбувається на другому з них з метою отримання несанкціонованого доступу до вузла та інформації. Спроба доступу може бути безпосередньою, коли відбувається подолання засобів захисту периметру або вживлення шкідливих програм («троянський кінь»). Можливі ще опосередковані спроби доступу (наприклад, DoS атаки), коли відбувається втручання в роботу системи через налаштовані системні служби чи сервіси.

Основним засобом захисту від подібних правопорушень є ***система виявлення вторгнень*** – сукупність програмних та апаратних засобів, які аналізують мережні ресурси на наявність підозрілих або нетипових для мережі подій

Існує багато реалізацій подібних систем, але їх поєднують схожі функціональні вимоги:

– працювати безперервно без втручання людини;
– бути стійкою до збоїв;
– протистояти спробам руйнування системи;
– мати мінімальну надмірність;
– враховувати можливі відхилення від нормальної поведінки;
– бути легко адаптованою до певної мережі,
– адаптуватися до змін власної структури при подальшому вдосконаленні системи;
– бути стійкою до дезінформації.

Відповідно до напрямку дослідження в першу чергу нас цікавлять системи, які відрізняються за наступними критеріями:

– спосіб збору інформації;
– підхід та методи виявлення вторгнень;
– методи аналізу даних та стану системи.

Існує два основні типи систем виявлення вторгнень (СВВ):

1)Мережні СВВ (network intrusion detection system), які виявляють атаку на мережу в цілому.

2)Системні СВВ (Host-based intrusion detection system), виявляють атаку на певний вузол мережі.

Мережні СВВ працюють з мережними потоками даних, контролюють пакети в мережному оточенні і виявляють спроби проникнути всередину системи.

Переваги їх використання:

– можна повністю приховати в системі;
– моніторинг трафіку з великою кількістю цілей;
– можна здійснювати перехоплення вмісту всіх пакетів.

Серед недоліків слід відзначити те, що система лише видає сигнал тривоги, не може визначити, чи була атака успішною та інші.

Системні СВВ, на відміну від мережних, контролюють тільки один вузол, відстежуючи події, пов'язані з ним.

В СВВ використовуються два типи методів аналізу стану системи:

виявлення зловмисної поведінки, коли поточна послідовність дій в системі порівнюється з шаблонами атак. В результаті аналізу виділено основні параметри дій, типи шаблонів, що відповідають сигнатурі атак, а також основні чинники, що впливають на ефективність методу.

Відмінність методу *виявлення аномальної поведінки* полягає в тому, що визначають відхилення поточного стану системи від законної «звичайної» діяльності об'єкта. Для цього необхідно задати значення відповідних атрибутів методу.

В ході дослідження було розглянуто роботу найпопулярніших на цей час систем виявлення вторгнень, таких як Solarwinds, OSSEC, Suricata тощо. Усі наведені системи мають свої можливості та обмеження. яку систему обрати для використання буде залежати від цілей захисту, наявних технічних ресурсів та можливостей, а також переваг фахівця з кіберзахисту систем та мереж.

Одержано 19.04.2022

УДК 004.056.5

СТРУКОВ Володимир Михайлович,
кандидат технічних наук, доцент,
професор кафедри кібербезпеки та DATA-технологій факультету № 6
Харківського національного університету внутрішніх справ
https://orcid.org/0000-0003-4722-3159;
ГНУСОВ Юрій Валерійович,
кандидат технічних наук, доцент,
завідувач кафедри кібербезпеки та DATA-технологій факультету № 6
Харківського національного університету внутрішніх справ
https://orcid.org/0000-0001-5435-5921;
УЗЛОВ Дмитро Юрійович,
кандидат технічних наук,
доцент кафедри штучного інтелекту
Харківського національного університету радіоелектроніки
https://orcid.org/0000-0003-3308-424X

МОЖЛИВОСТІ ВИКОРИСТАННЯ МЕТОДІВ ГЛИБОКОГО АНАЛІЗУ «СЛАБКИХ СИГНАЛІВ» В УМОВАХ БОЙОВИХ ДІЙ

У розвинених країнах світу у поліцейській діяльності в рамках впровадження предикативної моделі діяльності [1, 3, 4] ефективно використовуються системи аналітичної розвідки і прогнозування подій, які застосовують сучасні методики глибинного аналізу і прогнозування кримінальних подій на основі аналізу так званих «слабких сигналів» [1]. Сутність цієї методики заснована на припущенні, що організовані кримінальні угрупування під час планування злочинів або терактів всіляко приховують свої наміри і плани, тобто у відкритих джерелах відсутня інформація, яка безпосередньо свідчить про підготовку кримінального злочину або терористичного акту. Тому безпосередньо застосувати інформацію, отриману з відкритих джерел, методами OSINT для профілактики, виявлення і попередження таких протиправних дій, як правило, не має можливості. В таких випадках розвинені аналітичні платформи [2] здійснюють збір широкого кола фактів і даних, які можуть бути тим чи іншим чином опосередковано свідчити про злочин, що готується. В якості прикладів такого типу даних, які використовуються для прогнозування злочинності ОЗУ, можна навести показник частки зайнятих повний робочий день в загальній чисельності осіб в працездатному віці або спалахи сонячної активності [1]. При цьому треба усвідомлювати, що «слабкий сигнал» вказує на вірогідність, а не на обов'язковість того, що та чи інша подія здійсниться. В останні роки у правоохоронній практиці розвинених країн використовується метод визначення «слабких

сигналів» на основі алгоритму розпізнавання образів. Метод спирається на глибоко розроблені алгоритми розпізнавання образів, в якості яких виступають не тільки графічні образи, а й певні характеристики числових рядів, а також рядів нечислової статистики. В даному контексті цей метод полягає в наступному. Задається деяка подія. Протягом наперед заданого тимчасового періоду, що передує події, програмно-апаратним чином виділяються будь-які стійкі патерни, послідовності, кореляції, пов'язані з цією подією. Далі знайдені патерни і кореляції перевіряються не на навчальній вибірці, а на реальній статистичній сукупності.

Як вважають експерти-аналітики такі методи дозволяють ефективно виявляти фінансові злочини, підготовку терористичних актів, приготування до розгортання військових дій і збройних пограбувань банків і ювелірних магазинів. І практика застосування подібних систем (Palantir (США), ePOOLICE (Європол)) підтверджує це [2].

Доцільність використання подібних технологій і методик глибинної аналітики і практичного досвіду їх застосування є особливо актуальною в умовах розгортання бойових дій в України. Оскільки великі військові операції, спеціальні операції, їх планування і підготовка до реалізації відносяться до типу подій, про які на ранніх етапах відсутня безпосередня інформація у відкритих або доступних суб'єкту аналітичної розвідки джерелах.

Список використаних джерел

1. Інформаційні технології у правоохоронній діяльності. Частина 1: Високотехнологічні тренди у правоохоронній сфері зарубіжних країн: навч. посіб. [В.М. Струков, Д.Ю. Узлов, Ю.В. Гнусов та ін.] ; за заг. ред. канд. техн. наук, доц. В.М. Струкова / Харків. нац. ун-т внутр. справ. Х. : ТОВ «ДІСА ПЛЮС», 2020. 276 с.

2. Струков В.М., Узлов Д.Ю., Гнусов Ю.В. Інструментальні інтелектуальні платформи для кримінального аналізу. *Право і безпека*. Вип. 4(83). 2021. с. 64-79.

3. Uzlov D., Strukov V., Vlasov O. Using Data Mining for Intelligence-Led Policing and Crime Analysis. – IEEE 2018 International Scientific-Practical Conference Problems of Infocommunications. Science and Technology (PIC S&T), - pp. 499-502.

4. Узлов Д.Ю., Струков В.М., Власов О.В. Методологічний апарат аналітичної роботи в Національній поліції України // Застосування інформаційних технологій в діяльності НПУ: матеріали наук.-практ. семінару(21 грудня 2018 р., Харків) МВС України, Харків. нац. ун-т внутр. справ: ХНУВС, 2017. С.64-66.

Одержано 16.04.2022

UDC 004.49

WEILING Cao,
Intermediate Grade of Experimenter, Teacher of Department of IT Information Centre Neijiang Normal University Neijiang (China);
SEMENOV Serhii,
Doctor of Science, Professor, Professor of the Department of Cybersecurity and Information Technology, Kharkiv National Economic University

AUTOMATED PENETRATION TESTING METHOD USING DEEP MACHINE LEARNING TECHNOLOGY

Using computer systems in almost all in all areas in social life and the increase in the number of information security incidents have updated the problem of data and software protection. One of the ways to improve cybersecurity is through the use of penetration testing methods and tools. This applies both to the areas of real production and practical services, and to the area of software development [1].

Until recently, penetration testing was done manually. At the same time, first of all, based on their own experience and erudition, the testers needed to analyze the computer system to detect

vulnerabilities. Only then can you enter the system and compromise the software. This is a rather laborious task, on the one hand, it requires a large amount of tester knowledge, and on the other hand, it has many risks of a subjective nature. Therefore, more and more organizations have recently been using penetration attack planner options based on automated targeting system models. So, for example, the company Core Security using this idea since 2010 in its tool Core IMPACT uses the attack planner MetricFF [2]. In addition, Core Security began the practice of implementing certain ethical cyberattacks in accordance with the known exploits of software vulnerabilities [3]. However, no uniform solution has been obtained for penetration testing procedures.

The aim of the work is an automated penetration testing method using deep machine learning technology. For this, it is necessary to solve a number of particular scientific problems:

1Explore the factual data collection capabilities of the Shadov system for the design of attack trees, as well as the Mulval platform for generating attack trees.

Develop a method for forming a matrix of cyber intrusions using the Mulval tool.

Improve the Deep Q - Lerning Network method for analyzing cyber intrusion matrices and finding the optimal attack trajectory.

Conduct a comparative study of the automated penetration testing method.

The general structure of the method can be represented as a set of methods and tools in Fig. 1.

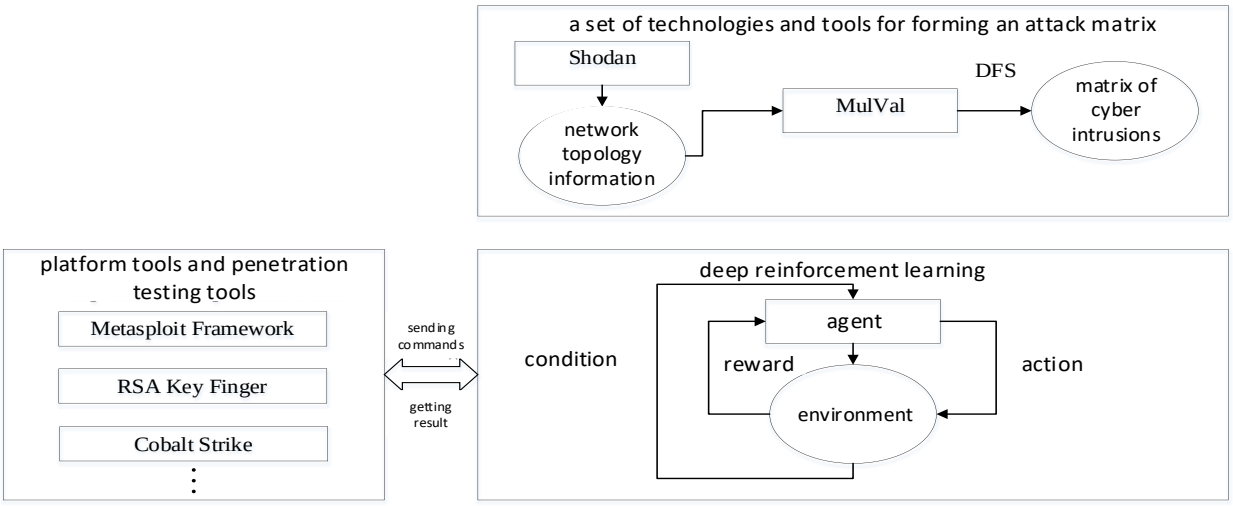

Fig. 1 General structure of the automated penetration testing method

As shown in Figure 1, the structure of the method implies the presence of three components: a set of technologies and means of forming an attack matrix; deep reinforcement learning for processing attack matrix data; tools, platforms and penetration testing tools.

Literature

1. Semenov, S. ., Liqiang, Z., Weiling, C., & Davydov, V. (2021). Development a mathematical model for the software security testing first stage. Eastern-European Journal of Enterprise Technologies, 3(2 (111), 24–34. https://doi.org/10.15587/1729-4061.2021.233417.

2. Hoffmann J. The Metric-FF Planning System: Translating ”Ignoring Delete Lists” to Numeric State Variables. *Journal of Artificial Intelligence Research*, 2011. Vol. 20, pp. 291–341.

3. Obes J. L., Sarraute C., Richarte G. G. Attack planning in the real world. arXiv: Cryptography and Security, 2013.

Одержано 14.04.2022

UDC 343.21

ZAVORINA Mariia Artemivna,
Student of Computer Science Faculty, Artificial Intelligence Specialism of Kharkiv National University of Radio Electronics

METHODS OF DEALING WITH THE CRIME OF CARDING

Nowadays IT-technology and internet sphere is developing more and more and besides the positive aspects of it there are some negative. The internet frauds are spreading all over the world and cybercrimes are the major problems. They touch different parts of our life, but, obviously, the financial side is being the most damaged.

Carding is one of the most popular cybercrime. The term “carding” means fraudulent transactions with credit cards (credit card details) that are not approved by the cardholder. This may be the theft or illegal receipt of a credit card, copying card details for further falsification, copying card details for making purchases over the Internet without the participation of the cardholder.

In any case, the main goal of criminals is to gain access to other people’s money. To achieve this goal, attackers come up with different ways to obtain the necessary information. The required data is PIN-code, CV code, expire date and number of the card, also name and surname of the owner.

But how to protect yourself from the carding? There are several ways to do it.

Keep your credit card PIN, passwords, login data for Internet banking in a safe place, best of all - in your own memory.

Minimize cases of using a bank card in suspicious places; if possible, use a bank card in well-visible premises.

Type your PIN quickly, with learned movements and, preferably, using several fingers at once - this will make it more difficult for intruders to recognize your movements. If possible, cover the hand typing PIN with the other hand, purse or some other object.

If the bank of your bank card has in it’s the service of quickly notifying the cardholder about the facts of debiting (SMS notifications), connect it for the fastest response to illegal debits.

Use bank cards with an embedded microchip

Be very careful when making an online purchase. Use only official and trusted sites.

Use ATMs located in bank branches or in places with video surveillance.

Do not use unlicensed software or download it for free from suspicious sites.

In conclusion, there is no panacea against carding crimes. The topic of carding still remains in the discussion field and is really relevant. However, the issues raised are not final and require additional and separate research or scientific study.

Одержано 01.05.2022

Наукове видання

ПРОТИДІЯ КІБЕРЗЛОЧИННОСТІ ТА ТОРГІВЛІ ЛЮДЬМИ

Збірник матеріалів
Міжнародної науково-практичної конференції
(27 травня 2022 року, м. Харків)

Відповідальний за випуск: *О. В. Манжай*
Комп'ютерне верстання: *К. М. Салашна*

Формат 60х84 /8. Ум. друк. арк. 7,7. Обл.-вид. арк. 4,8.
Видавець і виготовлювач –
Харківський національний університет внутрішніх справ,
просп. Л. Ландау, 27, м. Харків, 61080.
Свідоцтво суб'єкта видавничої справи ДК № 3087 від 22.01.2008.