УДК 004.056.5:347.965.43(477)
DOI https://doi.org/10.32782/2524-0374/2023-10/94

КІБЕРБЕЗПЕКА ТА КІБЕРГІГІЄНА ЯК ЗАСОБИ ЗАПОБІГАННЯ ВТРУЧАННЯМ В ДІЯЛЬНІСТЬ ЗАХИСНИКА ЧИ ПРЕДСТАВНИКА ОСОБИ

CYBER SECURITY AND CYBER HYGIENE AS MEANS OF PREVENTING INTERFERENCE IN THE ACTIVITIES OF THE PROTECTOR OR REPRESENTATIVE OF A PERSON

Медведенко Н.В., к.ю.н.,
старший науковий співробітник відділу організації наукової роботи
Одеський державний університет внутрішніх справ

Медведенко С.В., доктор філософії, доцент,
декан факультету підготовки фахівців для підрозділів превентивної діяльності
Одеський державний університет внутрішніх справ

Дана стаття присвячена питанням, які виникають у сфері гарантування конституційних прав особи, серед яких право на правничу допомогу, що реалізується шляхом залученням захисника чи представника особи для вирішення тих чи інших справ, а також проблемам пов'язаним із втручанням в їх діяльність.

У роботі розглянуто та проаналізовано погляди законодавця та науковців на визначення поняття «втручання в діяльність» та запропоновано уніфікацію визначення «втручання в діяльність захисника чи представника особи».

З'ясовано сутність запобігання втручанню у діяльність захисника чи представника особи складовими якого є заходи щодо попередження, недопущення та припинення негативного впливу, забезпечення належного рівня захищеності під час здійснення ними представницької діяльності.

Відмічено, що питання безпеки особи, суспільства, запобігання злочинності, забезпечення правопорядку в державі, наразі невід'ємно пов'язані з забезпеченням інформаційної безпеки та її складової – кібербезпеки.

Встановлено, що навідміну від фахівців даної сфери, законодавець розглядає кібербезпеку з широкого погляду, охоплюючи і інші аспекти, пов'язані з захистом даних або пристроїв, підключених до мережі, від несанкціонованого доступу та використання у злочинних цілях.

Розглянуто особливості комплексного підходу до забезпечення захисту та запобігання загрозам, з урахуванням побудови ІТ-інфраструктури. Приділено увагу можливостям інформаційних технологій, тим способам та засобам, використання яких надає можливість доступу до данних, та устаткування особи, а отже для втручанням у діяльність захисника чи представника особи. Запропоновано ряд рекомендацій для мінімізації можливості доступу до даних або пристроїв та відповідно втручанню в діяльність.

Авторами зроблено ряд висновків, зокрема про те, що запобігання злочинності є прерогативою не лише правоохоронних органів, а й суспільства загалом та окремих осіб, кожен в силу своїх можливостей може сприяти його забезпеченню, зокрема дотримуючись рекомендацій кібергігієни та ключових правил кібербезпеки.

Ключові слова: правнича допомога, представник, захист прав та інтересів особи, адвокат, запобігання, кібербезпека, кібергігієна, втручання у діяльність захисника чи представника особи.

This article is devoted to the issues arising in the field of guaranteeing constitutional rights of an individual, including the right to legal aid, which is realized by engaging a defense counsel or a representative of an individual to resolve certain cases, as well as to the problems associated with interference with their activities.

The work considered and analyzed the views of the legislator and scientists on the definition of the concept of «interference in the activity» and proposed the unification of the definition of «interference in the activity of the defender or representative of a person».

The essence of prevention of interference with the activities of a defense counsel or a representative of a person, which includes measures to prevent, prevent and terminate negative influence, and to ensure an adequate level of security during their representation activities is clarified.

It was noted that the issues of personal and social security, crime prevention, ensuring law and order in the state are currently inextricably linked to ensuring information security and its component - cyber security.

It was established that, unlike specialists in this field, the legislator considers cyber security from a broad perspective, covering other aspects related to the protection of data or devices connected to the network from unauthorized access and use for criminal purposes.

Features of a comprehensive approach to protection and prevention of threats, taking into account the construction of IT infrastructure, are considered. Attention is paid to the possibilities of information technologies, those methods and means, the use of which provides the possibility of access to data, and the equipment of the person, and therefore to interference in the activities of the defender or representative of the person. A number of recommendations are offered to minimize the possibility of accessing data or devices and, accordingly, interfering with activities.

The authors made a number of conclusions, in particular that the prevention of crime is the prerogative not only of law enforcement agencies, but also of society in general and individuals, everyone can contribute to its provision by virtue of their capabilities, in particular by following the recommendations of cyber hygiene and key rules of cyber security.

Key words: legal aid, representative, protection of the rights and interests of a person, lawyer, prevention, cyber security, cyber hygiene, interference in the activity of a person's defender or representative.

Конституція України гарантує невідчужуваність та непорушність прав і свобод людини і громадянина, забезпечення яких є головним обов'язком держави [1]. Право на професійну правничу допомогу є одним з ключових, адже його реалізація забезпечує особі можливість максимального захисту її інтересів у будь яких сферах та ситуаціях. Особа вільна у виборі захисника чи представника її інтересів, в певних випадках держава надає правничу допомогу безоплатно.

Враховуючи основоположність права на захист, втручання у діяльність захисника чи представника особи є категорично недопустимим, адже в результаті, посягає на реалізацію конституційних прав особи, тому законодавством встановлено юридичну відповідальність за такі дії. Так, Кримінальний кодекс України містить ряд положень, які покликані гарантувати захисникам чи представникам особи безпеку, свободу та незалежність їх діяльності щодо надання правничої допомоги, і відповідно реалізацію права на правничу допомогу і захист особі, яка їх потребує.

Ця проблематика становила науковий інтерес багатьох вчених серед яких А.М. Бабенко, В.В. Голіна, С.Ф. Денисов,

М.В. Джафарова, О.М. Джужа, А.Ф. Зелінський, С.Г. Керимов, А.В. Кирилюк, Є.В. Марич, Ю.В. Нікітін, Г.О. Світлична, Є.Л. Стрельцов, Л.І. Шаповал та інші.

Метою даної статті є встановлення шляхів, засобів та способів запобігання втручанню у діяльність захисника чи представника особи за допомогою сучасних інформаційних технологій та дотримання правил кібергігієни.

Втручання в діяльність захисника чи представника особи, погроза або насильство щодо них, умисне знищення або пошкодження їх майна, посягання на життя захисника чи представника особи у зв'язку з їх професійною діяльністю можуть негативно впливати на ефективність правової допомоги, що надається, та забезпечення прав особи, яка за нею звернулася, а також мати й більш довгострокові негативні наслідки, як для конкретного захисника чи представника особи, так і загалом для правозахисної сфери. Саме тому в законодавстві України закріплено кримінальну відповідальність за такі дії і визначено доволі суворе покарання.

Щодо поняття «втручання в діяльність захисника чи представника особи», то законодавець в статті 397 Кримінального кодексу України пропонує такими діями вважати вчинення в будь-якій формі перешкод до здійснення правомірної діяльності захисника чи представника особи по наданню правової допомоги, або порушення встановлених законом гарантій їх діяльності та професійної таємниці [2].

Якщо розглядати саме термін «втручання в діяльність» тих чи інших суб'єктів, то він має кілька визначень у законодавстві.

Так, втручання в діяльність судових органів розглядається як втручання в будь-якій формі в діяльність судді з метою перешкодити виконанню ним службових обов'язків або добитися винесення неправосудного рішення, тобто втручання направлене і на спонукання особи до порушення закону (ст. 376 КК України) [2].

Втручання в діяльність працівника правоохоронного органу, судового експерта, працівника державної виконавчої служби, приватного виконавця визначено як вплив у будь-якій формі на на таку особу, а також на її близького родича з метою перешкодити виконанню нею службових обов'язків, здійсненню судово-експертної діяльності, або з метою добитися прийняття незаконного рішення (ст. 343 КК України) [2].

Втручання у діяльність державного діяча встановлено як незаконний вплив у будь-якій формі на відповідну особу з метою перешкодити виконанню ними службових обов'язків або добитися прийняття незаконних рішень (ст. 344 КК України) [2].

Вказані визначення мають спільну рису – метою втручання є перешкодження виконання службових обов'язків, або спонукання до порушення закону шляхом прийняття незаконних рішень. Тоді як поняття «втручання в діяльність захисника чи представника особи» відрізняється і, на нашу думку, його можна було б уніфікувати, додавши фразу «або добитися вчинення незаконних дій».

Провідне місце серед суб'єктів, які забезпечують надання правничої допомоги та представництво інтересів особи в суді та інших органах займає адвокатура. Адвокатською діяльністю, відповідно до ст. 1 закону України «Про адвокатуру та адвокатську діяльність» є незалежна професійна діяльність адвоката щодо здійснення захисту, представництва та надання інших видів правничої допомоги клієнту.

Гарантії адвокатської діяльності закріплені в законі України «Про адвокатуру та адвокатську діяльність», професійні права, честь і гідність адвоката гарантуються та охороняються Конституцією України та іншими нормативно-правовими дукументами, наприклад Кримінальним кодексом України. Серед гарантій:

– заборона на будь-які втручання і перешкоди здійсненню адвокатської діяльності;

– заборона вимагати від адвоката, його помічника, стажиста, особи, яка перебуває у трудових відносинах з адвокатом, адвокатським бюро, адвокатським об'єднанням, а також від особи, стосовно якої припинено або зупинено право на заняття адвокатською діяльністю, надання відомостей, що є адвокатською таємницею;

– життя, здоров'я, честь і гідність адвоката та членів його сім'ї, їх майно перебуває під охороною держави;

– адвокату гарантується право на забезпечення безпеки під час участі у кримінальному судочинстві;

– заборона на втручання у приватне спілкування адвоката з клієнтом; забороняється втручання у правову позицію адвоката.

Втручання в діяльність захисника чи представника особи будь-яким чином є прямим порушенням принципів здійснення адвокатської діяльності, якими є верховенство права, законність, незалежність, конфіденційність та уникнення конфлікту інтересів [3]. Хоча, як вірно відмітив Марич Є.В., «адвокатура і займає одне з провідних місць серед суб'єктів надання правничої допомоги та є важливою частиною системи практичної реалізації конституційних гарантій, однак правнича допомога при вирішенні справ в адміністративному суді не може зводитися лише до адвокатської діяльності [4].

Це твердження також стосується як надання правничої допомоги в інших сферах судочинства, так і представницької діяльності законних представників особи (батьків, усиновителів, опікунів, піклувальників); представників юридичних осіб (керівника, юриста, призначеного працівника) та тої, яку здійснюють за договором: адвокати, юрисконсульти, співробітники юридичних фірм.

Відповідно до положень Цивільного процесуального кодексу України сторона, третя особа, а також особа, якій законом надано право звертатися до суду в інтересах іншої особи, може брати участь у судовому процесі особисто та (або) через представника. Навіть в разі особистої участі право мати представника зберігається. Як учасника судового процесу юридичну особу представляє її керівник, член виконавчого органу, іншу особа, уповноважену діяти від її імені відповідно до закону, статуту, положення, трудового договору (контракту). Представником у суді може бути адвокат або законний представник [5].

Отже, розглядаючи діяльність захисника чи представника особи, можливо відмітити, що ними є доволі широка категорія осіб, які за своїми законними, службовими повноваженнями чи повноваженнями на підставі договору виконують функції представництва чи надання правничої допомоги в судовому процесі, або інших сферах діяльності.

Термін запобігання надзвичайно часто використовується в нормативно-правовій базі, особливо щодо питань забезпечення правопорядку та безпеки, але законодавчого закріплення саме в розрізі цих питань він так і не отримав.

Так законодавець пропонує кілька визначень з використанням слова «запобігання»:

– *запобігання* – зменшення кількості та шкідливості для довкілля: матеріалів та речовин, що містяться в пакованні та відходах паковання... [6];

– *запобігання небезпеці* – всі вимоги або заходи, які передбачаються або проводяться на підприємстві для уникнення або обмеження небезпек, обумовлених професійною діяльністю [7];

– *запобігання комп'ютерним атакам* – комплекс організаційно-технічних заходів, спрямованих на забезпечення належного рівня захищеності від комп'ютерних атак [8].

В свою чергу, наукова думка також пропонує кілька варіантів роз'яснення цього поняття. Значення слова

«запобігати», за версією академічного тлумачного словника української мови, означає – не допускати, заздалегідь відвертати що-небудь неприємне, небажане [9].

Найчастіше науковцями юристами запобігання розглядається саме з погляду запобігання злочинності.

Деякі науковці ототожнюють поняття запобігання з поняттям профілактики, недопущення та попередження. Інші вкладають окремий зміст у кожне з цих понять. Наприклад, А. Ф. Зелінський визначав, що метою «профілактики» є загальне запобігання криміногенним ситуаціям, їх усунення, ослаблення дії криміногенних факторів, захисту об'єктів від посягань. А «запобігання» злочинам має конкретику – воно спрямоване на перешкоджання здійсненню злочинного наміру конкретної особи до початку посягання на стадіях виявлення наміру або готування до злочину. Тоді як «припинення» направлене на злочинну діяльність, що вже розпочалася, та має за мету забезпечити ненастання її шкідливих наслідків [10, с. 141–142].

Ряд правознавців підтримують його думку відмічаючи, що «запобігання злочинів зводиться до припинення злочинної діяльності на початковому етапі, коли злочинець тільки замишляє, планує вчинення певного діяння (тобто на стадії, коли його діяльність ще не є кримінально караною)». А запобігання злочинності є системою, що об'єднує об'єкти профілактики, основні рівні й форми профілактики, заходи попереджувального впливу, суб'єктів профілактики, які виконують цю роботу [11, с. 49].

В свою чергу, Джужа О.М., Кирилюк А.В. виділяють додаткові аспекти визначаючи «запобігання злочинам» як «специфічний напрям спеціально-кримінологічної профілактики, що складається із сукупності заходів, спрямованих на окремі групи та конкретних осіб, які виношують злочинні наміри, замислюють вчинення злочинів і позитивно сприймають злочинний спосіб життя, з метою дискредитування злочинної поведінки, відмови від злочинної мотивації та наміру або продовження злочинної діяльності» [12, с. 195–196]. Запобігання злочинам, на їх думку, здійснюється в проміжок часу між моментом формування злочинного мотиву і початком вчинення злочину.

Заслуговує на підтримку позиція Голіни В.В., який розглядає запобігання злочинності більш широко – на його думку нею є «сукупність різноманітних видів діяльності і заходів у державі, спрямованих на вдосконалення суспільних відносин з метою усунення негативних явищ та процесів, що породжують злочинність або сприяють їй, а також недопущення вчинення злочинів на різних стадіях злочинної поведінки» [13, с. 53].

Підтримуючи широкий погляд на запобігання злочинності, з урахуванням того, що вона поширюється і на інші сфери життєдіяльності суспільства, Б.М. Грек, та Ю.В. Нікітін розглядають її як особливий вид соціального управління покликаний забезпечити безпеку правоохоронюваних цінностей, який полягає в розробці та здійсненні спеціальних заходів щодо виявлення та усунення детермінант злочинності, а також здійсненні запобіжного впливу на осіб, схильних до протиправної поведінки [14, с. 148].

Відтак, запобігання втручанню у діяльність захисника чи представника особи можливо визначити як сукупність заходів щодо попередження, недопущення та припинення негативного впливу, забезпечення належного рівня захищеності під час здійснення ними представницької діяльності.

В сучасному світі питання безпеки особи, суспільства, запобігання злочинності, забезпечення правопорядку в державі невід'ємно пов'язані з забезпеченням кібербезпеки, інформаційної безпеки. Стрімкий розвиток технологій, що супроводжує людську діяльність, сприяв появі нових можливостей та інструментів для її здійснення, призвів до появи нових видів діяльності, одночасно з'явились і нові способи та знаряддя для протиправних дій, втручання в роботу чи чинення перешкод.

Законодавство України містить визначення кібербезпеки в «широкому» значенні, а саме кібербезпекою є «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» [15].

Відповідно до положень Регламенту Європейського Парламенту і Ради (ЄС) № 2019/881 від 17 квітня 2019 «кібербезпека» означає діяльність, необхідну для захисту мережевих та інформаційних систем, користувачів таких систем та інших осіб, які зазнають впливу кіберзагроз [16].

Але фахівці ІТ індустрії, як правило, розглядають поняття кібербезпеки з «вузького» спеціалізованого погляду, визначаючи її як заходи, які вживають для захисту даних або пристроїв, підключених до мережі, від несанкціонованого доступу та використання у злочинних цілях. Кібербезпека спрямована на захист комп'ютерних та серверних систем, програм користувачів та даних, які вони в них зберігають [17].

Існує і більш лаконічне визначення кібербезпеки як безпеки ІТ систем (обладнання та програм). При цьому кібербезпека виступає складовою інформаційної безпеки, яка є безпекою інформації установи, організації чи компанії, у тому числі в ІТ системах [18].

Спеціалісти IBM визначають, що кібербезпекою є будь-яка технологія, захід або практика для запобігання кібератакам або пом'якшення їхніх наслідків «*Cybersecurity refers to any technology, measure or practice for preventing cyberattacks or mitigating their impact*». Вона спрямована на захист систем, додатків, комп'ютерних пристроїв, конфіденційних даних і фінансових активів приватних осіб і організацій [19].

Захист та запобігання загрозам мають комплексний характер та поширюються на всі рівні ІТ-інфраструктури:

– безпека критичної інфраструктури, що захищає комп'ютерні системи, програми, мережі, дані та цифрові активи, від яких залежить національна безпека суспільства, економіка та громадська безпека;

– безпека мережі, яка полягає в запобіганню несанкціонованому доступу до мережевих ресурсів, а також виявленню та зупинці кібератак та поточних порушень безпеки мережі, водночас гарантуючи, що авторизовані користувачі мають за потребою безпечний доступ до необхідних мережевих ресурсів;

– безпека кінцевих точок захищає ці пристрої (сервери, настільні комп'ютери, ноутбуки, мобільні пристрої) та їх користувачів від атак, а також захищає мережу від зловмисників, які використовують кінцеві точки для здійснення атак;

– безпека програм захищає програми, що працюють локально та в хмарі, запобігаючи несанкціонованому доступу та використанню програм і пов'язаних даних;

– хмарна безпека захищає хмарні послуги та активи організації – програми, дані, сховище, інструменти розробки, віртуальні сервери та хмарну інфраструктуру;

– інформаційна безпека (InfoSec) забезпечує захист всієї важливої інформації організації, як цифрових файлів і даних, так і паперових документів, фізичних носіїв інформації, від несанкціонованого доступу, розголошення, використання чи зміни. Безпека даних, захист цифрової інформації, є складовими інформаційної безпеки та пов'язані із кібербезпекою;

– мобільна безпека охоплює технології, які є специфічними для смартфонів і мобільних пристроїв, а також пов'язана з рішеннями уніфікованого керування кінцевими

точками, які дозволяють керувати конфігурацією та безпекою для всіх кінцевих точок (не тільки смартфонів, а й планшетів, ноутбуків тощо) з єдиної консолі.

Існує багато способів і засобів для втручанням у діяльність будь-якої фізичної чи юридичної особи, зокрема й в діяльність захисника чи представника особи серед яких є використання можливостей інформаційних технологій. Серед актуальних та популярних можна виділити наступні:

– Raspberry Pi – це одноплатний комп'ютер, який використовується для запуску різних операційних систем, для їх злому та, як правило, після цього знищується щоб не залищати інформації та слідів;

– *Flipper Zero* – багатофункціональний інструмент, який є набором датчиків, чіпів і антен та найчастіше використовується для клонування ключів, але може використовуватися для зламу різних пристроїв та зчитування карток;

– *HakCat WiFi Nugget* є інструментом із відкритим кодом. Цей пристрій має крихітний OLED-екран, декілька кнопок і мордочку котика і допомагає отримати доступ до Wi-Fi;

– *Wi-Fi адаптер Alfa* має хорошу підтримку з системою Linux, може підтримувати зовнішню антену та покривати велику площу, використовується для злому паролів;

– *USB Rubber ducky* – це HID (накопичувач), який використовують для введення команд, він може мати попередньо підготовлену інформацію для автоматизації завдання, швидко запускати сценарії та зберігати необхідну інформацію на SD-карті;

– *LAN Turtle* – зовнішній пристрій, який має багато варіантів використання*:* як інструмент адміністратора мережі, для віддаленого перехоплення мережевих пакетів, для налаштування в якості зовнішнього мережевого адаптера між кабелем Ethernet і USB-портом системи, для Recon і PenTesting, для атак SSH, MITM;

– *Proxmark III* – пристрій, який дозволяє визначати, зчитувати та клонувати мітки RFID (радіочастотна ідентифікація) найчастіше використовується для дублювання ключкарток, а отже отримання доступу;

– *Keylogger* – программа або зовнішній пристрій USB, який можна використовувати для зчитування натискання клавіш клавіатури, фіксації руху комп'ютерної миші, створення скриншотів екрану тощо, для зберігання облікових даних, може працювати як точка доступу Wi-Fi, підключається з будь-якого комп'ютера, смартфона чи планшета;

– *HackRF One* – це платформа радіо з відкритим кодом, яку можна використовувати як радіопередавач/приймач, а також для захоплення/перехоплення радіосигналу, для злому автомобілів, супутникового зв'язку, прослуховування зв'язку Wakil Taki (рації), атаки на GPRS [20, 21].

Зазначене є лише невеликою частиною серед пристроїв, програмного забезпечення, призначених для зламу, доступу до приміщень, зв'язку чи інформації і демонструє, що кожен може бути вразливим і доступним для вторгнення, витоку та збору інформації. Держава захищає своїх громадян та систему державних і не державних органів, установ, організацій визначивши кримінальну відповідальність за створення з метою протиправного використання, розповсюдження або збуту шкідливих програмних чи технічних засобів, а також їх розповсюдження або збут (Стаття 361-1 КК України); незаконне втручання в роботу автоматизованих систем в органах та установах системи правосуддя (Стаття 376-1 КК України). Окрім того забезпеченням кібербезпеки займаються спеціалізовані підрозділи такі як Державна служба спеціального зв'язку та захисту інформації України, яка є органом, призначеним серед іншого і для формування та реалізації державної політики у сферах криптографічного та технічного захисту інформації, кіберзахисту, поштового зв'язку спеціального призначення, урядового фельд'єгерського зв'язку, активної протидії агресії у кіберпросторі [22]. Департамент кіберполіції Національної поліції України, Ситуаційний центр забезпечення кібербезпеки Служби безпеки України. Але, в першу чергу, кожен особисто повинен дотримуватися правил кібербезпеки та кібергігієни.

Діяльність з кіберзахисту на практиці тісно пов'язано з кібергігієною, яку визначають як «уміння, навички користування інформаційними технологіями, спрямовані на здійснення заходів щодо своєчасного виявлення, запобігання і нейтралізації реальних і потенційних кіберзагроз» [23].

Ці навички та уміння необхідно набувати та розвивати, щоб не стати легкою здобиччю для злочинців, які полюють за інформацією, адже представник (захисник) особи може стати мішенню для кібератак, метою яких буде отримання інформації, або для чинення перешкод його діяльності чи впливу, з метою спонукати до незаконних дій, тому необхідно дотримуватися правил для забезпечення захисту інформації та своїх пристроїв від кібератак та шкідливих програм. Зокрема рекомендується:

– користуватися офіційним програмним забезпеченням, вчасно оновлювати бази антивірусних та системних програм;

– не переходити за підозрілими посиланнями, що надійшли на e-mail, у месенджерах, соціальних мережах додатках, навіть від знайомих відправників, бажано переконатися, що звернення саме від тієї особи, адже профілі також можуть бути зламаними;

– за необхідності слід приховувати IP-адресу, використовуючи, наприклад, VPN-сервіс, браузера Tor, або анонімний проксі-сервер, який виконує функції посередника між пристроєм та інтернет-мережею;

– встановлювати обмеження для під'єднання за допомогою Bluetooth, вимикати його коли немає потреби, встановити сповіщення про під'єднання нових пристроїв;

– встановлювати пароль на файли, архіви з документами, зберігати їх на захищених носіях, за потреби використання екрануючого чохла фарадея, який не пропускає електромагнітні імпульси та унеможливлює вплив на пристрої;

– бажано надавати перевагу користування месенджерами з End-to-end шифруванням (наскрізне, кінцеве шифрування) – коли повідомлення шифруються при відправленні та розшифровуються при отриманні також підвищить безпеку спілкування та обміну даними.

Для захисту від фішингу – виду інтернет-шахрайства з метою отримання конфіденційних даних та інформації користувачів, окрім зазначеного вище, пропонується не використовувати персональних даних у публічних та незахищених мережах, створювати для різних акаунтів відмінні паролі.

Коли мова йде про захист інформації на будь-яких носіях слід завжди пам'ятати про людський фактор: не можна залишати нотатки з паролями в доступі чи на видноті, необхідно регулярно змінювати паролі, встановлювати двофактурну аутентифікацію, відслідковувати доступ обслуговуючого персоналу до устаткування, матеріалів та паперів. Контролюючи доступ до інформації, слід мати на увазі, що новий співробітник, або співробітник який звільняється, в більшій мірі може стати потенційною можливістю для витоку інформації.

Для представників (захисників) особи, які професійно займаються правничою діяльністю також рекомендується регулярно використовувати послуги спеціалістів, для здійснення перевірки вразливості систем, наявність порушення безпеки, пошук слабких місць, тестування на проникнення. В арсеналі таких фахівців широкий інструментарій, серед яких:

– *Nmap* (мережевий картограф), який здійснює пошук та виявлення взазливостей, створюючи карту мережі;

– *Acunetix* – автоматизований інструмент, для блокування ворожих зловмисників від несанкціонованого доступу, який може сканувати JavaScript, HTML5 і односторінкові програми як сканер безпеки та захистити веб-програми;

– *Burp Suite* є надійним проксі-інструментом для оцінки безпеки веб-сайту, здатним перехоплювати запити та відповіді між браузером користувача та цільовим веб-сайтом, а також забезпечує видимість функціональності веб-сайту;

– *Nikto* – безкоштовний веб-сканер із відкритим вихідним кодом, який перевіряє та тестує низку веб-серверів, щоб знайти застаріле програмне забезпечення, потенційно шкідливі CGI або файли та інші проблеми;

– *John the Ripper*, який є популярним зломщиком паролів, та одним із найкращих доступних інструментів для перевірки надійності паролів у ОС або для віддаленого аудиту, який здатний автоматично визначати тип шифрування та коригувати метод перевірки пароля.

Висновки. Вирішення справи та її результат завжди становить інтерес для її учасників та зацікавлених осіб, а отже може зазнавати впливу та втручання, зокрема через втручаня в діяльність захисника чи представника особи.

Впровадження новітніх досягнень в різні сфери нашого життя відкриває нові можливості, але це твердження є вірним і для злочинців також, тому потребує сучасних рішень, пересторог та комплексного підходу до забезпечення безпеки.

Запобігання злочинності є прерогативою не лише правоохоронних органів, а й суспільства загалом та кожної окремої особи, яка в силу своїх можливостей може сприяти його забезпеченню, зокрема дотримуючись кібергігієни та ключових правил кібербезпеки. Реалізація кожного кроку на цьому шляху потребує системності у державному управлінні, консолідації наукового потенціалу, громадської ініціативи, підтримки держави, залучення інвестицій, впровадження сучасних технологій та нових методів роботи, а також активної громадянської позиції кожного представника суспільства.

ЛІТЕРАТУРА

1. Конституція України : Закон України від 28 черв. 1996 р. № 254к/96-ВР. URL: http://zakon2.rada.gov.ua/laws/show/254%D0%BA/96-%D0%B2%D1%80/ (дата звернення: 15.10.2023).
2. Кримінальний кодекс України : Закон України від 05 квітн. 2001р. № 2341-III. URL: https://zakon.rada.gov.ua/laws/show/2341-14/conv#n2811 (дата звернення: 15.10.2023).
3. Про адвокатуру та адвокатську діяльність : Закон України від 05 лип. 2012 р. № 5076-VI. URL: https://zakon.rada.gov.ua/laws/show/5076-17#Text (дата звернення: 15.10.2023).
4. Марич Є.В. Характеристика суб'єктів надання правничої допомоги при вирішенні справ в адміністративному суді. *Юридичний науковий електронний журнал.* Запоріжжя. 2020. № 3. С. 497–501.
5. Цивільний процесуальний кодекс України : Закон України від 18 бер. 2004 р. № 1618-IV. URL: https://zakon.rada.gov.ua/laws/show/1618-15/conv#Text (дата звернення: 15.10.2023).
6. Про затвердження Технічного регламенту з підтвердження відповідності паковання (пакувальних матеріалів) та відходів паковання : Наказ Держспоживстандарт України від 24 груд. 2004 р. № 289. URL: https://zakon.rada.gov.ua/laws/show/z0095-05/ed20050205/find?text=%C7%E0%EF%EE%E1%B3%E3%E0%ED%ED%FF#Text (дата звернення: 15.10.2023).
7. Про затвердження Положення про порядок забезпечення працівників спеціальним одягом, спеціальним взуттям та іншими засобами індивідуального захисту (НПАОП 0.00-4.01-08) : Наказ, від 24 бер. 2008 р. № 53. URL: https://zakon.rada.gov.ua/laws/show/z0446-08/ed20091225/find?text=%C7%E0%EF%EE%E1%B3%E3%E0%ED%ED%FF+%ED%E5%E1%E5%E7%EF%E5%F6%B3#Text (дата звернення: 15.10.2023).
8. Угода про співробітництво і взаємодію між Адміністрацією Державної служби спеціального зв'язку та захисту інформації України і Службою інформації та безпеки Республіки Молдова : Угода, Міжнародний документ від 22 лют. 2017 р., 23 груд. 2016 р. URL: https://zakon.rada.gov.ua/laws/show/498_002-16/ed20161223#Text (дата звернення: 15.10.2023).
9. Словник української мови : в 11 т. / АН УРСР Інститут мовознавства. Київ : Наукова думка, 1970 – 1980. Т. 1 .799 с. URL: http://sum.in.ua/s/zapobighaty (дата звернення: 15.10.2023).
10. Зелінський А. Ф. Кримінологія : курс лекцій. Харків : Прапор. 1996. 260 с.
11. Титаренко О.О., Хорошун О.В. Стулов О.О. Кримінологія : конспект лекцій. Дніпро : ДДУВС, 2016. URL: https://dduvs.in.ua/wp-content/uploads/files/Structure/library/student/lectures/1125/11.1.pdf (дата звернення: 25.10.2023).
12. Кримінологія : підручник / О. М. Джужа та ін. ; за заг. ред. д-ра юрид. наук, проф. В. В. Чернєя ; за наук. ред. д-ра юрид. наук, проф. О. М. Джужі. Київ : НАВС, 2020. 612 с.
13. Кримінологія: Загальна та Особлива частини: підручник / І. М. Даньшин та ін.; за заг. ред. В. В. Голіни. 2-ге вид. перероб. і доп. Харків : Право, 2009. 288 с.
14. Кримінологія : підручник / А.М. Бабенко та ін. ; за заг. ред. Ю.В. Нікітіна, С.Ф. Денисова, Є.Л. Стрельцова. 2-ге вид., перероб. та допов. Харків : Право, 2018. 416 с.
15. Про основні засади забезпечення кібербезпеки України : Закон України від 05 жовт. 2017 р. № 2163-VIII. URL: https://zakon.rada.gov.ua/laws/show/2163-19/ed20220817#Text (дата звернення: 15.10.2023).
16. Регламент Європейського Парламенту і Ради (ЄС) 2019/881 від 17 квітня 2019 року про Агентство Європейського Союзу з питань мережевої та інформаційної безпеки (ENISA) та про сертифікацію кібербезпеки інформаційно-комунікаційних технологій, а також про скасування Регламенту (ЄС) № 526/2013 (Акт про кібербезпеку) : Регламент від 17 квіт. 2019 р. № 2019/881. URL: https://zakon.rada.gov.ua/laws/show/984_024-19/ed20190417#n136 (дата звернення: 15.10.2023).
17. Що таке кібербезпека? Заходи забезпечення кібербезпеки. *Dan-it.com.ua* : веб-сайт. URL: https://dan-it.com.ua/uk/blog/chto-takoe-kiberbezopasnost-mery-obespechenija-kiberbezopasnosti/ (дата звернення: 18.10.2023).
18. Юрій Гудзь. Кібербезпека чи Інформаційна безпека? *KO IT для бізнесу* : веб-сайт. URL: https://ko.com.ua/kiberbezpeka_chi_informacijna_bezpeka_120068#:~:text=%D0%9A%D1%96%D0%B1%D0%B5%D1%80%D0%B1%D0%B5%D0%B7%D0%BF%D0%B5%D0%BA%D0%B0%20%E2%80%93%20%D1%86%D0%B5%20%D0%B1%D0%B5%D0%B7%D0%BF%D0%B5%D0%BA%D0%B0%20%D0%86%D0%A2%20%D1%81%D0%B8%D1%81%D1%82%D0%B5%D0%BC,%D1%82%D0%BE%D0%BC%D1%83%20%D1%87%D0%B8%D1%81%D0%BB%D1%96%20%D0%B2%20%D0%86%D0%A2%20%D1%81%D0%B8%D1%81%D1%82%D0%B5%D0%BC%D0%B0%D1%85 (дата звернення: 18.10.2023).
19. What is cybersecurity? *IBM* : веб-сайт. URL: https://www.ibm.com/topics/cybersecurity (дата звернення: 18.10.2023).
20. Akash Ranjan Patel. Cyber Security. Hardware. Top 13 Hardware Hacking Tools Kit. *Akash Ranjan Patel* : веб-сайт. URL: https://akashranjanpatel.medium.com/cyber-security-hardware-top-13-hardware-hacking-tools-kit-fed172b9df20 (дата звернення: 18.10.2023).
21. Gadgets that break things: our favorite hacking hardware. *The verge*. : веб-сайт. URL: https://www.theverge.com/23379037/hacking-gadgets-cybersecurity-penetration-testing-hardware (дата звернення: 18.10.2023).
22. Про Державну службу спеціального зв'язку та захисту інформації України : Закон України від 23 лют. 2006 р. № 3475-IV. URL: https://zakon.rada.gov.ua/laws/show/3475-15#Text (дата звернення: 18.10.2023).
23. Про затвердження Положення про організаційно-технічну модель кіберзахисту : Постанова Кабінету Міністрів України від 29 груд. 2021 р. № 1426. URL: https://zakon.rada.gov.ua/laws/show/1426-2021-%D0%BF#Text (дата звернення: 22.10.2023).