Компютърни технологии, международно право и международни отношения

КОМПЮТЪРЪТ – МОЩНО СРЕДСТВО ЗА УСЪВЪРШЕНСТВАНЕ НА ПРАВНИТЕ ОТНОШЕНИЯ И ИЗТОЧНИК ЗА ИЗВЪРШВАНЕТО НА ИЗМАМИ

Гергана Атанасова

I. Създаване и усъвършенстване на компютъра

Преди да изтъкнем огромното значение на компютъра, едно от откритията на XX в., което извърши еволюция в развитието на обществените отношения, и да разкрием някои от формите на злоупотреба с компютърната информация, е необходимо да споменем голямата заслуга на неговите създатели.

С гордост трябва да отбележим, че не друг, а американският гражданин от български произход – физик, математик и електроинженер, Джон Атанасов чрез разработването на първия автоматичен електронен дигитален компютър направи откритие, дало нов облик на обществените отношения и променило същността на документооборота.[1] Изобретението е разработено в периода 1937 – 1941 г. в Държавния колеж на Айова, САЩ, където по това време Атанасов е професор по физика и математика. В своята практическа работа бележитият учен е подпомаган от Клифърд Бери – един от най-талантливите студенти на колежа. Двамата построяват прототип на новата изчислителна машина, който по-късно ще стане известен като компютър на Атанасов – Бери (Atanasoff – Berry Computer ABC). Втората световна война обаче спира развитието на проекта, като откритията на Джон Атанасов остават непатентовани. Това е причината да възникне съдебен спор относно откритието на компютъра. Джон Мокли и Джон Екърт претендират, че са създатели на първата електронна изчислителна машина, наречена ENIAC, и патентоват своята разработка. След дълъг съдебен процес, на 19 октомври 1973 г., Федералният съд на САЩ постановява, че Екърт и Мокли "не са изобретили първия автоматичен електронен дигитален компютър, а вместо това се извлекли

[1] Вж. Христо Протохристов, "Създателят на първия модерен компютър – по случай 100-годишнината от рождението на проф. Джон Атанасов", достъпна на www.inrue.bas.bg

същността му от Джон Атанасов"[2], т.е. в концепцията на ENIAC се съдържат изобретенията на Джон Атанасов.[3]

Пред Федералния съд в САЩ Джон Атанасов обобщава своето откритие относно компютъра като заявява: "Аз стигнах през зимата на 1937 г. до **четири решения относно моя проект за компютър:**

- за работа на компютъра ще се използва електричество и електроника;
- въпреки традицията, ще се работи с двоична система за изчисление;
- като запомнящи устройства ще се използват кондензатори, но регенеративни – с периодично възстановяване на записаната информация, за да се избегнат малките грешки;
- изчисленията ще се извършват по пътя на преките логически действия.

Сега съм удивен, но и удовлетворен от това, че всяко от моите четири решения се използва при конструирането на съвременните компютри".[4]

Откритието на Джон Атанасов поставя началото на бурното развитие на компютърната индустрия през следващите десетилетия. Последвалите разработки във връзка с компютърните технологии се основават на фундаменталното откритие на американския учен от български произход и водят до усъвършенстването на цифровия компютър и приспособяването му към нуждите на практиката. Те правят възможно извършването на широк кръг от операции от компютъра и по този начин обуславят приложението му във всички сфери на обществения живот.

През 1945 г. Джон фон Нойман лансира идеята за въвеждане на програма в паметта на компютъра като усъвършенства технологията на работа на компютъра.[5] Дотогава електронният компютър също е бил програмиран, но програмата се е създавала отвън. Това е друго еволюционно откритие по пътя към създаването на съвременния компютър. Като съществено откритие, свързано със съвременните компютърни технологии, трябва да отбележим и създаването на персоналния компютър и разработването на програми за него от американския програмист Бил Гейтс.[6]

---

[2] Пак там.

[3] Един от създателите на ENIAC – Джон Мокли, заимства принципа на работа на електронния дигитален цифров компютър при гостуването си в дома на Атанасов през 1940-41 г., когато двамата подробно обсъждат конструкцията на компютъра. Създателят. www.inrue.bas.bg

[4] Вж. сп. ЕИМ-свят, "Джон Атанасов – създателят на компютъра", юли 2001 г.

[5] Вж. " Христо Протохристов, цит. Същ.

[6] Биография на Бил Гейтс – достъпна на www.microsoft.com

Компютърът е проницателно технологично откритие, което съществено променя начина на създаване, ползване, обработване, съхраняване и разпространение на информацията. Откриването на компютъра преобразява съществуващите до този момент разбирания за работа с данни, създаване на документи и търсене и анализ на информацията. Информацията, която се съхранява в компютъра, е в електронна форма. Всичко в тази електронна (дигитална) технология представлява верига от байтове и следователно обичайната форма на документа не намира приложение. За записване на информацията в компютъра се използва т.нар. **двоичен код** на цифрите 0 и 1.

С различни комбинации от тези цифри се записват букви или цифров текст. Следователно информацията, обработвана от компютъра, е представена в цифров (дигитален) вид, докато класическият документ се съставя **чрез изписване върху хартия** на букви от съответната азбука и цифрите от 0 до 9. Това са два качествено различни механизма за представяне на информацията, които обуславят и други съществени различия между класически и дигитално представената информация.

Именно електронният характер на информацията, обработвана чрез компютъра, обуславя възможности, които хартиеният документ не притежава. Електронната информация притежава редица предимства пред хартиения документ, водещи до ускоряване, облекчаване и повишаване ефикасността на процеса на умствен и физически труд, на вземане на управленски и други решения.

Създаването на компютъра ограничи използването на всички останали технологии за производството на документи. В съвременните общества компютрите са в основата на производсвото на документи.[7] Компютърът гарантира бърз и евтин обмен на информацията без оглед на обема и разстоянията.

В паметта на компютрите може да се съхранява огромно количество информация, която да бъде възпроизвеждана неограничен брой пъти. Компютърните системи притежават възможности да генерират дори повече информация, отколкото можем да обработим.

Цялата информация, която веднъж е запазена в компютъра, остава в неговата памет. Дори и когато бъде изтрита, тя може да бъде възстановена.[8] Веднъж унищожен, оригиналът на хартиения документ, който също е носител на информация, не може да бъде възстановен. Предишните версии на електронната информация, автоматично съхранени и скрити от компютърната програма, могат да бъдат открити и възстановени.[9] Възможно е информацията, съхранявана в компютъра, да се раздели в

---

[7] The Future of Documents. http://en.wikipedia.org/wiki/document

[8] **Bruse, Duyshart** The Digital Document www.elsevier.com

[9] **Medford, N. J.** What is a digital document?, Information Today, 1998.

различни файлове и в такава форма тя ще бъде съхранена и защитена и ще може лесно да се ползва.[10]

Много съществена характеристика на информацията, съдържаща се в паметта на компютъра, се изразява в това, че тя често представлява **база от данни**, т. е. структурирана информация, която може да се обработва и анализира за вземане на управленски решения, разработване на стратегии и програми. Базата от данни притежава функцията "търсене и анализ" (т. нар. търсачка), което позволява и изготвянето на справки по даден проблем. Базата от данни архивира и съхранява огромен обем от информация. Класическият хартиен документ не притежава такива възможности. Извършването на такива операции (търсене и анализ) при използването на класически документи отнема много време и средства и трудно може да обхване необходимия обем от информация.

Благодарение на откритията на Джон Атанасов и на неговите последователи, които усъвършенстваха цифровия компютър, се стигна и **до създаването на най-съвършената форма на документа – електронния документ.** Характеристиките на електронния документ качествено измениха съдържанието на понятието "документооборот", тъй като са свързани с възможности, които хартиеният документ не притежава.

Електронният документ спестява на държавните органи и на гражданите голяма част от времето и разходите, необходими за създаването и използването на документа. Електронният документ се създава по-бързо и по-икономично от хартиения. Чрез него се спестяват време и средства, необходими за създаването на документа. Електронното предаване на информацията увеличава сигурността в документооборота, като изключва загубата на документи при изпращането им.[11]

II. Злоупотреба с компютърната информация и необходимост от нейната защита

Макар че компютърът е създаден с цел да бъде в услуга на обществото, в процеса на неговото усъвършенстване се извършват редица злоупотреби с компютърната информация, компютърните мрежи и системи. Това поражда необходимостта от използването на специални средства за защита на информацията в компютъра, именно – създаването на потребителски (доверителни) системи, развитие на биометрични уреди, създаване на продукти за защита на компютърните мрежи (защитни стени,

---

[10] **Bruse, Duyshart** The Digital Document www.elsevier.com

[11] **Medford, N. J.** What is a digital document?, Information Today, 1998.

виртуални частни мрежи). В тази насока работят и редица държавни и международни организации.[12]

Ръстът на компютърните злоупотреби е свързан с развитието на компютърните системи и технологии. Колкото повече се усъвършенства компютърната обработка на данните, толкова по-големи възможности има за злоупотреба с компютърната информация. Разширяването на приложното поле на компютрите ги прави достъпни до широк кръг от хора и по този начин се увеличават възможностите за злоупотреба със съдържащите се в тях данни. Обстоятелството, че все повече хора ползват компютър, позволява те да експериментират, да изучават как работи и какви манипулации могат да се извършват с него. Това предоставя възможност и за проучване на начините за нерегламентиран достъп до информацията вътре в компютъра. Уязвимостта на компютрите се увеличава и от обстоятелството, че връзката и взаимодействието между тях се осъществява чрез мрежа. По този начин злоупотребата с един от компютрите, включени в мрежата, може да предизвика сериозна верижна реакция в другите системи. И ако по-рано един нарушител е можел да повреди само един компютър, една локална мрежа или една инсталация, с разпространението на компютърните мрежи върху големи територии вече е възможно едно лице да разруши работата на правителствени учреждения, цели национални компании или интернационални организации и фирми.

Ето защо първите компютри не са предоставяли особено големи възможности за злоупотреба с компютърната информация. Те са били много големи, скъпо струващи и много малко разпространени.[13] Такива компютри са притежавали само правителствени организации и големи фирми. Това е ограничавало възможностите за злоупотреба с компютърната информация. Дори програмистите не са знаели как да тестват написаните от самите тях програми. Това правели инженерите, създали дадения компютър.[14] Именно поради незнание външните потребители не са имали възможност да злоупотребяват със съществуващите тогава компютърни технологии. Поради това на този етап от развитието на компютъра не е имало възможност за злоупотреба с компютърните технологии в съвременния смисъл на това понятие и

---

[12] По-подробно вж. **Синягина, Н.; Мирчев, И.; Дамянов., И; Христов, С**., Защита на компютърната информация; изд. на ЮЗУ "Неофит Рилски"; 2005; с. 22.

[13] Конструираният компютър ENIAC е използван за балистични изчисления по време на Втората световна война, а по-късно и за проверка на конструкцията на водородната бомба. Тежал е 30 тона и е работил с 18000 радиолампи. Британският компютър Colossus пък е използван за разработване на вражески кодове отново по време на Втората световна война – IBM PC 20 години по-късно. www.newtesk.bg.

[14] **Синягина, Н.; Мирчев, И.,; Дамянов., И; Христов, С.**, Цит. съч., с. 18.

защитата на компютърната информация се е осъществявала предимно чрез физическа защита на компютрите (аларми, пазачи, специални сгради).[15]

През 60-те и 70-те години на миналия век се създава третото поколение компютри, при които технологиите са значително изменени. Компютрите се изграждат на базата на интегрални схеми. Конструират се компютри, работещи в режим time-sharing, при който потребителите вече могат да работят непосредствено с компютъра.[16] В резултат на това възникват възможности за злоупотреби и от страна на потребители. Така се появяват по-сериозни проблеми, свързани със защитата на компютърната информация.

След 70-те години на XX в. се развива и възможността за достъп до компютрите от отдалечени места, което се постига благодарение на усъвършенстване на телекомуникациите. В резултат на това възникват възможности за съвместна употреба на програми и данни от различни потребители. Това още повече усложнява процеса на компютъризация и предоставя нови възможности за злоупотреба с компютърните данни.

Големите фирми, най-вече банките, започват да извършват транзакции он-лайн, ползвайки бази от данни. Появяват се **т.нар. мини компютри**. За първи път се появяват констатации за компютърна престъпност, но все още компютърните престъпления имат незначителен дял в ръста на престъпността.

Следващ еволюционен етап в разширяването на приложното поле на компютъризацията, благоприятстващ и злоупотребите с компютърните технологии, е **разпространението на персоналния компютър**. Персоналните компютри получават широко разпространение в края на 70-те и началото на 80-те години на миналия век и са достъпни за хора от всички възрасти и професии в цял свят.[17]

Доказателство за усъвършенстването на нерегламентираните манипулации с компютърни данни е и обстоятелството, че на този етап от развитието на компютърните технологии се появяват и **първите вируси**. През 1988 г. е създаден първият компютърен червей (worm)[18], който се разпространява чрез Интернет, като само в САЩ са заразени 6000 компютъра. Червеят "тръгва" от Масачузетския технологичен институт (MIT), след това поразява компютърни системи в Кембридж, Калифорния,

---

[15] Пак там.

[16] Пак там.

[17] Първият прототип на персонален компютър е създаден от Алан Клен пред 1973 г., но Altair е първият масов персонален компютър /1974 г./. През 1981 г. американската компания IBM пуска за масова употреба серия от модели на произведени от нея персонални компютри – http://bg.wikipedia.org/wiki/PC

[18] **Синягина, Н.; Мирчев, И.,; Дамянов., И; Христов, С.**, Цит. съч., с. 20; **Копчева, М.** Компютърни престъпления, изд. Сиби, 2006; с. 12.

Лос Аламос, Пътсбърг.[19] И преди разработването на компютърния червей е имало случаи на заразяване на компютри от вируси. За разлика от тези вируси обаче Интернет-червеят е първият регистриран червей, разпространен по мрежата, който е имал потенциал да блокира голяма част от световноизвестните компютърни инсталации. Този вирус се размножава много бързо като използва грешки в кода на съответните програми и операционни системи. През този период се разработват и други вируси, чието разпространение обаче не е толкова мащабно, както на червея от 1988 г. През 1987 г. т.нар. Хаус клуб в Западна Германия създава вирус, който прониква и заразява компютрите на НАСА. През 1988 г. студент от Йерусалимския университет създава "троянски кон" и "бомби".[20]

Компютърните злоупотреби се увеличават значително в началото на 90-те години на XX в. Тогава се създават т.нар. отворени системи и големи бази от данни, което значително увеличава рисковете по отношение на компютърната безопасност. Вече широко се употребява световната информационна мрежа Интернет и предоставянето на услуги по електронен път.

Нарастването и усъвършенстването на злоупотребите с компютърните системи и технологии поражда необходимост от специални средства за защита на компютърната информация. Създават се специализирани механизми за защита на компютърните информационни данни: потребителски (доверителни) системи, биометрични уреди, продукти за защита на компютърните мрежи (защитни стени, виртуални частни мрежи). В тази насока работят и редица специализирани държавни и международни институции. Държавни организации в тази област са Computer Emergency Response Team (CERT) и National Security Agency (NSA). С проблемите на компютърната защита се занимават и известни международни организации като American Bankers Association (ABA); American National Standard Institute (ANSI); Institute of Electrical and Electronics Engineers (IEEE) и др.[21]

В процеса на усъвършенстване и защита на компютърната информация се разработват и внедряват и редица международни стандарти. Основните стандарти в тази област са разработени в т.нар. Оранжева книга (Orange book). Това е сборник от критерии за оценка на сигурността на компютърната информация, разработен от Националния център за защита

---

[19] Компютърният червей е разработен и разпространен от Робърт Морис – аспирант в Корнелския университет. За деянието си той бил осъден на 3 години лишаване от свобода, глоба от 10000 долара и 400 часа общественополезен труд – www.soft-press.com – Интернет червеят от 1988 г.

[20] **Синягина, Н.; Мирчев, И.,; Дамянов., И; Христов, С.**, Цит. съч., с. 20.

[21] **Синягина, Н.; Мирчев, И.,; Дамянов., И; Христов, С.**, Цит. съч., с. 20; **Копчева, М.**, Цит. съч., с. 22.

на компютрите (National Computer Security Center – NCSC). Оранжевата книга регламентира основните положения при изграждане на системите за защита и до днес се използва от специалистите в тази област. През 1990 г. в Германия е разработен стандарт, известен като Бялата книга.[22] Този стандарт обаче в голямата си част възпроизвежда Оранжевата книга.

Специализираната защита на компютърните технологии се усъвършенства и в технологично отношение. От края на миналия и началото на настоящия век се създават предимно такива продукти за защита, които да станат част от самите компютърни програми и да предпазват информацията в компютъра от всякакъв вид неоторизиран достъп.

III. Правна защита срещу компютърната престъпност

Актуалността, важността и значимостта на проблема за компютърната престъпност в съвременността са безспорни и това се обуславя от няколко съществени обстоятелства.

Първо, компютърните престъпления накърняват **съществени обществени отношения –** те засягат икономиката; отношенията, свързани със създаването, ползването и опазването на документите и др. В този смисъл компютърните престъпления накърняват управленската, научно-изследователската и др. видове сложна и отговорна човешка дейност. Жертви на тези престъпления са предприятия, учреждения и организации, които използват компютри в своята работа. Посочените негативни резултати се дължат на широкото приложно поле на компютрите в дейността на човека. Именно достъпността им увеличава възможностите за злоупотреба с компютърната информация, защото предоставя възможност за изучаването на компютърните технологии и използването на техните възможности за неправомерен достъп до компютърните информационни данни.

На второ място, спецификата на компютърните системи и технологии обуславя и **специфичните особености на компютърните престъпления.** Компютърната измама накърнява **и специфични за този вид престъпност обществени отношения** – отношенията, свързани със законосъобразното създаване, ползване, заличаване или изтриване на компютърни информационни данни. Техен **предмет** могат да бъдат компютърни информациони данни; **средство** за извършване на престъплението може да бъде внасянето, заличаването или изтриването на компютърна информация и др. Всичко това изисква установяването на самостоятелна правна уредба на тази категория престъпления, която предоставя възможност да се вземат предвид техните специфични

[22] Пак там.

особености. Това позволява и да се обособи самостоятелна съдебна практика в областта на компютърната престъпност, която да обогати достиженията на наказателноправната наука в тази сфера. Освен това развитието на компютърната престъпност поставя и изскване правоприлагащите органи да притежават качествено нови знания.

Трето, наред със сериозността на обхвата на компютърната престъпност **огромен е и размерът на вредите за стопанството от тези престъпления.** Ежегодните загуби на националните икономики от компютърна престъпност се оценяват на: за САЩ – 100 млрд. долара; за Великобритания – 4,45 млрд. долара; за страните от Западна Европа – 30 млрд. долара.[23]

Четвърто, неправомерният достъп до компютърна информация се използва и за извършването на други престъпления. Организираната престъпност използва все повече различни технически средства – от обикновени персонални компютри до глобални информационни мрежи, вкл. и Интернет. Практически всеки втори подправен паричен знак се изготвя при използване на компютърна обработка и разпечатка на цветен принтер.[24]

Пето, възможностите на компютърните технологии позволяват **дистанционно извършване на престъпленията**, без да е необходимо физически да се проникна в помещенията на учреждения, предприятия и организации, за да се получи достъп до съответната база от данни. "Нематериалният" обмен на информацията чрез компютърните технологии допълнително усложнява разкриването и разследването на престъплението.

Въпреки разработването и прилагането на специализирани средства за защита на компютърната информация, злоупотребите в тази област не могат да бъдат преодолени. Сериозността на тези проблеми е толкова голяма, че защитата на съответните категории обществени отношения се осъществява от най-съвършения механизъм за защита на обществените отношения – правото. Поради това наказателното право е мощно средство за борба с компютърната престъпност, тъй като предоставя възможност **за санкциониране на компютърните престъпления.** Целта на институционализирането на компютърните престъпления е именно в това те да се обвържат с **определени правни последици,** които се изразяват в налагането на наказание при осъществяване на състава на съответното компютърно престъпление. Докато непозволеният достъп до данните в компютъра не може да бъде санкциониран по силата на съответните технически правила, то наказателното право предвижда санкция за тези деяния. Поради това обособяването на компютърните злоупотреби като

[23] Казанцев, В. В. Криминалистическое исследование средств компютерных технологии и програмных продуктов – http://allpravo.ru/library/doc5195p0/instrum5196/item5199.html
[24] Пак там.

самостоятелна категория престъпления е основната предпоставка за постигането на по-голяма ефективност в борбата с този род неправомерни деяния. Посредством регламентирането на компютърни престъпления в наказателното право в този клон на правото се институционализира и **нов вид престъпност**, непозната на законодателя преди създаването и разпространението на съвременния компютър.

IV. Компютърна измама по чл. 212а НК на Република България

Компютърната престъпност и законодателната уредба на компютърните престъпления в нашата стана възникват много по-късно, отколкото в западноевропейските държави и САЩ. Въпреки че до демократичните промени България е водеща държава в Източния блок в създаването на компютърни технологии, те не намират широко приложение в практиката. До 1989 г. у нас не е развито използването на компютри нито в отделните стопански отрасли, нито в административната сфера.[25]

С преминаването на Република България към демократична форма на управление и пазарно стопанство все повече се разширява приложното поле на компютърните системи и технологии. Те се превръщат в неизменна част от дейността на държавните институции, частния бизнес, компютри се използват и от отделните домакинства.

Въпреки това едва през 2002 г. се криминализират проявите, засягащи нормалното функциониране на компютърните системи и технологии. До този момент престъпните деяния, при които компютърът е предмет и средство за извършване на престъпление, са квалифицирани като документни престъпления, длъжностни присвоявания, документни измами и др., без да се отчитат специфичните особености на компютърното престъпление.

През 2002 г. в България е приет Закон за изменение и допълнение на Наказателния кодекс (ДВ, бр. 92/2002 г.), с който **за първи път** се уреждат **компютърните престъпления.** Новите престъпни състави са уредени в самостоятелна глава IX "а" от Особената част на Наказателния кодекс – "Компютърни престъпления". Извън тази глава са уредени няколко престъпления, които също са свързани с компютърните технологии и при които се използват възможностите на компютъра. Отделни състави на компютърни престъпления са уредени и в глава III от Особената част на НК – гл. II – "Престъпления против личността" – разпространение в Интернет на материали с порнографско съдържание по чл. 159, ал. 1; "Престъпления против правата на гражданите" – компютърно пиратство по чл. 172, ал. 2;

---

[25] Първото компютърно престъпление в България е установено едва през 1983 г. – касиерка на Балкантурист – София извършва крупно присвояване на парични суми – вж. Бобев, К., Криминалистика, Унив. издателство "Св. Кл. Охридски", 2001, с. 229.

гл. V – "Престъпления против собствеността", р. IV – "Измама" – **компютърна измама по чл. 212а**; гл. VI – "Престъпления против стопанството", р. IV – "Престъпления против паричната и кредитната система" – предварителна дейност за подправяне на парични знаци чрез компютърни програми по чл. 246; гл. IX – "Документни престъпления" – лъжливо електронно деклариране по чл. 313.

Следователно двата основни състава на компютърната измама са уредени в чл. 212а от особената част от Наказателния кодекс: "Който с цел да набави за себе си или за другиго облага, възбуди или поддържа заблуждение у някого като внесе, измени, изтрие или заличи компютърни информационни данни или използва чужд електронен подпис, и с това причини на него или на другиго вреда, се наказва за компютърна измама с лишаване от свобода до 6 години и глоба до 6000 лева." (чл. 212а, ал. 1)

Тъй като компютърната измама е уредена в гл. V – "Престъпления против собствеността", р. IV "Измама" от особената част на НК и като се имат предвид съответните признаци на състава на престъплението, а именно, че компютърната измама може да се извърши с користна цел и че нейният престъпен резултат се изразява в причиняването на вреда, се прави изводът, че обект на компютърната измама са обществените отношения, които се засягат с традиционните престъпления против собствеността (кражба, грабеж и др.), а това са отношенията, които гарантират нормалното осъществяване на правото на собственост върху движими или недвижими вещи. С оглед на особения начин или метод, който се използва за възбуждане и поддържане на заблуждение при компютърната измама (внасяне, заличаване, изменение или изтриване на компютърни информационни данни), следва, че компютърната измама засяга и един специфичен кръг от обществени отношения – отношенията, свързани със законосъобразното създаване, ползване или заличаване на компютърните информационни данни. Следователно компютърната измама е престъпление с два обекта.

Предмет на престъплението по чл. 212а, ал. 1 са компютърни информационни данни, за които е дадено легално определение в чл. 93, т. 22 от НК. Съгласно тази норма компютърни информационни данни е всяко представяне на факти, информация или понятия във форма, поддаваща се на автоматична обработка, включително такава програма, която е в състояние да направи така, че дадена компютърна система да изпълни определена функция.

Не може да се приеме, че измаменото лице също е предмет на престъплението.[26] Въздействието върху измаменото лице (възбуждането и поддържането на заблуждение у него чрез внасяне, изменение, заличаване

[26] Вж. **Стойнов, Ал.**, Престъпления против собствеността, Сиби, 2003 г., с. 159.

или изтриване на компютърни информационни данни) е само специфичен метод или начин на осъществяване на изпълнителното деяние на престъплението. Мотивирането на измаменото лице да извърши акт на имуществено разпореждане се включва в изпълнително деяние на компютърната и на другите видове измама по р. IV, гл. V от особената част на НК. Мотивирането обаче се осъществява по специфичен начин на възбуждане и поддържане на заблуждение. При компютърната измама това се постига чрез специфични манипулации, а именно чрез внасяне, изменение, заличаване или изтриване на компютърни информационни данни или използване на чужд електронен подпис. Ето защо не е правилно да се посочва, че измаменото лице е предмет на престъплението, тъй като то търпи съответното престъпно въздействие. Предметът на престъплението по чл. 212а, ал. 1 от НК е изрично посочен като признак на престъпния състав. Посредством въздействието върху компютърните информационни данни биват увредени именно обществените отношения, които гарантират законосъобразното манипулиране с компютърната информация.

Изпълнителното деяние на компютърната измама има две форми. Те се изразяват във **възбуждане или поддържане на заблуждение у определено лице. Заблуждението** е неправилната представа у измаменото лице относно определени факти или обстоятелства от обективната действителност и по-конкретно относно правното основание или условията, при които измаменият трябва да осъществи определено правно действие или бездействие. **Възбуждането на заблуждение** е такова въздействие върху съзнанието на измамения, което формира у него неправилните представи. **Поддържането на заблуждение** предполага вече формирани неправилни представи у измаменото лице относно правното основание или условията, при които ще се извърши имуществено разпореждане. Изисква се също така тези представи да не са формирани в съзнанието на измаменото лице със съдействието на дееца. Заблуждението трябва да е възникнало без участието на субекта на престъплението. При поддържане на заблуждение "деецът проявява активност с цел утвърждаване на една невярна представа и има определен принос за заблуждението."[27] Следователно в резултат на дейността на извършителя се задълбочава неправилната представа у измаменото лице. То добива още по-голяма увереност, че неговите неверни представи относно определени обстоятелства съответстват на действителността.

Възбуждането и поддържането на заблуждение са форми на изпълнителното деяние и при класическата измама. Характерен за компютърната измама е специфичният начин за осъществяване на

[27] Вж. р. 555-87-ВС.

изпълнителното деяние – чрез неправомерна промяна на съществуващи компютърни информационни данни (внасяне, изменение, заличаване или изтриване) или използване на чужд електронен подпис.

Внасянето на компютърни информационни данни представлява въвеждане на данни в компютърната система или мрежа. Те могат да бъдат въведени ръчно или чрез използване на друга компютърна система, свързана с предмета на престъплението. По този начин се увеличава съществуващият информационен масив и при осъществяване на заложена операция програмата използва и данни, които са отсъствали от системата при създаването на програмата.

Изменението на компютърни информационни данни е друг начин за осъществяване на изпълнителното деяние на престъплението, при който отделни елементи от информационния масив или съществуващата програма се променят в сравнение с тяхното състояние при първоначалното им залагане.

Изтриването на компютърни информационни данни намалява количеството на информационния масив като се премахват елементи от него или се премахват елементи от дадена компютърна програма, съществували при създаването им. При изтриването на данни от компютъра е възможно да бъде възстановена, макар и много трудно, първоначалната им достъпност до потребителя.

При **заличаването** на компютърни информационни данни се премахват данни от носителя им. За разлика от изтриването, при заличаването данните не могат да бъдат възстановени.

Другият начин за възбуждане и поддържане на заблуждение е използването на чужд електронен подпис. Самият електронен подпис е вид компютърни информационни данни. Следователно по своята същност използването на чужд електронен подпис е внасяне на данни в дадена компютърна система. Този извод се налага от легалното определение на електронния подпис, дадено в чл. 13, ал. 1 от Закона за електронния документ и електронния подпис. Следователно при използването на чужд електронен подпис в компютърната информационна система се въвеждат данни, които идентифицират определен правен субект, различен от дееца. По този начин се създава неправилната представа у определено лице, че електронното изявление принадлежи на лицето, което се идентифицира с данните от подписа, а не на лицето, действително направило изявлението. Така се създава неистински електронен документ. Това следва от легалното определение за неистински документ (чл. 93, т. 6 от НК).

От обективна страна компютърната измама се характеризира и с поведението на измаменото лице. Под влиянието на неправилните представи относно действителността измаменият осъществява действие или бездействие с правно значение, в резултат на което сам търпи или

причинява вреда на трето лице. Поради това пострадало от престъплението може да бъде както измаменото лице, така и друго физическо или юридическо лице.

Компютърната измама по чл. 212, ал. 1 от НК е резултатно увреждащо престъпление – съставът на престъплението изисква да е настъпила вреда. В закона не се посочва изрично какъв е характерът на вредата. Следва да се приеме, че престъпният резултат може да бъде не само причиняване на имуществени вреди, но и съчетание от имуществени и неимуществени вреди.

Признак от обективната страна на състава на престъплението е особената **причинна връзка**, която съществува между деянието и престъпния резултат. Тя се опосредява от поведението на измаменото лице. Престъпният резултат (причиняването на вредата) е пряка последица от имущественото разпореждане, осъществено от измаменото лице. Но разпореждането от своя страна е следствие от неправилната представа на измаменото лице относно правното основание или условията на това разпореждане. А тази неправилна представа е формирана, поддържана или използвана посредством осъществяването на изпълнителното деяние на престъплението (възбуждане, използване или поддържане на заблуждение чрез неправомерно манипулиране с компютърни информационни данни).

Субектът на престъплението е "общ" и може да бъде всяко наказателноотговорно лице.

От субективна страна е характерно, че престъплението се извършава само с пряк умисъл.

Вторият основен състав на компютърната измама е уреден в чл. 212а, ал. 2 от НК: "Същото наказание се налага и на този, който без да има право, внесе, измени, изтрие или заличи компютърни информационни данни, за да получи нещо, което не му се следва."

Изпълнителното деяние на престъплението се изразява само в незаконното манипулиране с компютърни информационни данни, а не и във възбуждането и поддържането на заблуждение у определено лице, което е изпълнителното деяние на компютърната измама по чл. 212а, ал. 1 НК. Поради това съставът на ал. 2 е формулиран по-широко и обхваща всички случаи на неправомерна промяна на компютърни информационни данни. Когато тази промяна е начин за възбуждане или поддържане на заблуждение у определено лице, тогава се осъществява съставът по чл. 212а, ал. 1 НК.

Предмет и на това престъпление са компютърни информационни данни.

Престъпният състав по ал. 2 поставя изрично изискването субектът **да няма право** да извършва съответните манипулации с компютърните данни. За престъплението по ал. 1 не се поставя изрично такава изискване,

но то трябва да е налице, за да се квалифицира деянието като престъпление. Това е напълно логично, защото, за да бъдат формирани или поддържани определени неверни представи у едно лице, които да го мотивират към извършване на акт на имуществено разпореждане, манипулирането с компютърните информационни данни трябва да противоречи на изискванията на закона. Ако манипулирането е законосъобразно, то няма да е от естество да възбужда или поддържа заблуждение у определено лице.

Посоченият признак от обективната страна на състава на престъплението означава, че лицето не трябва да е оправомощено според действащото законодателство да извършва съответните манипулации с компютърни информационни данни.

Компютърната измама по ал. 2 е резултатно престъпление. При осъществяване на изпълнителното деяние (внасяне, изменение, заличаване или изтриване) се променя съществуващият информационен масив. Ето защо престъпният резултат настъпва веднага след довършване на изпълнителното деяние.[28] Други автори споделят становището, че компютърната измама по ал. 2 е формално престъпление. То е довършено с осъществяване на изпълнителното деяние.[29] Трябва обаче да се има предвид, че с извършването на изпълнителното деяние настъпват неправомерни промени в съществуващите компютърни информационни данни и именно те са резултат от престъпното деяние. Не е възможно да бъдат извършени съответните манипулации, без да бъдат засегнати неправомерно данните, съдържащи се в компютъра.

И при двата престъпни състава от субективна стана като форма и вид на вината законът изисква **пряк умисъл**. И при двата престъпни състава деецът преследва особена цел. За престъплението по чл. 212а, ал. 2 тази цел се изразява в получаването на нещо от дееца, което "не му се следва", т. е. в получаването на облага (предимно материална, но може и неимуществена), която деецът няма право да получи. Поначало тази облага има имуществен характер, което е отразено и в самия термин "получи". Този термин предполага, че облагата има материален характер – това могат да бъдат вещи, пари, носител на компютърни информационни данни. Но формулировката на закона не изключва възможността и целената облага да има неимуществен характер.

Субектът на престъплението е "общ". Това може да бъде всяко наказателноотговорно лице. Субекти на престъплението могат да бъдат както лица, които имат право да извършват съответните действия с компютърни информационни данни, но осъществяват манипулации, които

---

[28] Вж. **Стойнов, Ал.**, Цит съч., с. 165.
[29] Вж. **Копчева, М.**, Цит. съч., с. 104.

не са им разрешени от закона, така и лица с неразрешен от закона достъп до данните.

Заключение

Едно от еволюционните открития на XX в. – компютърът, твърде бързо се превърна и в предмет и средство за извършване на престъпления. Създадена, за да бъде в услуга на обществото, компютърната технология вече е и източник за извършване на измами. Компютърните данни са непознат досега на наказателното законодателство и наука предмет и средство за извършване на престъпление. Компютърната информация има качествено нова същност – специфичният начин на нейното създаване (в електронна (дигитална) форма, съхраняване (в паметта на компютъра), ползване и унищожаване (посредством компютърна обработка), обуславя и специфичния начин на злоупотреба с информацията в компютъра. Неправомерното манипулиране с данните се материализира по особен начин. Възможно е това да се извърши от разстояние – чрез свързване в компютърната мрежа от един компютър може да се проникне в данните на друг компютър. Не е необходимо физически да се преодоляват разстояния, прегради, да се проявява особена физическа активност, каквато е необходима при други видове престъпления – убийство, кражба, грабеж и др. Всички тези характеристики на електронното представяне на данните поставят много и сложни въпроси във връзка с правната уредба, разследването и разкриването на тази категория престъпления.