ОСОБЕНОСТИ НА СЪДЕБНИТЕ ЕКСПЕРТИЗИ ПРИ РАЗСЛЕДВАНЕ НА КИБЕРПРЕСТЪПЛЕНИЯ[1]

доц. д-р Невена Русева[2]
Русенски университет „Ангел Кънчев“
nruseva@uni-ruse.bg

Резюме: *В изложението е извършен анализ на приложението на съдебните експертизи при разследване на киберпрестъпления, като са обсъдени основните задачи, които подлежат на решаване в хода на експертното изследване. Обсъждането на горните въпроси е диференцирано, като е отнесено към отделните престъпни състави за киберпрестъпленията, предвидени в НК, респ. към предмета на доказване и обстоятелствата, подлежащи на установяване в хода на разследването.*
Ключови думи: *съдебни експертизи, киберпрестъпления, разследване, доказване, вещи лица, наказателен процес, досъдебно производство*

FEATURES OF FORENSIC EXPERTISE IN THE INVESTIGATION OF CYBERCRIME

Assoc. Prof. Nevena Ruseva, PhD
„Angel Kanchev” Univesity of Ruse
nruseva@uni-ruse.bg

Abstract: *The presentation analyzes the application of forensic expertise in the investigation of cybercrimes, discussing the main tasks that are subject to resolution in the course of the expert examination. The discussion of the above issues is differentiated, referring to the individual criminal offenses for cybercrimes provided for in the Criminal Code, respectively. to the subject of proof and the circumstances subject to establishment in the course of the investigation.*
Keywords: *forensic examinations, cybercrimes, investigation, evidence, experts, criminal trial, pre-trial proceedings*

Систематичното място, което заемат компютърно-техническите експертизи в класификацията, въведена в Приложение № 1 от Наредба № Н-1 от 14.02.2023 г. е в Клас „Съдебни инженерно-технически експертизи“.

Приложението на обсъждания вид експертизи в наказателното производство и най-вече в неговата досъдебна фаза, се обсъжда, като е разгледано в две направления:

[1] Докладът е представен на Кръгла маса, посветена на борбата с киберпрестъпността, организирана от Бургаски свободен университет, съвместно с Апелативна прокуратура – Бургас на 03.12.2025 г. – бел. авт.

[2] Авторът е доцент в Русенски университет „Ангел Кънчев“, преподавател по криминалистика и съдебни експертизи с дългогодишен стаж като разследващ полицай, автор на публикации в национални и международни издания, посветени на доказването в наказателното производство, както и на особеностите в криминалистическата тактика при прилагане на отделни способи на доказване, вкл. на приложението на съдебните експертизи в досъдебната фаза на наказателния процес.

- при разследване на посочените в криминалистичната наука „същински“ компютърни престъпления, които в контекста на настоящото изложение наричаме *киберпрестъпления;*
- при разследването на т.нар. несъщински компютърни престъпления, вкл. при разследване на друго престъпление, във връзка с .извършването на което са били използвани компютърни системи или носители на компютърни данни.

В българската правна теория няма въведена дефиниция за *киберпрестъплението*, вкл. такава не е предвидена и в наказателния ни закон, но през призмата на утвърдените доктрини в системата на националната и международна национална сигурност, може да приемем, че *киберпрестъплението* може да бъде определено като:

„Форма на престъпна деятелност, осъществена в интерактивна информационна среда, при която се засягат обществени отношения, свързани с експлоатацията на информационни и технологични структури, системи и мрежи, посредством които се осъществява онлайн комуникация“[3].

В контекста на горното и за нуждите на настоящото изложение, извеждаме и дефиниция за компютърно-техническите експертизи по следния начин:

„Извършено по реда на НПК ненаучно изследване от лица със специални познания в областта на компютърната техника и технологиите, което е насочено към събиране и анализ на информационни данни, свързани с предмета на разследване и извеждане на изводи и заключения, отнесени към поставените от възлагащия орган въпроси“.

Тези *въпроси*, наричани още *задачи*, най-често се отнасят до различни области от сферата на информационните, комуникационни и мрежови технологии.

Компютърно-техническите експертизи, както и останалите видове експертизи, като процесуален инструмент и доказателствен способ в българския наказателен процес, се назначават и извършват по правилата, предвидени в разпоредбите на чл. 144 НПК – 154 НПК вкл. Тук следва да се посочи и друго правно основание, което навежда към необходимост от назначаване на компютърно-техническите експертизи в определени хипотези, а именно – ***Конвенцията за престъпления в кибернетичното пространство****, приета на 109-то заседание на Комитета на Министрите на Съвета на Европа и открита за подписване в Будапеща на 23.11.2001 г. Конвенцията е ратифицирана в Р България със закон, приет на 05.04.2005 г.*[4]. В нея са начертани общите насоки за разследване на за престъпления в кибернетичното пространство, които насоки са отнесени към процедурния ред, свързан с изискване, претърсване, изземване, съхраняване и **изследване** на информационни данни, свързани с предмета на разследване. По правилата на действащия Наказателно-процесуален кодекс[5], визираното в горната Конвенция **изследване** може и следва да се осъществява единствено чрез предвидения в НПК процесуален инструмент – експертизата.

Компютърно-технически експертизи се назначават и могат да дадат отговори на редица относими към делото въпроси, съобразно различни критерии, основния от

[3] В този смисъл, прецизни и новаторски са дефинициите е съжденията на проф. д-р Илин Савов в публикацията му, посветена на киберпрестъпленията „Един поглед върху същността на киберпрестъпленията“, сп. Политика и Сигурност, бр. 3 от 2017 г.

[4] Изд. от МП, обн. ДВ, бр. 76/15.09.2006 г., в сила за Р България от 01.08.2005 г.

[5] В сила от 29.04.2006 г., Обн. ДВ. бр.86 от 28 Октомври 2005г., посл. изм. и доп. ДВ. бр.97 от 14 Ноември 2025 г.

които е спрямо вида на разследваното престъпление, респ. систематичното място, което заема в НК и според конкретната следствена ситуация.

В този смисъл, като се имат предвид престъпните състави, въведени в Наказателния кодекс, но без да претендираме за изчерпателност, можем да систематизираме компютърно-техническите експертизи в следния ред:

1. Експертизи, назначавани при разследване на престъпленията, включени в Глава девета „а“ от НК, озаглавена *Компютърни престъпления:*

1.1. Неправомерно осъществен достъп до информационна система или части от нея – престъпление по чл. 319 а НК.

Предметът на доказване на горното престъпление предполага в кръга от обстоятелствата, подлежащи на установяване, които могат да бъдат решени посредством експертиза, да бъдат включени въпроси относно:

- Установяване на IP адреса, от който е осъществен достъп до информационната система; установяване на конкретното устройство (компютър или друго устройство) по MAC адрес или други идентификационни белези, от което е осъществен достъпа; установяване и анализ на осъществените достъпвания (хронология на достъпвания) до устройството/информационната система в определен период от време; установяване на време и място на достъпване до информационната система; установяване на механизъм/начин на осъществяване на достъпа; каква е степента на технологична защитеност на компютърното устройство и/или информационна система, станали обект на посегателство, вкл. за наличие или липса на защитни мерки за достъп; дали и какви последици са настъпили в резултат на извършения неправомерен достъп и др. Наред с горните въпроси, в случай, че по делото са налице данни за предварително подготвяна и обсъждана престъпна дейност между отделни лица, на вещото лице следва да бъде поставена задача да бъдат изведени запаметените в мобилното устройство – обект на изследване данни (съдържание) относно: телефонен указател, регистър на входящи и изходящи, вкл. пропуснати и отхвърлени повиквания и кратки текстови съобщения, както и кореспонденция (чат), осъществена под формата на съобщения през социални мрежи и др.

1.2. Неправомерно добавяне, копиране, използване, внасяне на промени, пренос, изтриване, повреди, влошаване, скриване или унищожаване на компютърни данни в информационна система или спиране на достъпа до такива данни – престъпление по чл. 319б НК.

Възлагането на експертизи за разследване на престъпление от този вид предполага необходимост от изясняване на следните въпроси:

- Наред със задачите, изброени по-горе в т. 1.1. от настоящото изложение, на вещото лице могат да бъдат поставени задачи, свързани с изясняване на въпроси относно вида на посегателство (конкретното изпълнително деяние) досежно естеството и степента на засягане на компрометираните компютърни данни; установяване на първоначалното състояние на компрометираните компютърни данни; възстановяване на изтритите, променени, повредени, скрити или влошени данни; установяване на начините и използваните средства/инструменти, посредством които са извършени съответните посегателства; да бъде установено в интернет историята, съхранена в представените устройства – обекти за изследване, има ли регистрирани влизания/достъпвания до конкретни електронни адреси и инсталирани приложения и в какви периоди от време и др.

1.3. Въвеждане на компютърен вирус в информационна система или компютърна мрежа – престъпление по чл. 319г НК.

Разследването на горното престъпно посегателство, което от обективна страна предполага задължително настъпване на престъпен резултат, изисква изясняване на въпроси относно следното:

- да се посочи дали представените обекти за изследване (информационна система или компютърна мрежа, вкл. части от тях) съдържат зловреден софтуер и определяне на вида и естеството му; установяване на първоначалното състояние на компрометираните информационна система или компютърна мрежа; нивото и степента на защита, които те са имали преди посегателството, вкл. чрез пароли или системи за достъп; да се опишат приложенията и използваните софтуери в представените обекти за изследване, като бъдат посочени вида, предназначението и периода на инсталиране на всяко от тях; установяване на въведени антивирусни програми и източника, от който са инсталирани, както и време и механизъм на инсталирането им; да се посочи дали в представените обекти за изследване има инсталиран конкретно посочен (индивидуализиран) софтуер и в случай, че има такъв, да бъде направено описание относно предназначението му, периода на инсталиране/въвеждане, периоди на достъпване (използване), начин на достъпване и използване; определяне на вида и естеството на компютърния вирус/зловреден софтуер[6] и ясно установяване на пораженията над информационната система или компютърна мрежа, които е нанесъл или би могъл да нанесе; механизъм, по което е извършено въвеждането на компютърния вирус и установяване дали от разстояние или чрез пряк достъп е извършено това; има ли регистрирани в информационна система или компютърна мрежа влизания/достъпвания до конкретни електронни адреси и инсталирани приложения и в какви периоди от време и др. Наред с горните въпроси и съобразно наличните данни по делото и конкретната следствена ситуация, на вещото лице могат да бъдат поставени и задачи, свързани установяване на трансгранични маршрути на електронни данни и престъпни инфраструктури (сървъри, мрежи) извън страната.

1.4. Създаване, набавяне за себе си или за другиго, внасяне, изнасяне, прехвърляне, превозване, предоставяне или по друг начин разпространяване на компютърни програми, пароли, кодове или други подобни данни за достъп до информационна система или част от нея с цел да се извърши престъпление по

[6] Дефиницията, въведена от Microsoft за зловреден софтуер сочи: „*Злонамереният софтуер е злонамерен софтуер, предназначен да нарушава работата, да повреждa или да получава неоторизиран достъп до компютърни системи. Киберпрестъпниците използват злонамерен софтуер, за да заразяват устройствата с цел кражба на данни, получаване на банкови данни, продажба на достъп до компютърни ресурси или лична информация или изнудване на плащания от жертвите*.“ - https://www.microsoft.com/bg-bg/security/business/security-101/what-is-malware#:~:text=13%20%D0%BC%D0%B8%D0%BD%D1%83%D1%82%D0%B8-,%D0%94%D0%B5%D1%84%D0%B8%D0%BD%D0%B8%D1%86%D0%B8%D1%8F%20%D0%B7%D0%B0%20malware,%D0%B8%D0%B7%D0%BD%D1%83%D0%B4%D0%B2%D0%B0%D0%BD%D0%B5%20%D0%BD%D0%B0%20%D0%BF%D0%BB%D0%B0%D1%89%D0%B0%D0%BD%D0%B8%D1%8F%20%D0%BE%D1%82%20%D0%B6%D0%B5%D1%80%D1%82%D0%B2%D0%B8%D1%82%D0%B5.

чл. 171, ал. 3[7], чл. 319а, чл. 319б, чл. 319в или чл. 319г НК - престъпление по чл. 319д НК.

Специфично за обсъжданото съставно престъпление е, че негов субект може да бъде не лицето, което извършва компютърно престъпление, а лице, което създава, придобива или разпространява средства, предназначени за извършването на друго престъпно посегателство – по чл. 171, ал. 3 , чл. 319а, чл. 319б, чл. 319в или чл. 319г НК. Обект на такова посегателство в настоящия текст могат да бъдат лимитивно изброените в състава на чл. 319б НК: компютърни програми, пароли, кодове или други подобни данни за достъп до информационна система или част от нея. Именно особения характер на това престъпление, което по своята същност представлява своеобразно престъпно намерение, улесняващо или подготвящо друго престъпление, предполага необходимост от решаване на комплекс от значими за делото задачи, което може да се реализира единствено чрез извършване на компютърно-техническа експертиза. Основните такива задачи са свързани с:

- Установяване на конкретното действие, вида и естеството му (изпълнителното деяние), посредством което е настъпил престъпния резултат (напр. създаване или внасяне на хакерски инструменти, програмни продукти, зловреден софтуер или т.нар. „фишинг платформи“ за преодоляване или промяна на пароли, защити и др.); времето и начина на извършването му; механизма, по който е извършено конкретното действие и обхвата на пораженията, които са нанесени с извършването; изясняване на конкретния компрометиран обект на посегателство (компютърни програми, пароли, кодове или други подобни данни за достъп до информационна система или част от нея), вкл. относно времето и мястото на първоначалното им инсталиране/въвеждане в съответната информационна система и източника, от който са придобити; установяване на вида и степента на постигане на специалната цел, предвидена в разпоредбата на чл. 319д, а именно – дали и в каква степен е осъществен състава на изброените в текста престъпления и др.

1.5. Доставяне на информационни услуги в нарушение на разпоредбите на чл. 6, ал. 2, т. 5 от Закона за електронния документ и електронните удостоверителни услуги[8] – престъпление по чл. 319е.

Престъплението по чл. 319е НК предполага изясняване на въпроси, свързани с:

- Установяване на точния механизъм, по който е осъществено доставянето на информационни услуги – относно време, място, начин, източник и степен на това доставяне. В тази връзка пред вещото лице следва да бъдат поставени задачи, насочени към изясняване на механизма, по който е реализиран процесът на предаване или осигуряване на информационните услуги, вкл. чрез установяване на IP адреса, от

[7] Чл. 173. (1) Който издава или използва под свое име или под псевдоним чуждо произведение на науката, литературата или изкуството или значителна част от такова произведение, се наказва с лишаване от свобода до три години или с глоба от сто до триста лева, както и с обществено порицание. ...

(3) Когато деянието по ал. 1 е извършено в интернет или са причинени значителни вредни последици, наказанието е лишаване от свобода до шест години и глоба до десет хиляди лева.

[8] Съгл. чл. 6, ал. 2, т. 5 от Закона за електронния документ и електронните удостоверителни услуги Посредникът при електронното изявление е длъжен да… съхранява информацията по т. 3 (за точно определяне на времето и източника на предаваните електронни изявления) в срок от една година – бел. авт.

който е осъществено деянието; установяване на конкретното устройство (компютър или друго устройство), от което е осъществено доставянето на горните услуги чрез съответния MAC, както и установяване на естеството на конкретните компрометирани електронни услуги, основно такива, свързани с електронния подпис, електронната идентификация и удостоверителните услуги. На вещото лице следва да бъдат поставени и задачи с оглед изясняване на въпроси, свързани с въведените и налични в информационна система или компютърна мрежа технически мерки за защита на електронния подпис, електронния печат и удостоверителните средства и др.

2. Извън т.нар „същински“ компютърни престъпления, в НК са предвидени и други престъпни състави, които включват престъпно използване на информационни данни и компютърни мрежи или части от тях, а именно при условно наречените в криминалистичната теория „несъщински“ компютърни престъпления:

2.1. Разпространение /използване и държане на порнографски материали.

Разследването на престъпления, свързани с разпространение на порнографски материали чрез информационна или съобщителна технология или по друг подобен начин предполага назначаване на компютърно-техническа експертиза, която да отговори на въпроси относно:

- Установяване съдържанието на съответната информационна система/ устройство и посочване вида, естеството, местоположението, времето на инсталиране и на експортиране на съответните файлови единици, носещи характер на „порнографско съдържание“; да се опишат приложенията и използваните софтуери, свързани с набиране и обработка на файлове с процесно съдържание, съхранявани в представените обекти за изследване, като бъдат посочени вида, предназначението и периода на инсталиране на всяко от тях; проследяване на „интернет историята“ на съответната система/устройство, които са обект на изследване, както и проследяване на връзките, посещавани от съответните потребители/устройства; установяване на достъпваните адреси и прикачените файлове, които са насочвани (изпращани) към тях, вкл. относно времето/периода, когато е извършвано това;

В хода на разследване на престъпления по чл. 159, ал. 6 НК (относно държане или набавяне чрез информационна или съобщителна технология или по друг начин порнографски материал, за създаването на който е използвано лице, ненавършило 18 години, или лице, което изглежда като такова) и престъпления по чл. 159, ал. 7 НК (за съзнателно осъществен достъп до порнографски материал, за създаването на който е използвано лице, ненавършило 18-годишна възраст, или лице, което изглежда като такова, чрез използване на информационна или съобщителна технология), наред с горните задачи, поставени пред компютърно-техническата експертиза, следва да бъдат установени и обстоятелства, свързани с безспорно изясняване на възрастта на лицето, използвано за създаване на порнографските материали.

Обсъдените по-горе задачи, които могат да бъдат поставени за решаване в акта за назначаване на експертиза, се отнасят в голяма степен и към въпросите, подлежащи на установяване чрез компютърно-техническа експертиза при разследване на престъпления по чл. 155а НК и чл. 155б НК.

2.2. Престъпления, включени в Глава трета, раздел V. *Нарушаване неприкосновеността на кореспонденцията* от НК.

В текста на чл. 171, ал. 4 НК е предвидена наказателна отговорност при неправомерно нарушаване неприкосновеността на кореспонденцията, когато предмет на деянието са компютърни данни, изпращани в рамките на една или между повече информационни системи, включително електромагнитни емисии от информационна система. Задачите, поставени за решаване пред вещото лице, на което се възлага компютърно-техническа експертиза, могат да са насочени към:

- Установяване вида, съдържанието и обема на компютърните данни, предмет на деянието; установяване на конкретното устройство (компютър или друго устройство) по MAC адрес или други идентификационни белези, от което е осъществен достъпа; установяване и анализ на осъществените достъпвания (хронология) до устройството/информационната система в определен период от време; определяне на конкретните информационни системи, от и до които са изпращани компютърните данни и тяхното индивидуализиране; определяне на точния механизъм, посредством който е извършено конкретното деяние, довело до нарушаване неприкосновеността на кореспонденцията и в какво се изразява това нарушаване и др.

2.3. Компютърна измама по чл. 212а НК.

Изпълнителното деяние на престъплението по ал. 1 от чл. 212а НК се изразява в това, чрез извършване на лимитивно изброени в текста действия: възбуждане или поддържане заблуждение у някого, като бъдат внесени, изменени, изтрити или заличени компютърни данни или използва чужд електронен подпис, да бъде причинена вреда. Престъплението по ал. 2 на чл. 212а НК въвежда като резултат от извършването му получаването на облага.

Предметът на доказване на престъпленията по чл. 212 НК предполага при разследването, наред с останалите способи на доказване, предвидени в НПК, също и назначаване и извършване на компютърно-техническа експертиза, посредством която да бъдат решени следните задачи:

- Изясняване на въпросите, посочени в т. 1.2. по-горе от настоящото изложение, които се отнасят до изпълнителните деяния, предвидени в чл. 319 б НК, а именно *внасяне, изменение, изтриване и заличаване (скриване/унищожаване)* на компютърни данни. Наред с това следва да бъде възложено установяване на съдържанието на информационни данни в обекта на изследване, времето на инсталиране на процесните файлове, приложени или софтуери, свързани с измамливите действия на извършителя; комуникацията с пострадалото лице/лица, осъществена по електронен път, както и прикачените файлове към тази комуникация и др. В случай, че за предмета на доказване са от значение вида, естеството и обема на конкретни файлове, то вещото лице следва да извърши анализ и детайлно изследване и на тяхното съдържание.

Тук е мястото, където следва да бъде обсъдено все по-често срещаната форма на измама посредством използване на изкуствен интелект, независимо дали в т.нар. ѝ класическа форма – по чл. 209 или по чл. 212а – чрез клониране на глас в телефонните измами, чрез възпроизвеждане на изображения, лица и събития, разпространяване на фалшиво съдържание и др. В разглежданите хипотези компютърно-техническата експертиза може да се назначи и като комплексна – с участието на специалист от областта на лицевата идентификация и да бъдат поставени въпроси, насочени към изясняване на обстоятелства, свързани с използване или не на изкуствен интелект при визуализирането на конкретни изображения на лица.

2.4. Използване на платежен инструмент или данни от платежен инструмент без съгласието на титуляря – чл. 249 НК

Предвид многообразието на механизмите/начините, по които може да бъде извършено престъпление по чл. 249 НК, също толкова многообразни и отнесени към конкретната следствена ситуация могат да бъдат задачите, поставяни на вещото лице, ангажирано с изготвяне на компютърно-техническа експертиза. Обекти на такава експертиза могат да бъдат телефони, таблети, компютри, софтуери, отделни програмни продукти, информационни мрежи и др. В отделните хипотези като обекти на изследване могат да бъдат включени още устройства за блокиране на банкови карти в банкомати (АТМ), устройства, предвидени за скимиране, т.е. за клониране на банкови карти, които подлежат на самостоятелно експертно изследване. Неправомерно използване на платежен инструмент или данни от него може да бъде осъществено и посредством извършване на престъпления от обсъдените по-горе – създаване и използване на специализиран зловреден софтуер, измама в интернет пространството, неправомерно осъществен достъп до информационна система или части от нея и др. И именно като съобразят наличната доказателствена информация за механизма на достъпване до данните на процесния платежен инструмент, разследващите органи следва да формулират и поставят задачите на компютърно-техническата експертиза, обсъдени по-горе в настоящото изложение.

Наред с посочените по-горе както *същински*, така и *несъщински* компютърни престъпления, престъпните посегателства, извършването на които е свързано с експлоатация на компютърни системи и устройства, могат да бъдат изключително разнообразни по вид, поради което е невъзможно да бъдат обсъдени и изброени лимитивно.

Като общоприложими правила за всички компютърно-технически експертизи, могат да бъдат посочени следните:

- → Прецизно и изчерпателно индивидуализиране на всеки обект на експертизата, който се представя на вещото лице;
- → Събиране на достатъчна по вид и обем изходна доказателствена информация относно извършваната престъпна деятелност и лицата/устройствата, които имат отношение към нея;
- → Прецизиране на периода, в който е извършено престъплението, респ. периода, който подлежи на изследване и анализ в хода на експертизата;
- → Използване на инструментариума на международната правна помощ в хода на наказателното производство с оглед събиране на информация от други държави по съответния процесуален ред;
- → Обсъждане и преценка за възможността експертизата да бъде възложена на чуждестранно вещо лице[9] – самостоятелно или като колективна – с участието на такова от страната ни.

[9] В тези случаи е необходимо вещото лице да отговаря на съответните изисквания, за да може да му бъде възложено изготвяне на експертиза, вкл. на условията, съдържащи се в чл. 7, ал. 3, т. 4 НАРЕДБА № Н-1 ОТ 14 ФЕВРУАРИ 2023 Г. ЗА ВПИСВАНЕТО, КВАЛИФИКАЦИЯТА И ВЪЗНАГРАЖДЕНИЯТА НА ВЕЩИТЕ ЛИЦА – бел. авт.

И на последно място, но не по важност – възлагащите компютърно-техническа органи следва при възможност предварително да формулират и обсъдят с вещото лице въпросите, подлежащи на установяване и да ги съобразят с техническите възможности те да бъдат решени именно с този вид експертиза и именно в определен момент от разследването.

ИЗТОЧНИЦИ:

1. Владова-Недкова, И. Разследване на компютърни престъпления, С., Софи Р, 2023, ISBN 2010014736
2. Павлов, Хр. Проблеми в организацията на съдебната експертиза в България, Световна наука 2018, № 1 /29/, Януари 2018
3. Савов, И. Един поглед върху същността на киберпрестъпленията, сп. Политика и Сигурност, бр. 3/ 2017 г.