РАЗСЛЕДВАНЕ НА КОМПЮТЪРНИ ПРЕСТЪПЛЕНИЯ

гл. ас. д-р Чавдар Грошев
ПУ „Паисий Хилендарски" – Пловдив

Резюме: *В статията са разгледани най-често извършваните компютърни престъпления, като са анализирани използваните способи за доказване. Този вид престъпления в последните години заемат все по-голям дял в статистиката на престъпността. Тяхното противодействие изисква подготвени кадри и добра материално-техническа база на разследващите органи.*

Ключови думи: *разследване, компютърни престъпления, противодействие, способи.*

COMPUTER CRIME INVESTIGATION

Assist. Prof. Chavdar Groshev, PhD
University of Plovdiv

Abstract: *The article examines the most frequently committed computer crimes, analyzing the methods of proof used. In recent years, this type of crime has taken an increasingly large share in crime statistics. Their counteraction requires prepared personnel and a good material and technical base of the investigative bodies.*

Keywords: *investigation, computer crimes, countermeasures, methods.*

I. Увод

Компютърните престъпления са сравнително нови като вид, в сравнение с другите конвенционални престъпления /кражби, грабежи убийства и т.н./. При сегашното развитие на информационните технологии, заемащи различни аспекти от обществения живот, трудно бихме могли да си представим извършването на престъпления в която и да е сфера /особено на икономиката или финансите/, без да е използвана компютърна информационна система[1]. Това важи особено за дейността на организираните престъпни групи които, използвайки дигиталните технологии, развиват нови форми на традиционната престъпна дейност /напр. чрез група в приложението „телеграм" се разпространяват наркотици, продават се маркови стоки, без разрешение на маркопритежателя и т.н./.

[1] Съгл. чл. 93, ал.1, т. 21 от Наказателния кодекс: „Информационна система" е всяко отделно устройство или съвкупност от взаимосвързани или сходни устройства, което в изпълнение на определена програма осигурява или един от елементите на което осигурява автоматична обработка на данни, както и компютърните данни, съхранявани, обработвани, извличани или предавани от такова устройство или група от устройства с цел оперирането с тези данни и използването, защитата и поддръжката им;

Всичко това води до извод, че популярното разделение на типични(същински) компютърни престъпления – по глава 9а от Особената част на НК /чл.319а-319е/[2] и компютърни престъпления в широк смисъл(несъщински) – тези, за чието извършване се използва компютърна система, практически е загубило своя смисъл. Понастоящем и в теорията, и в практиката масово се е наложил терминът „киберпрестъпления", с който се обозначават всички престъпни посегателства, при които се използва компютърна система и/или са извършени в дигитална среда. Поради тези причини, от важно значение при противодействие на компютърните престъпления, е познаването на основните форми на проявление на киберпрестъпността в интернет. В същото време развитието на дигитализацията и възможностите, които предоставя интернет пространството с възможност за анонимно достигане на която и да е точка по света, затруднява разследването им. Поради това, успешното им противодействие изисква добре обучени и разполагащи с подходящото техническо обезпечаване правоохранителни органи. Само ще отбележим, че в това отношение държавата следва да положи повече усилия, които да осигурят адекватна реакция срещу този вид престъпност.

II. Най-често извършваните компютърни престъпления:

- „компрометирането на междуфирмена кореспонденция" /компрометиран интерфейс/. Това е достъпване до пощенска кутия на жертвата или на нейн контрагент. Това най-често се получава, като ползвател на пощенската кутия въведе паролата си в отговор на т.нар. „фишинг" съобщение. След анализ от страна на извършителя за целите на използване на достъпената поща, се „подменя" истинската сметка, по която трябва да бъде извършено някакво заплащане, с номер на сметка, контролиран от него или от негови съучастници. За мотивация на жертвата, извършителят използва подобни съобщения, като водените до този момент, като целта е да убеди контрагента да смени номера на банковата сметка, под предлог „ревизия на движенията по сметката от банката" или „данъчна ревизия". Задължително се изисква и копие от преводното нареждане (т.нар. СУИФТ съобщение), за да се разпоредят със сумата в максимално кратък срок след получаването й. Така, чрез манипулиране на междуфирмената кореспонденция, дейците се намесват /обикновено при изпратена проформа фактура от реален кореспондент/ в кореспонденцията, като заблуждават фирмата, която трябва да преведе пари, че сметката, по която следва да бъде преведена сумата, е друга.

- „нигерийска измама". Най-общо схемата се състои в мотивиране на жертвата да изпрати определена сума пари, за да получи много по-ценна пратка /сума пари от наследство или печалба от лотария, в която жертвата дори не е участвала/. Първият контакт обикновено е или чрез фишинг имейл, или в платформа за социална комуникация (Фейсбук, Скайп, сайт за запознанства и др.). Вариантите да се мотивира жертвата да изпрати пари на непознат са различни, като най-често използваните са: помощ за изнасяне на голяма сума пари от друга държава; получаване на чек или печалба от лотария, или изпращане на много рядка и ценна вещ. Най-честият претекст е необходимостта от заплащане на митнически или банкови такси. Обикнове-

[2] За подр. вж. Дончева, Д. Компютърни престъпления по Глава девета „а" от Наказателния кодекс, Правна мисъл № 2, 2003, стр. 98-106

но малката сума, която се изисква за плащане от жертвата, на база на очаквана голяма печалба, претъпява вниманието й.

- „романтична връзка". Използва се виртуална романтична връзка с измамника. Обикновено парите се изпращат като предоставен заем от жертвата или за получаване на ценна пратка. В други случаи парите се изпращат за получаване на виза, за закупуване на самолетен билет или за помощ на близък на измамника. Много често за мотивиране на жертвата се използват видеоразговори по Skype или Viber, както и обмен на снимки. Жертвата бива заблудена, че контактува с високопоставен служител/ка с положение в обществото. Подобно на „нигерийската измама" и тук целта е да се мотивира жертвата да изпрати определена сума пари на дееца. Често след изпращане на първоначална сума, спрямо жертвата бива поддържано заблуждение, с цел да продължи да превежда пари.

- „разпространение на порнографски материали[3]". Съществуват много места в Интернет, служещи за организиране на търговия или размяна на детска порнография. Много порнографски сайтове служат за прикриване на друг вид незаконна дейност, като склоняване към проституция, трафик на хора и др.

- изнудване, принуда, чрез заплахи, че ще бъде публикувана придобита лична информация на жертвата. При този вид посегателство или е достъпено до компютърната система и е извлечена информация, или е осъществена комуникация с жертвата и тя е изпратила лична информация. За съжаление все повече деца са потърпевши от такива престъпления.

III. Разследване на компютърни престъпления.

Както всяко престъпление, така и компютърните престъпления, имат собствена криминалистическа характеристика. Всяко едно действие в дигитална среда оставя следи /напр. изпращане на имейл, снимки, получаване на писма и др./. Работата на разследващите органи е да ги установят, да ги фиксират и да ги изземат по съответния процесуален ред. Криминалистическата тактика на разследване на компютърно престъпление обхваща на първо място събиране на необходимата информация за вида на извършеното престъпление. Обикновено законният повод е уведомяване на полицейските органи или прокуратурата за извършено престъпление /нерегламентиран достъп, компютърен вирус, компютърна измама, някаква промяна в компютърната система и т.н/. В зависимост от получената информация се решава и първият въпрос – дали да бъде образувано досъдебно производство на осн. чл. 212, ал.1 от НПК /с постановление на прокурора при наличие на кумулативните предпоставки: законен повод и достатъчно данни за извършено престъпление/. Липсата на достатъчно данни и липсата на необходимост от неотложни процесуални действия обосноваят извършване на проверка по реда на Закона за съдебната власт. Спецификата на тези престъпления и особено възможността за бързото заличаване на следите, налагат в повечето случаи образуване на досъдебно производство. При неотложност, досъдебното производство се образува при хипотезата на чл. 212, ал.2 от НПК – със

[3] Съгласно чл. 93, ал.1, т.28 от Наказателния кодекс : „Порнографски материал" е изготвен по какъвто и да е начин, неприличен, неприемлив или несъвместим с обществения морал материал, чието съдържание изобразява реално или симулирано блудствено действие, съвкупление, полово сношение, включително содомия, мастурбация, сексуален садизъм или мазохизъм, както и похотливо показване на половите органи на лице;

съставяне на протокола за първото действие по разследване/. Тази хипотеза е най-често използвана при образуване на дела за компютърни престъпления[4].

1. Процесуално-следствени действия при разследването.

Планирането, организирането и предприемане извършването на конкретните следствени действия зависи от изграждането и проверката на възможните версии в конкретната ситуация. Най-общо може да се каже, че обстоятелствата, които подлежат на установяване, са кой е пострадал, в какво се изразява посегателството, кога, къде и как е извършено престъплението, кой го е извършил[5], с какви мотиви и цели.

Планиране на разследването обхваща както отделните действия, така и самият алгоритъм на поведение. Предприемането на следствените действия зависи и от придобитата оперативна информация, която може да е с ключово значение при разследването. Какви действия следва да бъдат извършени при разследването зависят и от това дали престъплението вече е извършено /довършено/ или е в процес на извършване /напр. периодично разпространяване на порнографски материали с детска порнография или използване на нелегален софтуер и т.н./.

При разследването могат да бъдат използвани всички процесуални способи, предвидени в чл. 136 от НПК, като едни от основните и най-често използвани способи за събиране на доказателства при разследване на този вид престъпления са оглед, претърсване, изземване, обиск и специални разузнавателни средства. Кой способ ще бъде избран, както и дали ще е необходимо да бъдат използвани в комбинация, зависи от конкретната специфика на разследваното събитие.

1.1. Планиране и подготовка за претърсване.

Извършва се, когато има достатъчно основание да се предполага, че в някое помещение или лице се намират информационна система или носители, съдържащи такива данни, имащи значение за разследваното събитие. В тази връзка следва да бъде сторено следното:

- да бъдат проучени всички събрани материали, като бъдат установени връзките, начинът на комуникация и местоположението /при възможност/ на извършителя и евентуалните съучастници.

- да бъде установено как информационната система е свързана в мрежата – има ли изнесени работни места с възможност за дистанционен достъп до устройствата. Оперативната информация е от изключително важно значение за планирането на конкретните действия.

- да се определи броят на специалистите – технически помощници, които ще участват в претърсването. Това зависи от броя на помещенията и информационните системи, които се очаква да бъдат посетени и иззети. Необходимо е да се прецени и броят на вещите лица, които да присъстват, с оглед изготвяне на експертиза в хода на разследването.

[4] На практика предварителната проверка е по-рядко използван механизъм. Това е така, защото при този вид престъпления заличаването на следите е лесно и бързо, и събирането им обикновено става при неотложност.

[5] Тук важна роля има полицейската регистрация. За подр. вж. Бързинска, Цв., Полицейската регистрация в светлината на Решение на Съда на ЕС, пети състав от 26.01.2023 г. по дело С-205/21, Сборник с доклади от ЮМНК, ВУСИ, Пловдив 2023, стр. 35-53

- осигуряване на различни инструменти, материали, с които да се маркират и изземат компютърните системи и периферни устройства /при необходимост/.

- изготвяне на следствено-оперативен план с необходимите реквизити – време и начин на извършване, състав на участниците, мерки за безопасност на служителите, технически средства, които ще се използват – осветление, камери, металотърсачи, флашки, външни дискове и др., помощни средства, които могат да се използват – белезници, палки, чували, лепенки, транспортни средства и т.н.

1.2. Провеждане на претърсване и изземване. Обиск.

- извършва се или след предварително разрешение от съдия от съответния първоинстанционен съд, или от съдия от първоинстанционния съд, където се провежда действието. В случаите на неотложност протоколът следва да се представи пред съда за одобрение, не по-късно от 24 часа от приключване на действието.

- при претърсването се поставя охрана, с оглед недопускане да се изнасят материали от помещенията.

- предотвратява се всякаква възможност за комуникация на лицата в помещението, посредством всякакви устройства както помежду им, така и с външни лица.

- незабавно се предотвратява достъпа на лицата в помещението до всякакви компютърни системи, периферни устройства и достъп до захранването.

- при необходимост може да се извърши и обиск на присъстващите лица при наличие на предпоставките на чл. 164 от НПК.

- установява се броят на компютърните системи, като специалистът технически помощник изготвя огледално копие т.нар. „имидж-копие“ на информацията. Принципно, ако е събрана информацията, която допринася за разследването – компютърната система се изключва по правилния начин /shut down/, след което се разкачва от кабелите. Кабелите се разкачват от страната на компютъра, а не от контакта. Извършените действия се описват подробно в протокол.

- изземва се цялата техническа документация, относима към информационната система – бележници, документи, и т.н., в които може да се съдържат пароли, кодови за достъп и т.н.

- изземват се носителите на информация – флашки, дискове, карти, и т.н. Когато се прецени, че няма риск от последващо въздействие върху носителя на компютърните информационни данни се изземват само данните – при изготвяне на огледално копие на цялото съдържание на носителя. Изземва се хардуера /твърдия диск/, при необходимост от назначаване на експертиза.

- в случай на необходимост от идентифициране на лица могат да се снемат дактилоскопни и ДНК следи от компютърната система и периферните устройства- клавиатура, мишка, принтер, рутер и т.н.

- по преценка на ръководещия екип могат да бъдат иззети всички устройства, служещи за въвеждане на данни – мишка, клавиатура, скенери, четци и т.н.

- вещите се предоставят на поемните лица и другите присъстващи, запечатват се с лепенки, опаковат се и се запечатват.

- за извършените действия се съставя протокол, в който се посочва времето и мястото на претърсването, участвалите лица, описва се всичко, което е намерено с индивидуализиращите признаци /марка, модел, номер и т.н/. Изготвят се снимки и/или видеоклип.

- иззетите компютърни системи и периферни устройства се транспортират и съхраняват така, че да се избегне електромагнитно или механично въздействие вър-

ху тях. Те са веществени доказателства по делото и на тях може да бъде извършен оглед по реда на НПК.

Без изричното разрешение на специалиста – технически помощник не следва да се изключва или включва компютърната система. Не се стартират никакви файлове. Когато се касае за оглед на персонален компютър, следва да се установи дали той се намира в работен режим /изображение на екрана, шум от вентилатор, светеща индикаторна лампичка и др./ Ако компютърът е в работещ режим е абсолютно задължително да се направи оглед с компютърен специалист – технически помощник на устройството в работещ режим. Фиксира се в работещ режим, като се изготвят снимки.

В някои случаи достъпването до определени файлове от компютърната система изисква кодове и пароли. В случай, че лицата не ги дадат, то е необходимо да се извършат всички възможни действия на място, преди да се изземат устройствата. Възможно е лицата, намиращи се в помещението, доброволно да преотстъпят кодовете и паролите. В тези случай, специалистите – технически помощници проверяват дали те са правилни, като е възможно след това с тях отново да се достъпи, при допълнителен оглед на веществени доказателства.

IV. Последващ етап от разследването.

При промяна на интерфейса /компрометиран интерфейс/ в дадена компютърна система се установява от къде е достъпено до електронната поща на пострадалия/ от коя електрона поща/[6]. Проверява се от разследващите историята на влизанията на пощата на жертвата /проверява се за неоторизирани влизания в пощата на българското дружество/[7]. Възможно е да е компрометирана пощата на дружеството контрагент. Ако се установи това, провежда се кореспонденция с партньорските служби в съответната държава. Основният принцип, който е приложим е – следваме пътя на парите – къде са преведени. Прави се проверка по линия на банковите преводи. Възможно е да се сторнира преводът. Ако преводът е към трето лице се изследва въпросът – кой е титуляр на сметката, за т.нар. „финансово муле“ ли се касае, през колко сметки са преминали парите и т.н. Може да се изисква информация и от доставчиците на компютърно-информационни услуги[8]. Видно е, че едно разследване с международен елемент изисква партньорството на различни служби, като е необходимо съобразяване както с международното, така и с вътрешноправното /националното/ действащо законодателство.

[6] Обикновено се касае за достъпване на електронната поща на някакво дружество.

[7] В много случаи е необходимо да се проследи хронологията от интернет браузъра /GOOGLE CROME, FIREFOX, MOZILLA и др./ С тях обикновено се достъпва до интернет. Как се установява дали има хакване? За всеки един сайт може да се установи кой го поддържа /администратор на сайта – системният администратор/. След като се установи това обстоятелство – изисква се съответната информация. Whois.domaintools.com – съдържа се информация за сайта, за „ай пи“ адрес и т.н.

[8] Вж. чл. 93, ал.1, т. 23 от НК: „Доставчик на компютърно-информационни услуги“ е всяко юридическо или физическо лице, което предлага възможността за комуникация чрез информационна система или което обработва или съхранява компютърни данни за тази комуникационна услуга или за нейните ползватели;

V. Разпит на свидетели, пострадали и обвиняем. Назначаване на криминалистични и други видове експертизи.

Разпитът на различни лица при разследването на компютърните престъпления следва да бъде извършен след предварителна подготовка от страна на разпитващия.[9] Това е необходимо, тъй като се касае за строго специфична материя, при разследването на която следва да бъдат прецизирани задаваните въпроси, след предварително проучване на наличните на този етап събрани доказателства по делото.

За целта на разследването могат да се назначат различни компютърно-технически експертизи – софтуерна, хардуерна, информационна и т.н. които да дадат отговор на поставените въпроси. При изготвянето на експертизите експертът може да възстанови и файловете, които са били изтрити от твърдия диск. Възможно е да се назначат и класически криминалистични експертизи – дактилоскопна, ДНК, графическа и др. При необходимост може да бъде назначена всякаква експертиза, чието заключение да допринесе за изясняване на фактическата обстановка – видеотехническа, лицево-идентификационна, психиатрична, стоково-оценъчна и т.н.

В заключение – развитието на дигитализацията обуславя все по-нови форми на престъпни посегателства. За съжаление, въпреки безспорните достойнства на изкуствения интелект, на мнение сме, че използването му за осъществяване на престъпни намерения ще затрудни тяхното разследване. Успешното противопоставяне изисква повишаване на подготовката на правоохранителните органи, призвани да се борят срещу този род престъпления в сферата на компютърните технологии.

VI. ИЗПОЛЗВАНИ ИЗТОЧНИЦИ:

[1] Конституция на Република България;
[2] Наказателен кодекс;
[3] Наказателно-процесуален кодекс;
[4] Закон електронните съобщения;
[5] Закон за европейската заповед за разследване;
[6] Владова-Недкова, И. Разследване на компютърни престъпления, С., 2023;
[7] Дончева, Д. Компютърни престъпления по Глава девета „а“ от Наказателния кодекс, Правна мисъл № 2, 2003, стр. 98-106;
[8] Павлов, Хр. Използване на специални компютърни знания при разследване на компютърни престъпления, Бургас, 2018; стр. 100-102;
[9] Бързинска, Цв. Полицейската регистрация в светлината на Решение на Съда на ЕС, пети състав от 26.01.2023 г. по дело C-205/21, Сборник с доклади от ЮМНК, ВУСИ, Пловдив, 2023, стр. 35-53;

[9] За подр. вж. Павлов, Хр. Използване на специални компютърни знания при разследване на компютърни престъпления, Бургас, 2018, стр. 100-102.