https://doi.org/10.33919/ljnbu.24.2.1

СЪБИРАНЕ НА ЕЛЕКТРОННИ ДОКАЗАТЕЛСТВА ПРИ РАЗСЛЕДВАНЕ НА ПРЕСТЪПЕНИЯ, СВЪРЗАНИ С РАЗПРОСТРАНЕНИЕ НА СИНТЕТИЧНИ НАРКОТИЦИ

Веселин Вучков[1]
Даниел Делчев[2]

Резюме: В нашето съвремие електронните доказателства намират все по-широко приложение в разследването на престъпления. Динамичното развитие на съвременното общество и бума на технологиите, както и тяхното приложение във всеки един аспект от ежедневието ни, способстват това, все по-голям процент от извършваните противоправни деяния да оставят „електронна следа“ при извършването си. Изключение от това не прави и дейността по разпространението на синтетични наркотици. Настоящата публикация има за цел да разгледа основните аспекти на престъпленията, свързани с разпространението на синтетични наркотични вещества и особеностите, свързани с това, като същевременно представи възможностите за използване на електронните доказателства и даде примери за някои практики, които биха могли да бъдат активно прилагани с цел предотвратяване и намаляване на престъпленията в тази сфера.

Ключови думи: синтетични наркотици, електронни доказателства, разследване, престъпления, разпространение, нелегални пазари.

I. Увод

Производството и разпространението на наркотични вещества продължава да бъде проблем с глобални измерения, като в последно време се наблюдава значително повишаване на производството на синтетични наркотици. От друга страна, приложението на електронните доказателства в сферата на разследването се утвърждава все по-устойчиво. Събирането на електронни доказателства се превръща във важна част от дейността по разкриването на престъпления, включително на тези, свързани с разпространението на синтетични наркотични вещества. При събирането на електронни доказателства следва да бъдат спазвани

[1] Професор в департамент „Право“ на НБУ, в ЮЗУ – Благоевград и в Академия на Министерството на вътрешните работи; доктор; ел. поща: vvuchkov@nbu.bg

[2] Преподавател в катедра „Публично-правни науки“ на Академия на Министерството на вътрешните работи; доктор; ел. поща: DStDelchev@mvr.bg

с повишено внимание съществуващите правни норми и процедури, които закрепят нормативно валидността на тази правно-регламентирана дейност.

II. Изложение

В световен мащаб производството и разпространението на фентанил се е увеличило, а популярността му продължава да нараства. Агенцията за борба с наркотиците на САЩ определя фентанила като синтетичен опиоид, който обикновено се използва за лечение на пациенти с хронична болка или силна болка след оперативна намеса[3]. В Република България фентанилът попада в Списък II от Наредба за реда за класифициране на растенията и веществата като наркотични: „вещества с висока степен на риск, намиращи приложение в хуманната и ветеринарната медицина“.

Освен фентанила, сериозна заплаха за общественото здраве представляват и други синтетични наркотици, като синтетични канабиноиди и различни синтетични стимуланти. Един от основните рискове при синтетичните наркотици е обстоятелството, че те могат да притежават висока потентност. Потентността при наркотичните вещества представлява интензитета на ефекта, който се получава от употребата на доза от съответното вещество[4]. Колкото по-висока е потентността на наркотика, толкова по-силен е ефектът му върху човешкия организъм.

В рамките на Европейския съюз се осъществява активна законодателна политика с цел предотвратяване разпространението на наркотични вещества, в частност на синтетични наркотици. Регламентите, които имат отношение към контрола върху синтетичните наркотици, са на първо място Регламент 302/93, с който се създава Европейския център за мониторинг на наркотиците и наркоманиите (ЕЦМНН). С Регламент 1920/2006 се засилва ролята на ЕЦМНН в контрола върху новите психоактивни вещества, като тенденцията за повишаване ролята на Центъра продължава и с последващите Регламенти 2017/2101 и 2022/1924, с които се подготвя създаването на Агенция на Европейския съюз по наркотиците (АЕСН). АЕСН се създава и функционира въз основа на Регламент 2023/1326, който е и действащият към настоящия момент регламент, с предмет контрол върху синтетични психоактивни вещества. Регламентът усъвършенства правната регламентация, отнасяща се до новите синтетични наркотици, чието действие, макар и да наподобява това на традиционните наркотици, може да бъде много по-интензивно. Благодарение на Регламента се повишават възможностите на Европейския съюз да реагира бързо и пълноценно на нарастващата заплаха от разпространение на синтетични наркотици.

Въпреки активната законодателна политика, в ЕС продължава разпространението на синтетични наркотици, особено сред младите хора, голяма част от които не са запознати с вредния им ефект. В Наказателния кодекс на Република България са определени високи наказания за разпространението на наркотични вещества. Чл. 354а от Кодекса гласи: „Който без надлежно разрешително произведе, преработи, придобие или държи наркотични вещества или техни аналози с цел разпространение, или разпространява наркотични вещества или техни аналози, се наказва за високорискови наркотични вещества или техни аналози – с лишаване от свобода от две до осем години и с глоба от пет хиляди до двадесет хиляди лева, а за рискови наркотични вещества или техни аналози – с лишаване от свобода от една

[3] *[online]*. Достъпно: https://www.dea.gov/resources/facts-about-fentanyl. [Посетено на: 20.09.2024].

[4] *[online]*. Достъпно: https://www.sciencedirect.com/topics/immunology-and-microbiology/drug-potency. [Посетено на: 20.09.2024].

до шест години и с глоба от две хиляди до десет хиляди лева. Когато предмет на престъплението са прекурсори или съоръжения, или материали за производство на наркотични вещества или техни аналози, наказанието е лишаване от свобода от три до дванадесет години и глоба от двадесет хиляди до сто хиляди лева“. Въпреки определените високи наказания, не само в България, но и в световен мащаб разпространението на синтетични наркотици нараства[5].

Ефективното противодействие на разпространението на синтетични наркотици следва да се осъществява не само чрез обособяване на ясни критерии, чрез които да се осъществява събирането на доказателства за извършването на такива деяния, но и посредством активна превантивна дейност. Последната е усложнена поради факта, че в различните социални мрежи и по медиите като цяло не рядко се осъществява индиректна реклама на различни наркотични вещества.

Действащата нормативна уредба ясно забранява всякаква форма на реклама на наркотични вещества. В Закона за контрол на наркотичните вещества и прекурсорите, и по-конкретно в чл. 7 е посочено: „Забранява се пряката и непряката реклама пред обществеността на наркотичните вещества и растенията от Списъците по чл. 3, ал. 2, т. 1, 2 и 3 и лекарствените продукти, съдържащи наркотични вещества“. В т. 30 от Допълнителните разпоредби на същия закон е дадено легално определение на понятието „непряка реклама“, която според законодателя следва да се разбира като „всяка форма на търговско послание, съобщение, препоръка или действие, която използва име и/или изображение, представляващо или наподобяващо наркотично вещество, за реклама върху стоки и рекламни продукти”. Така формулирано обаче понятието не посочва всички възможности, чрез които може да бъде реализирана непряка реклама. Частта от изречението: „всяка форма на търговско послание, съобщение, препоръка или действие, която използва име и/или изображение, представляващо или наподобяващо наркотично вещество...“ води до извода, че формата на търговското послание, съобщение, препоръка или действие следва задължително да използва име и/или изображение, представляващо или наподобяващо наркотично вещество, за да може деянието да бъде квалифицирано като „непряка реклама“ по смисъла на закона.

Тук обаче може да бъде повдигнат въпрос, свързан с действие, което наподобява използването на наркотично вещество, но самото действие не използва име и/или изображение. Като пример може да бъде посочено действието с пръст, който с движение минава под ноздрата и представлява обществено популярен жест, свързан с употребата на високорисковото наркотично вещество – кокаин. Могат да бъдат дадени и други примери за индиректна реклама на наркотични вещества чрез действия, които обаче не използват име и/или изображение, но за по-голямата част от обществото съдържанието на тези действия/жестове е очевидно. Това обаче не представлява предмет на настоящото изследване. Във всички случаи е необходимо текстът на т. 30 от Допълнителните разпоредби на Закона за контрол на наркотичните вещества и прекурсорите да бъде редактиран, като в него ясно залегне идеята, че непряка реклама на наркотични вещества може да бъде осъществявана по много и различни начини, като законодателят следва да отчете различните субкултури (особено сред младите хора) и характерните за тях жаргонни изрази и жестове.

Индиректните реклами, особено тези, в които участват популярни личности, способстват за повишаване на интереса на младите хора да опитат даден наркотик. Пазарите, където се осъществява активна търговия на синтетични наркотици, бързо се адаптират към промените в нормативната уредба и към цялостните опити на правоприлагащите органи да противодействат на тази дейност. Характерното за синтетичните наркотици е, че пазарите

[5] *[online]*. Достъпно: https://www.unodc.org/unodc/en/data-and-analysis/world-drug-report-2024.html. [Посетено на: 20.09.2024].

за разпространение могат да бъдат и напълно легални от гледна точка на правноорганизационната им форма. Такива са отделните аптеки, които са лицензирани да продават лекарства, съдържащи наркотични вещества, като например: диазепам, кодеин, оксикодон, метилфенидат, ксанакс и др.

Възможността за осъществяване на сделки с лекарствени продукти, съдържащи наркотични вещества, е нормативно закрепена в чл. 33, ал. 1 от Закона за контрол върху наркотичните вещества и прекурсорите (ЗКНВП) , съгласно който: „Търговия на дребно, съхраняване и отпускане на лекарствени продукти, съдържащи наркотични вещества от списъците по чл. 3, ал. 2, т. 2 и 3, се извършват с лицензия, издадена от министъра на здравеопазването или от оправомощен от него заместник-министър“, като освен този текст по отношение на процедурата за получаване на лицензия имат отношение текстовете на чл. 33а и 41, ал. 1 от ЗКНВП.

В чл. 70, ал. 1 от Наредба № 4 от 4 март 2009 г. за условията и реда за предписване и отпускане на лекарствени продукти, е нормативно закрепено предписването на лекарствени продукти с електронно предписание (включително и такива лекарства, които съдържат наркотични вещества), като в чл. 70, ал. 2 е посочена процедурата, която се осъществява по електронен път и посредством която се отпускат електронно предписани лекарствени продукти. Електронните предписания действително имат редица преимущества пред хартиените рецепти, като:

- Ограничаване възможностите за извършване на фалшификации на предписанието в сравнение с това на хартиен носител. Въпреки че тези възможности намаляват, те все пак не изчезват, поради което разследването на деяния, свързани с предписването на фалшиви предписания следва да става посредством събирането на доказателства както в обективната действителност, така и в дигитална среда. Общите мерки за осигуряване на сигурността на Националната здравно-информационна система (НЗИС), са изброени в чл. 36 от Наредба № Н-6 от 21 декември 2022 г. за функционирането на Националната здравно-информационна система, които включват ограничения на достъпа до нея, включително и по отношение на времетраенето на този достъп; осигуряване на подходящи софтуерни и хардуерни решения за безпрепятственото функциониране на системата; обезпечаване на високи нива на осигуреност на схемите за електронна идентификация; създаването и приложението на собствен стандарт за сигурност на НЗИС. В чл. 36, ал. 2 изрично е посочено, че достъп до базите данни е разрешен само на обслужващите ги модули. Въпреки приложението на всички тези мерки, все пак съществуват софтуерни възможности, посредством които да бъде осигурен нерегламентиран достъп до НЗИС, които ще бъдат разгледани по-долу;
- Осигуряване на достъп на самия лекар до цялостна информация за здравословното състояние на пациента посредством софтуерен интерфейс на системата за електронни рецепти. В чл. 3, ал. 1 от Наредбата за функциониране на НЗИС е посочено, че в системата се събира, обработва и съхранява информация за здравното състояние на населението чрез създаване и поддържане на електронен здравен запис, който е индивидуален за всеки гражданин;
- Осигуряване на цялостно проследяване на процеса на предписване на лекарство от страна на лекаря и изпълнението на електронното предписание от магистър-фармацевт в определена аптека;
- Намаляване на хартиения оборот и цялостно оптимизиране на дейността по издаване на рецепти от гледна точка на бързина на процедурата;
- Осигуряване на възможност за генериране на статистически данни, свързани със здравословното състояние на населението чрез анализ и обобщаване на информацията от централизираната система за издаване на електронни предписания.

Въпреки безспорните положителни характеристики на електронните предписания, все пак съществува възможност за тяхното фалшифициране. Това може да стане чрез неоторизиран достъп до системата, която управлява издаването на електронни рецепти. За Република България функционира Национална здравно-информационна система (НЗИС)[6]. Системата отговаря на високи стандарти за осигуряване на сигурност за достъп до нея и за защита на информацията, която се въвежда, обработва и съхранява, но това не може да ограничи в пълна степен възможностите да бъде осъществен нерегламентиран достъп до съдържанието ѝ и до нейния интерфейс с цел генериране на електронни рецепти.

При установяване на нерегламентиран достъп до НЗИС правоприлагащите органи от своя страна трябва в максимално кратки срокове да си осигурят достъп до компрометираната система и да я изолират, предотвратявайки всякакъв последващ достъп до нея от страна на извършителя на правонарушението. При спазване на изискването за бързина в действията на разследващите органи, в по-голяма степен се гарантира и предотвратяване последващото разпространяване на вредоносния софтуер. Необходимо е да бъдат събрани всички възможни електронни доказателства, като лог[7]-файлове и други файлове при фактически осъществена хакерска атака.

Електронните доказателства (ЕД) по своята същност представляват разновидност на невещественните доказателства[8]. ЕД могат да бъдат определени като „електронни данни, които са свързани с обстоятелствата по делото, допринасят за тяхното изясняване и са установени по реда на НПК“[9]. Във всички случаи електронните доказателства следва да са съобразени с общите изисквания за наказателно-процесуалното разбиране за „доказателство“, формулирано в чл. 104 от НПК[10].

Валидността на електронните доказателства в рамките на процесуалноправната дейност по доказване фалшифицирането на електронна рецепта е безспорна, но при условието, че лог-файловете (като типични доказателства за установяване на факта на фалшифициране на електронна рецепта) се анализират внимателно и при наличие на съответни професионални познания от страна на правоприлагащия орган, с цел да бъдат установени елементите на осъществения противоправен достъп до НЗИС. Лог-файловете биха могли да дадат ценна информация за дейности, осъществени от определен потребител, които се регистрират от съответния софтуер или от операционната система на компютъра.

Проблемът при лог-файловете е, че самите хакери при определени условия могат да ги изтрият или да променят тяхното съдържание, като по този начин предотвратят използването им като електронни доказателства[11]. Дали ще могат да ги изтрият, зависи от ниво-

---

[6] Националната здравно-информационна система е създадена в рамките на Договор за безвъзмездна финансова помощ (ДБФП) № BG05SFOP001-1.002-0007 от 21.03.2017 г., по проект „Доизграждане на националната здравна информационна система (НЗИС) – етап 1 и етап 2. вж. Национална здравно информационна система. Достъпно: https://his.bg/bg/about. [Посетено на: 23.09.2024].

[7] Лог-файлът представлява компютърен файл, който съдържа информация за действията, извършвани на съответния компютър, на чиято памет се съхранява – Английско-български речник на Кеймбридж. Достъпно: https://dictionary.cambridge.org/dictionary/english/log-file. [Посетено на: 23.09.2024].

[8] Вучков В. (2023). Електронните доказателства по наказателни дела и техните източници – необходими разсъждения. Юридическо списание на Нов български университет, бр. 2, 16.

[9] Маринова Г. (2002). Електронните доказателства. Списание Правна мисъл, бр. 3, 64-65.

[10] За доказателството в наказателния процес вж. Вучков В. (2023). Наказателен процес в схеми, таблици, определения. София: Сиби. 67 и 68 с.

[11] Изчистване на лог файлове (от англ. Log clearing) представляват техническите способи за премахване на лог файлове или други електронни доказателства от страна на дееца с цел да предотврати

то на достъп, което им е осигурено. При пълен root достъп[12] за хакера няма да представлява проблем да изтрие или промени съдържанието на лог-файловете, което неимоверно би затруднило разследващите органи. Най-добре би било лог-файловете да се съхраняват на сървър извън този, до който хакерът си е осигурил достъп. Тогава възможностите му да влияе върху лог-файловете рязко би намалял. Същото важи и за случаите, когато лог-файловете се съхраняват на облачна услуга[13] [14]. С цел по-пълноцелнно събиране на доказателства от лог-файлове, е наложително разследващите органи да бъдат снабдени със софтуерни инструменти, чрез които да анализират дали е имало зловредно влияние върху логовете.

Освен анализ на компютърния софтуер, чрез който е предписана фалшива рецепта за снабдяване със забранено лекарство, представляващо синтетичен наркотик, е необходимо да бъдат извършени и други процесуално-следствени действия за установяване на обективната истина. Такива са разпит на лекарите, които имат достъп до съответния компютър, като въпросите следва да бъдат ориентирани около това в какви часови интервали те са имали достъп. Чрез разпита могат да се съберат ценни данни, от които да бъде направен извод дали не е имало опит за нерегламентиран достъп до компютъра. В случай, че конкретен лекар е заподозрян като лице, което предписва фалшиви рецепти, е наложително и неговите колеги от други смени да бъдат внимателно разпитани. При разпитите разследващите органи трябва да се ръководят от законовото изискване за обективност, като задават внимателно преценени въпроси, съобразени с естеството на разследвания случай.

Допълнително е нужно извършването на оперативно-издирвателни мероприятия, за да се установи в кои помещения в болничното заведение има камери за видеонаблюдение, посредством които да се направи извод за осъществяване на достъп до конкретен компютър, с цел изготвяне на фалшива рецепта за набавяне на дадено лице със синтетичен наркотик. От особено значение е видеозаписите да са с висока разделителна способност, за да може ясно да бъдат идентифицирани лица, които биха представлявали интерес за разследващите органи.

Задължително е и извършването на внимателен оглед на помещението, където се намира компютъра и претърсване и изземване.

Нелегалното разпространение на синтетични наркотици може да се осъществява и чрез други форми, освен чрез използването на фалшиви рецепти. Особено популярни са пазарите на синтетични наркотици в т.нар. “Darknet”. Популярни в Darknet са следните синтетични наркотици:

събирането им като доказателства в полза на това, че същият е осъществил неправомерен достъп до даден компютър. вж. Gutpa. A., Anand A. (2017). Ethical hacking and hacking attacks. International Journal of Engineering and Computer Science. Volume 6, Issue 4.

[12] На англ. Root access – това представлява най-високото ниво на достъп, което може да бъде осигурено спрямо компютър. Root достъпът дава пълен достъп до цялостната функционалност на съответния инсталиран софтуер. Достъпно: https://nordvpn.com/cybersecurity/glossary/root-access/. [Посетено на: 24.09.2024].

[13] На англ. Cloud service – облачната услуга като термин може да бъде използван, когато се говори за за т. нар. облачни изчисления (cloud computing) или облачни хранилища на данни (cloud storage). Чрез облачните услуги най-общо се предоставят за безвъзмездно или възмездно ползване компютърни ресурси – вж. Достъпно: https://hicomm.bg/hi-tech/kakvo-predstavljavat-ay-oblachnite-uslugi-au.html. [Посетено на: 24.09.2024].

[14] Log-файлове могат да бъдат съхранявани в облачни хранилища на данни, например вж. Достъпно: https://cloud.google.com/storage/docs/access-logs. [Посетено на: 24.09.2024].

♦ Синтетичните канабиноиди. Това са лабораторно синтезирани химикали, чието действие върху човешката психика наподобява това на тетрахидроканабинола (ТХК). Синтетичните канабиноиди могат да бъдат много опасни – те причиняват халюцинации, повишаване на сърдечния пулс, позиви за повръщане и др.

♦ Синтетични катинони, които също биват наричани от продавачите „соли за вана". Те имат силно еуфоричен ефект, но същевременно употребяващият може да изпита параноя и халюцинации.

♦ Фентанил – има потентност, която надвишава тази на хероина и е особено популярен в Darknet, а фентаниловите аналози дори надвишават потентността на фентанила.

♦ Бензодиазепини – поначало са позволени от закона, като в Република България голяма част от тях попадат в Приложение № 3 към чл. 3, т. 3 от Наредба за реда за класифициране на растенията и веществата като наркотични[15] – т.нар. рискови вещества.

♦ MDMA – влияе на невротрансмитерите, което от своя страна оказва влияние върху настроението на употребяващия. Вследствие употребата на MDMA се освобождава голямо количество серотонин и допамин, което води до рязко повишаване на положителните емоции, изпитвани от употребяващия, като влиянието на наркотика е с продължителност средно от 3 до 8 часа.

Достъпът до Darknet се осъществява чрез специфичен браузър (Tor), който позволява голяма степен на анонимност на потребителя[16]. Първоначално Tor като уеб браузър е създаден с идеята да обезпечава анонимност при комуникиране в сферата на отбраната[17]. По-настоящем всеки потребител на интернет услуги може безплатно да свали на компютъра си Tor, като употребата му в голяма степен наподобява тази на познатите браузъри като Google Chrome, Mozilla Firefox и т.н. Влизайки в Darknet чрез Tor потребителят има достъп до голям брой нелегални пазари, в които свободно се продават синтетични наркотици. Установяването на продавачи и купувачи от страна на правоприлагащите органи зависи в немалка степен от самата подготовка на тези продавачи и купувачи. Има различни нива на сигурност, които те самите могат да си осигурят при осъществяване на достъп до Darknet.

• Базовото ниво, което позволява най-лесно да бъдат установени продавачите или купувачите, е ако използват единствено браузъра Tor, който осигурява голяма степен на анонимност, но за правоприлагащите органи не представлява особена трудност да установят участника в една сделка със синтетични наркотици, ако използва само този браузър. Това е така, защото достъпът до Tor-мрежата се отразява при доставчика на интернет услугата (от англ. ISP – Internet Service Provider). Такава информация може да бъде изискана от разследващите органи при подозрение за участие на даден потребител в нелегална дейност в Darknet.

• Второто ниво на сигурност е използването на Tor в комбинация с VPN[18]. Ако се използва VPN, IP адресът е скрит още в началото, т.е. още преди потребителят да си осигури достъп до сайт в Darknet.

---

[15] Наредба за реда за класифициране на растенията и веществата като наркотични – Обн. ДВ. бр.87 от 4 Ноември 2011г., изм. ДВ. бр.97 от 8 Ноември 2013г., доп. ДВ. бр.85 от 10 Октомври 2023г.

[16] Разработчиците на Tor бразузъра го определят като мрежа от доброволно действащи сървъри, които позволяват на потребителите да подобрят нивото на лична неприкосновеност и сигурност при използването на услуги в интернет вж. Достъпно: https://2019.www.torproject.org/about/overview. [Посетено на: 26.09.2024].

[17] Goldschlag D.M., Reed M.G., Syverson P.F. (1996). „Hiding routing information, International Workshop on Information Hiding", Springer, pp. 137– 150.

[18] от англ. VPN – virtual private network – виртуална частна мрежа. VPN може да бъде определен като частна мрежа, която е създадена и функционира в рамките на публична мрежова инфраструктура

• Третото и най-сигурно ниво за потребителите, което създава и най-много трудности на разследващите органи, е употребата на операционната система Tails Linux, инсталирана върху USB.

Събирането на доказателства за нелегални пазари на синтетични наркотици в Darknet изисква от разследващите органи да проучат внимателно популярните пазари, както и да съберат информация за по-известни продавачи в съответните сайтове. Това може да стане чрез събиране на информация за извършваните транзакции, посредством blockchain-анализ. Blockchain[19]- анализ може да се осъществи в публични регистри на криптовалути, като например btc.com. Това изисква търпение и усилия от страна на разследващите органи, заради псевдонимизацията[20], характерна за биткойн. В публичните регистри информацията за транзакция се представя като поредица от букви и цифри, което не е достатъчно, за да се идентифицира конкретно лице. Затова се използват различни софтуерни инструменти, като например oxt.me[21], благодарение на които може да се проследят парични преводи на биткойни, защото инструментът създава графика, тип „мисловна карта“ на транзакциите, което значително улеснява тяхното проследяване.

Много ценни за събиране на електронни доказателства с цел разкриване на деяния, свързани с нелегално разпространение на синтетични наркотици са т.нар. honeypots[22]. Това са сайтове в Darknet, които имат за предназначение събирането на информация, свързана с дейността и личността на техните потребители.[23] Подобни сайтове могат да бъдат от различен тип. Някои от тях могат да бъдат конкретно насочени към разузнавателна дейност, с цел събиране на информация за киберпрестъпници чрез наблюдение на провеждани от тях разговори в различни чатове и форуми в уебсайтове в Darknet. Други могат да бъдат създавани с цел да предоставят услуги за неправомерно проникване в компютърни информа-

---

(интернет) – вж. Yuan R., Strayer W.T. (2001). „Virtual Private Networks: Technologies and Solutions“. Addison-Wesley Professional, Boston. както и Schmeh K. (2003). „Cryptography and Public Key Infrastructure on the Internet“ John Wiley & Sons Inc.. New York.

[19] Blockchain представлява своеобразна публична счетоводна книга, която съществува в онлайн пространството и в която всички извършени трансакции се съхраняват в поредица (верига) от блокчета. Веригата от блокчета расте пропорционално с броя блокчета, които се добавят към нея (съответно с броя извършени нови трансакции). Най-популярното приложение на Blockchain технологията е по отношение на трансакции с виртуална валута Bitcoin – по-подробно за Blockchain вж. Zheng, Z., Xie, S., Dai, H., Chen, X., & Wang, H. (2018). “Blockchain challenges and opportunities: A survey”. International Journal of Web and Grid Services, 14(4), 352–375.

[20] Псевдонимизацията представлява замяната на информация, която може да бъде използвана за идентифициране на потребител с псевдоним, който от своя страна не позволява директно идентифициране на потребителя. вж. Casabona C.M.R. (2017). “Anonymization and Pseudonymization: The Legal Framework at a European level”. The Data Protection Directive and Medical Research Across Europe. Taylor & Francis. стр. 33 и сл.

[21] Oxt.me е софтуерен инструмент за анализ на Blockchain трансакции. вж. Достъпно: https://www.cypherhunter.com/en/p/oxt/. [Посетено на: 27.09.2024].

[22] от англ. Honeypot означава букв. ”гърне с мед” и представлява жаргонен израз за уебсайт със специфично предзначение. вж. Достъпно: https://www.dictionary.com/browse/honeypot. [Посетено на: 27.09.2024].

[23] Karthikeyan R.,Geetha D. T., Vijayalakshmi S., Sumitha R. (2017). “Honeypots for network security” International journal for Research & Development in Technology, vol. 7, no. 2, pp. 62–66.

ционни системи. Целта на събираната от този втори тип honeypot сайтове е да бъдат документирани потребители, които заявяват hacking услуги[24].

Honeypot – сайтове са били използвани успешно в събирането на електронни доказателства за противоправната дейност на големи пазари в Darknet, в които незаконно са се продавали синтетични наркотици, извън други, непозволени от закона стоки. Такива пазари са Silk Road 2.0 и AlphaBay. Дейността на Silk Road 2.0. е успешно преустановена, благодарение на усилията на правоприлагащите органи през 2014 г. Но предвид динамичността, характерна за интернет пространството и в частност за Darknet, потребителите на наркотични вещества се ориентират към нов пазар, наречен от разработчиците му Evolution. Сайтът бързо набира популярност, но скоро прекратява своето съществуване, като е заменен, в ролята му на популярна платформа за продажба на наркотични вещества, от AlphaBay. След успешна операция, в резултат на която правоприлагащите органи си осигуряват администраторски достъп до сайта, те го превръщат в своеобразна платформа за събиране на информация за потребителите му. С установяване на контрол върху сайта, същият е препрограмиран така, че да събира потребителските имена и паролите на потребителите, с цел същите тези потребителски имена и пароли да бъдат използвани, за да се провери в какви други сайтове, например за разпространение на наркотични вещества, същите тези потребители имат регистрация. Доказателства за реалната локация на купувачи и продавачи се събират посредством анализ на метадатата от изображения, качвани от самите тях на уебсайта. Тези дейности изискват специфични технически познания, но в резултат на тях се обезпечава правната дейност по събиране на електронни доказателства.

III. Заключение

Събирането на електронни доказателства за разследване на деяния, свързани с разпространение на синтетични наркотици е дейност, която тепърва ще разширява своя обхват, предвид развитието на дигиталните технологии и за съжаление неизбежно съпътстващото го създаване на нови вариации на синтетични наркотици. С цел успешното разкриване на подобни деяния е необходимо правоприлагащите органи да прилагат модерни техники и методи, които да им гарантират успех в динамичната среда на информационните технологии – новото поле за извършване на престъпления, утвърдило се в нашето съвремие.

Библиография

Вучков В. (2023). Електронните доказателства по наказателни дела и техните източници – необходими разсъждения. Юридическо списание на Нов български университет, бр. 2, 16.

Вучков В. (2023). Наказателен процес в схеми, таблици, определения. София: Сиби.

Маринова Г. (2002). Електронните доказателства. Списание Правна мисъл, бр. 3.

Casabona C.M.R. (2017). "Anonymization and Pseudonymization: The Legal Framework at a European level". The Data Protection Directive and Medical Research Across Europe. Taylor & Francis.

Goldschlag D.M., Reed M.G., Syverson P.F. (1996). "Hiding routing information, International Workshop on Information Hiding". Springer.

[24] Mairh A., Barik D., Verma K., and Jena D. (2011), "Honeypot in network security: a survey," in Proceedings of the 2011 international conference on communication, computing & security, pp. 600–605.

Gutpa. A., Anand A. (2017). Ethical hacking and hacking attacks. International Journal of Engineering and Computer Science. Volume 6, Issue 4.

Karthikeyan R., Geetha D. T., Vijayalakshmi S., Sumitha R. (2017). "Honeypots for network security". International journal for Research & Development in Technology, vol. 7, no. 2.

Mairh A., Barik D., Verma K., and Jena D. (2011), "Honeypot in network security: a survey," in Proceedings of the 2011 international conference on communication, computing & security.

Schmeh K. (2003). "Cryptography and Public Key Infrastructure on the Internet". John Wiley & Sons Inc.. New York.

Yuan R., Strayer W.T. (2001). "Virtual Private Networks: Technologies and Solutions". Addison-Wesley Professional, Boston.

Zheng, Z., Xie, S., Dai, H., Chen, X., & Wang, H. (2018). "Blockchain challenges and opportunities: A survey". International Journal of Web and Grid Services, 14(4).

COLLECTING ELECTRONIC EVIDENCE DURING THE INVESTIGATION OF CRIMES RELATED TO THE DISTRIBUTION OF SYNTHETIC DRUGS

Veselin Vuchkov[25]
Daniel Delchev[26]

Abstract: Electronic evidence is increasingly used in the investigation of crimes in contemporary times. The dynamics of development of modern society and the technological "boom", as well as the application of technologies in every aspect of our daily life, contribute to the fact that an increasing number of the committed illegal acts leave an "electronic mark". The activity of distributing synthetic drugs is no exception to this. This publication aims to examine the main aspects of crimes related to the distribution of synthetic narcotic substances and the specifics associated with them, while presenting the possibilities of using electronic evidence and offering examples of some practices that could be actively implemented in order to prevent and reduce crimes in this area.

Keywords: synthetic drugs, electronic evidence, investigation, crimes, distribution, illegal markets.

[25] Ph.D. in Law, Professor of Criminal Procedure Law in the Law Department of New Bulgarian University, South-West University "Neofit Rilski" and the Academy of the Ministry of Interior, e-mail: vvuchkov@nbu.bg.

[26] Ph.D. in Law, Lecturer in the Department of Public Law – Academy of the Ministry of Interior, e-mail: DStDelchev@mvr.bg.