ПРАВНА УРЕДБА НА КОМПЮТЪРНИТЕ ПРЕСТЪПЛЕНИЯ ПО БЪЛГАРСКОТО НАКАЗАТЕЛНО ПРАВО

I. Обща характеристика на компютърните престъпления

1. Исторически бележки

Понятието "компютърни престъпления" се появява за първи в специализираната научна литература през 60-те години на XX век във връзка със случаите на незаконно използване на компютърни системи, компютърен саботаж и компютърен шпионаж. Първите по-задълбочени изследвания в областта на компютърните престъпления са публикувани през 70-те години на XX век, провокирани от появата на няколко мащабни случая на злоупотреби, свързани с използването на информационни технологии. По същото време много държави приемат специализирано законодателство в областта на защитата на личните данни, в което включват разпоредби, санкциониращи посегателства срещу такива данни, събирани, съхранявани и предавани по електронен път. Исторически това са първите законови разпоредби в областта на компютърните престъпления.

В края на 70-те и началото на 80-те години въпросът за санкционирането на компютърните престъпления придобива все по-широко значение в резултат на драстично увеличилите се случаи на посегателства, извършени посредством използването на компютърни системи. Появяват се първите случаи на хакерство, компютърни вируси, компютърни измами, софтуерно пиратство и др. По отношение на много от тези прояви традиционното наказателно законодателство се оказва неприложимо, което принуждава много държави да приемат нови разпоредби, инкриминиращи различни видове компютърни престъпления, преди всичко в сферата на икономическите отношения.

През 90-те години на XX век компютърните престъпления надхвърлят границите на икономическата престъпност и започват да засягат все по-широк кръг обществени отношения в сферата на държавното управление, административните услуги, здравеопазването, транспорта и др. Бързото развитие на Интернет като глобална информационна и комуникационна среда също поставя редица сериозни проблеми пред наказателната политика на отделните държави. Информационните технологии се превръщат в средство за осъществяване на престъпна дейност от организирани групи и в сериозен фактор от гледна точка на националната и международната сигурност.

Всичко това води до непрекъснат стремеж на държавите към усъвършенстване на правната уредба на компютърните престъпления и дава нов тласък в развитието на международното сътрудничество в тази област. Приемат се множество нови разпоредби в националното законодателство на отделните страни и стартират редица международни инициативи, насочени към уеднаквяване на вътрешната уредба и създаването на механизми за ефективно международно сътрудничество в борбата с компютърната престъпност.

2. Сравнително-правен анализ на уредбата на компютърните престъпления[1]

В Европа правна уредба на компютърните престъпления съществува във всички държави-членки на Европейския съюз, както и в Швейцария, Норвегия, Исландия, Унгария, Естония, Латвия, Малта и др. Компютърните престъпления са законодателно уредени още в Съединените щати, Канада, Мексико, Австралия, Нова Зеландия, а също и в отделни държави от Азия (Япония, Сингапур, Китай, Малайзия, Индия), Южна Америка (Бразилия, Чили, Венецуела) и Африка (Южна Африка, Тунис).

В повечето държави правната уредба на компютърните престъпления е включена в наказателните кодекси на съответните страни. От гледна точка на систематичното място на уредбата по-често съставите на компютърните престъпления са формулирани като квалифицирани състави на традиционни престъпления като измама, нарушаване на авторски права и др., които се отличават от основния състав по специалния начин на извършване на престъплението. По-рядко компютърните престъпления са обособени в самостоятелни раздели на наказателните закони (Бразилия, Естония). В сравнително малко страни компютърните престъпления са уредени в специални закони (Китай, Индия), а в отделни държави съществува паралелна уредба в два нормативни акта (Япония, САЩ).

В част от държавите, предимно тези, в които компютърните престъпления са уредени със специален закон, правната уредба включва легални определения на основните понятия, използвани при формулирането на съставите (компютър, компютърна система, компютърна мрежа, компютърна програма, компютърни данни и др.).

Повечето държави предвиждат сходни санкции за компютърните престъпления. Най-често срещаното наказание е лишаване от свобода за различен срок (от 3 месеца до 12 години) в зависимост от характера на посегателството и размера на причинените вреди. Наред с лишаването от свобода като алтернативно или кумулативно наказание сравнително често е предвидена и глоба, като нейният размер обикновено зависи от размера на причинените вреди. В Китай като наказание е предвидено лишаването от право на достъп до Интернет за определен срок.

Според наказателните закони на повечето държави компютърните престъпления са от общ характер. Единствено в Германия и Полша са предвидени случаи на компютърни престъпления, които се преследват по инициатива на пострадалия.

3. Международни инициативи за противодействие на компютърната престъпност[2]

---

[1] Вж. по-подробно за нормативната уредба на компютърните престъпления в други държави: *Законодателно проучване на тема "Компютърни престъпления"*, Програма "Студенти на стаж към парламента", София, юли 2001 г. Изследването обхваща вътрешното законодателство на всички държави-членки на Европейския съюз и правни актове на държави от Източна Европа, Азия, Северна и Южна Америка.

Първите стъпки в областта на международното сътрудничество за противодействие на компютърните престъпления са инициирани в рамките на Организацията за икономическо сътрудничество и развитие (ОИСР) през 1983 г., когато в рамките на организацията е създадена експертна комисия за проучване на компютърните престъпления и необходимостта, която те пораждат, от промени в наказателното законодателство на държавите-членки. Комисията подготвя пакет от предложения, въз основа на които ОИСР приема препоръка към държавите-членки да предприемат мерки, осигуряващи приложението на тяхното наказателно законодателство по отношение на определени категории компютърни престъпления. Предложенията на комисията включват и списък от актове, които могат да послужат като основа за сближаване на различните подходи, предприети от отделните държави-членки.

Най-съществен принос в развитието на международното сътрудничество в областта на компютърните престъпления има Съветът на Европа. На 13 септември 1989 г. Съветът на Европа приема Препоръка № R(89)9, която съдържа списък на минимума посегателства, които трябва да бъдат инкриминирани от държавите-членки с цел постигането на обща наказателна политика в областта на компютърните престъпления. На 11 септември 1995 г. Съветът на Европа приема втора препоръка, отнасяща се до наказателно-процесуалните аспекти на създаването и използването на информационните технологии.

През 1997 г. към Съвета на Европа е създадена Експертна комисия по престъпленията в кибернетичното пространство, която има за основна задача да изследва и дефинира новите престъпления, юрисдикцията на държавите и наказателната отговорност във връзка с комуникацията чрез Интернет. Въз основа на резултатите от работата на експертната група е подготвен проект за Конвенция за престъпленията в кибернетичното пространство, която е приета на 109 заседание на Комитета на министрите на 8 ноември 2001 г. и е открита за подписване на срещата в Будапеща, Унгария, на 23 ноември 2001 г. Конвенцията е подписана от Република България на 23 ноември 2001 г., но все още не е ратифицирана. Поради липсата на необходимия брой ратификации Конвенцията за престъпленията в кибернетичното пространство все още не е влязла в сила.[3]

Конвенцията за престъпленията в кибернетичното пространство на Съвета на Европа дава определения на основните понятия във връзка с компютърните престъпления и предвижда конкретни мерки, които държавите-членки трябва да предприемат на национално равнище в областта на материалното и процесуалното наказателно право. Конвенцията определя четири основни категории престъпления:

---

[2] Вж. по-подробно за международното сътрудничество за противодействие на компютърните престъпления: *The Legal Framework – Unauthorized Access to Computer Systems. Penal Regulation in 44 Countries (Updated October 4, 2002) by Stein Schjolberg, Chief Judge, Moss District Court, Norway*

[3] Съгласно чл. 36, ал. 1 от Конвенцията за престъпленията в кибернетичното пространство Конвенцията влиза в сила на първия ден от месеца, следващ изтичането на тримесечен период от датата, на която пет държави, между които най-малко три държави-членки на Съвета на Европа, са я ратифицирали. По данни на Съвета на Европа към 1 януари 2004 г. Конвенцията е подписана от 37 страни (33 държави членки на Съвета на Европа, Канада, Япония, Южна Африка и Съединените щати), но е ратифицирана единствено от Албания, Хърватия, Естония и Унгария.

правонарушения срещу тайната, неприкосновеността и възможността за ползване на компютърни данни и системи (незаконен достъп, незаконно прихващане, посегателство срещу неприкосновеността на компютърни данни и компютърни системи, злоупотреба с устройства), компютърни престъпления (компютърна фалшификация и компютърна измама), правонарушения, свързани със съдържанието (правонарушения, свързани с детската порнография) и престъпления, свързани с посегателства срещу авторското право и сродните му права (масово разпространение на пиратски копия на защитени творби и др.).

В областта на наказателния процес конвенцията съдържа правила относно бързото запазване на данните, съхранявани в компютърните системи, и на данните, свързани с трафика, реда за предоставяне на такива данни, претърсването и изземването на съхраняваните компютърни данни, събирането в реално време на данни за трафика и на данни, свързани със съдържанието.

В сферата на международното сътрудничество конвенцията въвежда няколко нови форми на сътрудничество в допълнение към традиционните механизми, предвидени в Европейската конвенция за екстрадиция и Европейската конвенция за взаимопомощ по наказателни дела. Предвидено е и създаването на постоянно действаща мрежа за контакти (т.нар. мрежа 24/7), която да осигурява съдействие при разследването на компютърни престъпления.

В края на 90-те години компютърните престъпления и преди всичко вредното и незаконно съдържание в Интернет стават обект на внимание и от страна на Европейския съюз. През април 1998 г. Европейската комисия представя на Съвета резултатите от проведено изследване на тема "Правни аспекти на компютърните престъпления в информационното общество", по-известно като изследването COMCRIME.[4] През октомври 1999 г. на срещата в Тампере, Финландия, Европейският съвет излиза със заключение, че престъпленията в областта на високите технологии следва да бъдат включени в усилията за уеднаквяване на дефинициите и санкциите. Европейският парламент също призовава за приемане на уеднаквени определения на компютърните престъпления и за ефективна хармонизация на законодателството, особено в областта на материалното наказателно право. В хода на работата по проекта за Конвенцията за престъпленията в кибернетичното пространство на Съвета на Европа Съветът на Европейския съюз приема Обща позиция относно преговорите по конвенцията и включва някои елементи от нея като част от стратегията на Съюза за противодействие на престъпленията в областта на високите технологии.

На 26 януари 2001 г. Европейската комисия приема Предложение до Съвета и до Европейския парламент, озаглавено "Създаване на сигурно информационно общество чрез подобряване на сигурността на информационните инфраструктури и противодействие на компютърните престъпления".[5] Една година по-късно, на 19 април 2002 г., е публикувано и предложение на Европейската комисия за Рамково

[4] *Legal Aspects of Computer-Related Crime in the Information Society (COMCRIME-Study)*, prepared for the European Commission by Prof. Dr. Ulrich Sieber, University of Würzburg.

[5] Communication from the Commission to the Council, the European Parliament, the Economic and Social Committee and the Committee of the Regions *Creating a Safer Information Society by Improving the Security of Information Infrastructures and Combating Computer-related Crime* (COM(2002)890).

решение на Съвета относно посегателствата срещу информационни системи.[6] Предложението включва две разпоредби в областта на материалното наказателно право – относно незаконния достъп до информационни системи и относно незаконното посегателство срещу такива системи.

Мерки за противодействие на компютърните престъпления са предприети и в рамките на Групата на Осемте (Г-8) – организация на седемте най-развити индустриални държави в света и Русия. През 1997 г. подгрупата по високи технологии на главните експерти на Г-8 приема десет принципа и план за действие за борба с компютърните престъпления, а през март 1998 г. е създадена и мрежа от експерти (работеща постоянно 24 часа в денонощието, 7 дни в седмицата), за подпомагане на разследването на престъпленията в областта на високите технологии. Основните цели на тази мрежа са да осигури, че извършителите на компютърни престъпления не се ползват със закрила никъде по света и че правоприлагащите органи разполагат с необходимите технически и правни средства за откриването на извършителите на такива престъпления и тяхното своевременно привличане към отговорност. Прието е принципите да се прилагат както чрез сключването на международни договори, така и чрез приемането на национални закони и политики. Много други държави, извън Г-8, също се присъединяват към новосъздадената мрежа.

4. Компютърните престъпления в България

В България първите компютърни престъпления се появяват сравнително късно, причина за което е слабото развитие и ограниченото приложно поле на информационните технологии в периода преди промените от 1989 г. В края на 80-те и началото на 90-те години на XX век компютърната инфраструктура започва да навлиза масово в много сфери на обществения живот в страната, което закономерно довежда и до появата и постепенното разрастване на компютърната престъпност.

Първото регистрирано компютърно престъпление в България е крупно длъжностно присвояване, извършено от касиерка в "Балкантурист – София" през периода 1982 – 1983 г. За периода 1982 – 1990 г. в страната са регистрирани едва 7 случая на посегателства, извършени чрез използване на компютърни технологии. Това са преди всичко длъжностни присвоявания, измами, престъпления по служба и документни престъпления. През периода 1991 – 1995 г. тези случаи нарастват на 18, докато през 1996 – 2001 г. техният брой е около 200.[7]

Основната част от регистрираните компютърни престъпления в България са свързани с локални ведомствени компютри и компютърни мрежи. Последният такъв случай датира от декември 2002 г., когато вътрешна проверка в Министерството на вътрешните работи установява, че над 400 служители на министерството незаконно са събирали информация от системата на МВР.

---

[6] Commission proposal for a Council framework decision on attacks against information systems, presented by the Commission on April 19, 2002 (COM(2002)173 final).

[7] Вж. Бояджиева, Ю., *Престъпност по Интернет – криминологични аспекти*, Юридически свят, кн. 1, 2002 г.

С увеличаване на достъпа и потреблението на Интернет обаче все по-често започват да се регистрират и престъпления, извършвани в глобалната мрежа. През 1998 г. във Варна са разкрити извършителите на множество измами, свързани с поръчки по Интернет и получаване на стоки от САЩ и Европа чрез кредитни карти на чужди граждани или фалшиви карти с генерирани номера. В София е разкрита контрабанда по Интернет на ценни антични монети и археологически предмети, като извършителите организират аукциони с регистриран електронен адрес на страницата на американската компания "eBay".

Регистрирани са и първите случаи на престъпни посегателства чрез използване на електронна поща. Неизвестен извършител от Кърджали изпраща по електронната поща на националната телевизия bTV съобщение със заплаха за заложена бомба в студиото. Появяват се случаи на електронни финансови пирамиди (Варна, Добрич, Русе), при които извършителите въвеждат в заблуждение ползватели на Интернет, като изпращат по електронните им пощи съобщения за набиране на дарения, осигуряване на работа в чужбина и др.

Все по-сериозни стават и хакерските атаки срещу Интернет страници на държавни институции, търговски дружества и др. През февруари 1999 г. хакери атакуват страниците на Българската телекомуникационна компания и Комитета по пощи и далекосъобщения в знак на протест срещу предложението за въвеждане на лицензионен режим за доставчиците на Интернет. На 16 януари 2001 г. неизвестен хакер прониква в Интернет страницата на президента на републиката, като разбива защитата на страницата чрез използване на паролите на сътрудниците на президента, отговарящи за нейното актуализиране, и подменя оригиналното съдържание със свой собствен текст. Обект на хакерски атаки стават и официалните страници на основните политически партии в страната.[8]

На 30 август 2002 г. в Интернет се появява страница на банка ДСК, в която се съдържа невярна информация, че от 3 септември банката ще предоставя безлихвени кредити от 5 000 лв. и заеми до 10 000 лв. с нисък лихвен процент. На 21 септември 2002 г. авторът на сайта е разкрит от служители на Националната служба за борба с организираната престъпност (НСБОП). По данни на НСБОП извършителят е използвал логото на ДСК от Интернет страницата на чирпанския клон на банката и е направил нова страница, съдържаща невярната информация. По това време официалната страница на банка ДСК в Интернет е все още в процес на разработване.

Процъфтяващият бизнес на детската порнография по Интернет засегна и България. Сървъри на български Интернет доставчици се използват от неизвестни лица за поддържане на страници, съдържащи детски порнографски снимки и видеоклипове. В края на 2001 г. в Сливен беше разкрито производство на детски

[8] В началото на 2001 г. хакери проникват в страницата на Съюза на демократичните сили и на мястото на официалното съдържание поставят обидни и нецензурни съобщения. На 27 март 2002 г. хакер изпраща съобщение от името на Българската социалистическа партия, че партията е взела решение да се саморазпусне. Съобщението е изпратено до над 100 български и чуждестранни медии и агенции и до адресите на част от международните партньори на БСП в Европа. Първоначалната проверка показва, че потребителят е влязъл с интернет-карта през доставчик на Интернет услуги, но не е разбил защитата на сървъра, а е маскирал електронен адрес като този на партийния пресцентър. През септември същата година жертва на хакерска атака става и официалната страница на Националното движение Симеон II.

порнографски снимки, организирано от софийско студио, което е пускало фотографиите в порносайт по Интернет. През 2002 г. по сигнали на потребители органите на Министерството на вътрешните работи разкриват няколко случая на български сайтове с порнографско съдържание, на които са публикувани детски порнографски фотографии.

Зачестяват и случаите на разпространение и продажба чрез Интернет на пиратски копия на бизнес софтуер, енциклопедии и компютърни игри. Внушителен е и размерът на нелегалното предлагане на музика в MP3 формат чрез Интернет. През март 2003 г. Българската асоциация на музикалните продуценти (БАМП) подава в Националната служба за борба с организираната престъпност (НСБОП) първия в българската история сигнал за проверка на сървъри с нелицензирано музикално съдържание у нас. По данни на асоциацията нелегитимното предлагане на песни от някои български сайтове води до теглене на отделни заглавия от 60 до 80 хиляди пъти. Данните на Международната федерация за звукозаписната индустрия (International Federation of Phonographic Industry – IFPI), както и на Международния алианс по интелектуална собственост (International Intellectual Property Alliance – IIPA) и Алианса на производителите на бизнес софтуер (Business Software Alliance – BSA), публикувани в онлайн изданието Forbes през 2001 г. интернет пиратството в България е повече от 50% от общото потребление на музикални продукти в страната.

Глобалната мрежа се използва и за незаконно организиране на хазартни игри. През януари 2003 г. в Сливен служители на НСБОП разкриват мрежа за незаконни залагания на футболни мачове през Интернет. Заловени са петима извършители, които осъществяват нелегалната дейност виртуално чрез използването на компютри и свързани с тях мобилни телефони и приемат залози по Интернет от цялата страна.

II. Правна уредба на компютърните престъпления по българския Наказателен кодекс

Правната уредба на компютърните престъпления е създадена с измененията на Наказателния кодекс (НК) от септември 2002 г. (ДВ, бр. 92 от 2002 г.). Систематично основната част от съставите на компютърните престъпления са обособени в новосъздадената глава девета “а”, озаглавена “Компютърни престъпления”. Единствено компютърната измама (чл. 212а НК) е уредена в главата за престъпленията против собствеността, преди всичко поради близостта и с класическия състав на измамата по чл. 212 НК. Извън тези разпоредби с измененията бяха създадени и нови състави на други престъпления, като например нарушаване тайната на кореспонденцията (чл. 171, ал. 1, т. 3 и ал. 3 НК), унищожаване или повреждане на чуждо имущество (чл. 216, ал. 3 НК), лъжливо документиране (чл. 313, ал. 1 и 3 НК). Общото между тези новосъздадени състави е, че те по един или друг начин са свързани с използването на информационни технологии.

1. Основни понятия

1.1. Общи бележки

При формулирането на съставите на компютърните престъпления НК използва множество нови понятия. Прецизното определяне на съдържанието на тези понятия е от особено значение за ефективното приложение на новите разпоредби. Именно в тази насока обаче новите текстове разкриват известна непоследователност, което се дължи преди всичко на недостатъчно доброто терминологично съгласуване между внесените в Народното събрание проекти.[9] На първо място, голяма част от предвидените в първоначалните варианти на проектите легални дефиниции не намериха място в приетия текст на закона. По този начин останаха без легални определения основни понятия като "компютър", "ресурси на компютъра", "информационна мрежа", "компютърна програма" като частен случай на данни, "компютърен вирус" като частен случай на програма и др. Единствените понятия, за които НК в настоящата си редакция предвижда легални определения, са понятията "компютърна информационна система", "компютърни информационни данни" и "доставчик на компютърно-информационни услуги". На второ място, текстовете на самите разпоредби от особената част на НК се разминават терминологично с легалните дефиниции по чл. 93 НК. Подобно непоследователност може да доведе до съществени трудности в практиката при прилагането на закона, особено предвид сложната и недостатъчно добре позната материя, която тези текстове уреждат.

Чл. 93 НК дава легални дефиниции на три понятия – "компютърна информационна система", "компютърни информационни данни" и "доставчик на компютърно-информационни услуги". Определенията на тези понятия следват почти дословно дефинициите по Конвенцията за престъпленията в кибернетичното пространство.

2.2. Компютърна информационна система

Според чл. 93, т. 21 НК компютърна информационна система означава всяко отделно устройство или съвкупност от взаимносвързани или сходни устройства, което в изпълнение на определена програма осигурява или един от елементите на което осигурява автоматична обработка на данни. Определението обхваща всички устройства, предназначени за автоматична обработка на данни в цифрова форма. Такова устройство може да включва хардуер и софтуер, както и специални устройства за въвеждане, извеждане и съхраняване на информация. Освен всяко самостоятелно устройство, определението за компютърна информационна система включва и всяка съвкупност от взаимносвързани или сходни устройства, например устройства свързани посредством компютърна мрежа. "Автоматично" в случая

[9] Първоначално в Народното събрание бяха внесени два различни законопроекта за изменение и допълнение на НК, предвиждащи създаването на състави за компютърни престъпления. В окончателния си вариант измененията представляват комбинация между отделни текстове и от двата проекта. На практика при формулирането на съставите на повечето престъпления беше отдадено предпочитание на единия проект, докато за легалните определения на основните понятия беше използван другият проект. Крайният резултат от този подход е, че се достигна до нежелано разминаване между текстовете на престъпните състави и легалните дефиниции.

означава без пряка човешка намеса, а под "обработка на данни" се разбира, че данните в компютърната информационна система се обработват посредством изпълнение на компютърна програма. Компютърната информационна система обикновено се състои от процесор и различни устройства, които изпълняват определена специфична функция посредством взаимодействие с процесора.

Понятието компютърна информационна система не е използвано в нито един от текстовете в особената част на НК. Вместо него при формулирането на съставите на компютърните престъпления законодателят си служи с понятията "компютър" (чл. 319б, ал. 1, чл. 319г, ал. 1, чл. 216, ал. 3 НК), "информационна мрежа" (чл. 319г, ал. 1 НК), и "компютърна мрежа" (чл. 171, ал. 3 НК).

2.3. Компютърни информационни данни

Компютърните информационни данни са определени в чл. 93, т. 22 НК като всяко представяне на факти, информации 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. Определението се основава на дефиницията за данни на Международната организация по стандартизация (International Organization for Standardization – ISO). "Поддаващи се на обработка" означава, че данните са във форма, която позволява непосредственото им обработване от компютърна система. Терминът "компютърни" означава, че данните са в електронна или друга форма, позволяваща директна обработка. Тези данни могат да се съхраняват в както в компютърна информационна система, така и на друг носител, например дискета, компакт-диск, смарт-карта, чип и т.н.

Според посоченото определение компютърните програми също са компютърни информационни данни. В тази си част разпоредбата на чл. 93, т. 22 НК е неточна. Компютърните програми се различават съществено от компютърните данни, поради което *de lege ferenda* е препоръчително тези две понятия да бъдат отделени и за всяко от тях да бъде включено самостоятелно легално определение. Аргумент за това е и формулирането на престъпните състави в особената част на НК, където компютърните данни и компютърните програми са посочени като различни предмети на престъплението (чл. 319б, ал. 1 НК).

В особената част на НК понятието компютърни информационни данни е използвано единствено при формулиране на съставите на компютърната измама по чл. 212а, ал. 1 и 2 НК. В останалите случаи законът си служи с термина "компютърни данни" (чл. 319а, ал. 1, чл. 319б, ал. 1 НК). Въпреки терминологичната непоследователност на НК, двете понятия са идентични и следва да се разглеждат като синоними.

2.4. Доставчик на компютърно-информационни услуги

Според чл. 93, т. 23 НК доставчик на компютърно-информационни услуги е всяко юридическо или физическо лице, което предлага възможността за комуникация чрез компютърна система или което обработва или съхранява

компютърни данни за тази комуникационна услуга или за нейните ползватели.[10] Така дефинираното понятие обхваща много широк кръг лица, които са свързани по някакъв начин с предаването или обработката на данни чрез компютърни системи. Тези лица могат да бъдат разделени на три основни групи. На първо място това са всички лица (публични или частни), които предоставят на потребителите възможността да комуникират помежду си. Няма значение дали потребителите представляват затворена група (например работещите в едно предприятие, на които услугата се предоставя чрез корпоративна мрежа) или доставчикът предлага своите услуги публично, както и дали това става срещу заплащане или безплатно. На второ място са лицата, които съхраняват или по друг начин обработват данни от името на лицата, предоставящи посочените услуги. На трето място са лицата, които съхраняват или по друг начин обработват данни от името на потребителите на услугите.

Понятието доставчик на компютърно-информационни услуги не се среща никъде в особената част на НК. Единствено при формулирането на разпоредбата на чл. 319е НК законът говори за "доставяне на информационни услуги". Доколкото обаче тази разпоредба препраща към задълженията на посредника при електронно изявление по чл. 6, ал. 2, т. 5 от Закона за електронния документ и електронния подпис (ЗЕДЕП), приложение ще намери определението за посредник по чл. 6, ал. 1 ЗЕДЕП. Така на практика легалната дефиниция на понятието доставчик на компютърно-информационни услуги при сегашната редакция на съставите в особената част на НК остава излишно.

3. Нерегламентиран достъп до ресурсите на компютър, копиране и използване на компютърни данни без разрешение

Чл. 319а. (1) Който осъществи нерегламентиран достъп до ресурсите на компютър, копира или използва компютърни данни без разрешение, когато се изисква такова, се наказва с глоба до три хиляди лева.

(2) Ако деянието по ал. 1 е извършено от две или повече лица, сговорили се предварително за извършване на такова деяние, наказанието е лишаване от свобода до една година или глоба до три хиляди лева.

(3) Ако деянието по ал. 1 е извършено повторно, наказанието е лишаване от свобода до три години или глоба до пет хиляди лева.

(4) Ако деянията по ал. 1 – 3 са извършени по отношение на сведения, съставляващи държавна тайна, наказанието е от една до три години лишаване от свобода, ако не подлежи на по-тежко наказание.

(5) Ако от деянието по ал. 4 са настъпили тежки последици, наказанието е от една до осем години.

3.1. Нерегламентиран достъп до ресурсите на компютър

[10] В единия от първоначалните варианти на проекта беше предвидено включването на легално определение на понятието "доставящ информационни услуги". Според този текст доставящ информационни услуги е всяко лице, което обработва или съхранява компютърни данни в полза на услуги, даващи възможност за осъществяване на комуникация чрез компютърна система.

Разпоредбата на чл. 319а НК регламентира три различни основни състава: нерегламентиран достъп до ресурсите на компютър, копиране на компютърни данни без разрешение и използване на компютърни данни без разрешение.

Нерегламентираният достъп е едно от основните и най-често срещани посегателства срещу сигурността на компютърните системи и компютърните данни. Чрез него се накърнява поверителността и неприкосновеността на ресурсите на компютъра. Често нерегламентираният достъп е в основата и на други компютърни престъпления с по-висока степен на обществена опасност. [11]

Непосредствен обект на това престъпление са обществените отношения, осигуряващи неприкосновеността на компютърните данни и тяхната защита срещу неправомерен достъп и узнаване от други лица..

От обективна страна престъплението се характеризира със специфичен предмет на посегателство, определен в закона като ресурсите на компютър. НК не дава легално определение на понятието ресурси на компютъра.[12] Ресурсите на компютъра обхващат както компютърните информационни данни, които се съхраняват и/или обработват от компютърната информационна система, така и отделните устройства, които представляват елементи от тази система.[13]

Изпълнителното деяние на престъплението е формулирано като осъществяване на достъп. В обяснителния доклад към Конвенцията за престъпленията в кибернетичното пространство осъществяването на достъп е определено като проникване в определена компютърна система или част от нея, включително чрез друга компютърна система, когато двете системи са свързани помежду си посредством публични телекомуникационни мрежи или се намират в обща мрежа (например локална мрежа или Интранет). За да е налице осъществяване на достъп е достатъчно създаването на технологична възможност за достъп до определени устройства от компютърната информационна система или до определени компютърни данни, без да е необходимо върху тях да е упражнено определено въздействие. В този смисъл простото изпращане на съобщение или файл посредством електронна поща от една компютърна система до друга, както и на SMS до мобилен телефон, не може да се квалифицира като престъпление по чл. 319а, ал. 1 НК, тъй като такова действие не създава технологическа възможност за изпращача да получи достъп до компютърната система или компютърните данни на получателя.

Във всички случаи изпълнителното деяние може да бъде осъществено единствено чрез действие.

---

[11] Инкриминирането на нерегламентирания достъп като самостоятелно престъпление е в съответствие с разпоредбите на Конвенцията за престъпленията в кибернетичното пространство, която в чл. 2 позволява на страните да обявят за престъпление по вътрешното си право самия незаконен достъп до цялата или до част от определена компютърна система, без да е необходимо настъпването на друг престъпен резултат.

[12] Определение на понятието ресурси на компютъра беше предвидено в единия от първоначалните проекти за изменение и допълнение на НК, но не попадна в окончателния вариант на закона. Според него ресурси на компютъра са оперативната памет, външната памет, данни в оперативната памет или външната памет, както и процесорно време.

[13] Вж. също Дончева, Д., *Компютърни престъпления по глава девета "а" от Наказателния кодекс*, Правна мисъл, кн. 2, 2003 г. Според автора нерегламентиран достъп до ресурсите на компютър означава достигане до информация, съдържаща се в определен компютър, нейното узнаване.

От обективна страна е необходимо осъщественият достъп да е нерегламентиран. Нерегламентиран е всеки достъп, който е осъществен в нарушение не само на закона, но и на други нормативни актове, а също и в нарушение на съответните процедури.[14]

Достъпът няма да бъде нерегламентиран, когато е налице правно основание за неговото осъществяване. Основанието може да произтича от разпоредба на действащото законодателство (закон или подзаконов нормативен акт) или да следва по силата на частно-правна сделка. Така например достъпът няма да е нерегламентиран в случаите, когато е налице надлежно разрешение или съгласие от страна на собственика на системата или на друго лице, упражняващо определени права върху нея. Достъпът обаче ще бъде нерегламентиран, когато по силата на нормативен акт това лице няма право да предоставя достъп до компютъра на други лица, например поради завишени изисквания за сигурност по отношение на конкретния компютър.[15] Деянието няма да бъде съставомерно и в случаите, когато става въпрос за отворени системи, които са предназначени за свободен (неограничен) достъп. Такива са например страниците в Интернет, предназначени за свободен достъп. Самото поддържане на свободно достъпна страница в Интернет съдържа в себе си съгласието на нейния собственик до тази страница да имат достъп неограничен кръг потребители на глобалната мрежа.[16] На последно място достъпът няма да бъде нерегламентиран, когато той е осъществен от лице,

---

[14] Конвенцията за престъпленията в кибернетичното пространство използва термина "незаконен достъп" (illegal access), като го определя като "неправомерен достъп" (without right).

[15] Пример за такива завишени изисквания за сигурност са системите за издаване и управление на удостоверенията за усъвършенстван електронен подпис. Едно от изискванията по отношение на доставчиците на удостоверителни услуги, които издават удостоверения за усъвършенствани електронни подписи, е да осигурят надеждна защита на системите за издаване и управление на удостоверенията. Съгласно чл. 9 от Наредбата за дейността на доставчиците на удостоверителни услуги, реда за нейното прекратяване и за изискванията при предоставяне на удостоверителни услуги системите за издаване и управление на удостоверенията трябва да се намират в специално защитени помещения, до които достъп имат само надлежно овластени служители в съответствие с техните функционални задължения. Достъпът до тези системи на лица, които не са служители на доставчика на удостоверителни услуги, ще бъде във всички случаи нерегламентиран, дори когато те са получили разрешение от такъв служител.

[16] Когато едно лице поддържа страница в Интернет, то разполага с различни технически средства, чрез които осъществява на практика достъп до системите на потребителите, които посещават неговата страница. Най-разпространеното такова средство са т.нар. кукита (cookies) – съобщения, които сървърът, на който се намира определена страница в Интернет, изпраща до браузъра на потребителя, посещаващ тази страница. Тези съобщения се съхраняват в системата на потребителя и се изпращат обратно до сървъра всеки път, когато потребителят посещава същата страница. Основната цел на кукитата е идентифициране на потребителите и евентуално подготвяне на специален вид на страницата в зависимост от получената информация (например вместо стандартната заглавна страница потребителят получава заглавна страница с изписано неговото име). Според обяснителния доклад към Конвенцията за престъпленията в кибернетичното пространство приложението на такива стандартни средства, инкорпорирани в масово използвани протоколи и програми, само по себе си не може да се квалифицира като незаконен достъп, защото обстоятелството, че потребителят е решил да използва тези протоколи и програми означава, че мълчаливо се е съгласил с приложението на тези средства. В случая с кукитата това мълчаливо съгласие следва и от факта, че потребителят не е отказал изрично първоначалното им инсталиране, нито в последствие ги е премахнал от системата.

което изпълнява свои законово регламентирани правомощия, например при извършване на проверка от компетентен контролен орган. В този случай достъпът ще бъде регламентиран, независимо от наличието или липсата на разрешение или съгласие от страна на лицето, което администрира компютъра.

Престъплението е уредено като формално престъпление (престъпление на просто извършване). За съставомерността на деянието е достатъчно лицето да е осъществило нерегламентиран достъп до определени компютърни информационни данни. Престъплението е довършено със самото осъществяване на изпълнителното деяние без да се изисква настъпването на друг резултат.[17]

Субект на престъплението може да бъде всяко наказателно отговорно лице, което няма регламентирано право (законно основание) на достъп до ресурсите на компютъра. От субективна страна престъплението е умишлено. Деецът съзнава, че няма право на достъп до съответните данни, и въпреки това го осъществява.

Настоящата редакция на чл. 319а, ал. 1 НК определя един сравнително широк обхват на престъплението нерегламентиран достъп. В тази насока Конвенцията за престъпленията в кибернетичното пространство изрично предвижда възможност страните да ограничат приложното поле на наказателната репресия като предвидят допълнителни изисквания за съставомерността на деянието, например правонарушението да бъде извършено в нарушение на мерките за сигурност, с намерение да се получат компютърни данни или с друго престъпно намерение, както и във връзка с компютърна система, която е свързана с друга компютърна система. Българският закон възприема максимално широк подход и не предвижда подобни ограничения, с което значително разширява приложното поле на разпоредбата. Това е разумно, тъй като по този начин се осигурява защита срещу възможно най-широк кръг посегателства. Изключение от приложното поле на разпоредбата остават единствено случаите по чл. 9, ал. 2 НК, когато поради своята малозначителност деянието не е обществено-опасно или неговата обществена опасност е явно незначителна.

3.2. Копиране или използване на компютърни данни без разрешение

Непосредствен обект на това престъпление са обществените отношения, осигуряващи неприкосновеността на различните видове информация, когато тя е представена в електронен вид.

Предмет на престъплението са компютърни данни. Въпреки различната формулировка, под компютърни данни следва да се разбират компютърни информационни данни по смисъла на чл. 93, т. 22 НК. За съставомерността на деянието е без значение дали тези данни се съхраняват в определена компютърна информационна система или извън нея на друг носител. Така например данните за създаване на електронен подпис (съответно частният ключ в хипотезата на усъвършенстван или универсален електронен подпис), съдържащи се в една смарт-карта, са компютърни информационни данни по смисъла на чл. 93, т. 22 НК и

[17] Вж. също Дончева, Д., *Компютърни престъпления по глава девета "а" от Наказателния кодекс*, Правна мисъл, кн. 2, 2003 г. Според автора престъплението е резултатно, като резултатът се състои в достигане, узнаване на съдържащата се в компютъра информация.

осъществяването на нерегламентиран достъп до тях е съставомерно деяние по чл. 319а, ал. 1 НК.

Престъплението е уредено в два основни състава, които се различават по формата на изпълнителното деяние. В първия случай става въпрос за копиране на компютърни данни, а във втория – за тяхното използване.

Копирането представлява създаването на копие (дубликат) на определени компютърни данни. Самото копиране на компютърни данни по начало не накърнява целостта на тези данни. Особеното при копирането на компютърни данни се състои в това, че всички копия са идентични както помежду си, така и по отношение на оригинала (доколкото при компютърните данни изобщо може да се говори за оригинал в класическия смисъл на това понятие). Именно поради тази причина копирането на компютърни данни без разрешение е деяние с висока степен на обществена опасност, което следва да бъде инкриминирано.

Използването на компютърни данни означава употреба на вече съществуващи компютърни данни. Примери за използване на компютърни данни са въвеждането на компютърни данни в компютърна система, изпращане на компютърни данни, прехвърляне на компютърни данни върху различни преносими носители и т.н.

От обективна страна и по двата основни състава на престъплението е необходимо изпълнителното деяние да е било осъществено без разрешение, когато такова се изисква. Необходимостта от такова разрешение може да произтича както от разпоредбата на нормативен акт, така и по силата на частно-правна сделка. Моментът на получаване на разрешението е без значение. Деянието няма да бъде съставомерно както при предварително, така и при последващо разрешение.

В хипотезата на копиране на компютърни данни престъплението е резултатно, като резултатът е създаването на копие от съответните данни. В хипотезата на използване на данните престъплението е формално – достатъчно е да е осъществено определено действие със съответните данни, което може да бъде квалифицирано като използване.

Субект на престъплението може да бъде всяко наказателно отговорно лице. От субективна страна следва да е налице умисъл. Деецът съзнава, че за извършване на съответните действия е необходимо разрешение и че не е получил такова, но въпреки това копира, съответно използва, компютърните данни.

3.3. Квалифицирани състави на престъпленията по чл. 319а НК

Чл. 319а НК регламентира няколко квалифицирани състава на престъпленията нерегламентиран достъп и копиране или използване на компютърни данни без разрешение. Квалифициращите обстоятелства са свързани с предмета на престъплението (сведения, съставляващи държавна тайна), субекта на престъплението (две или повече лица или едно лице при условията на повторност) и престъпния резултат (настъпване на тежки последици).

При формулирането на квалифицираните състави българският закон използва преди всичко класически квалифициращи обстоятелства и не държи сметка за специфичния характер на тези престъпления. Не са взети предвид и предложените от Конвенцията за престъпленията в кибернетичното пространство

примерни квалифициращи обстоятелства като нарушаване на мерките за сигурност, престъпно намерение или нарушение във връзка с компютърна система, която е свързана с друга компютърна система. Безспорно е, че тези обстоятелства също повишават степента на обществена опасност на деянието, като в същото време отразяват някои от специфични особености на този вид деяния.[18] Така например обществената опасност на деяние, извършено чрез преодоляването на специални мерки за сигурност, не винаги ще бъде по-ниска от тази на деяние, извършено от две или повече лица, сговорили се предварително. При сегашната редакция на текста обаче наличието на някое от тези обстоятелства ще може да се преценява единствено при индивидуализацията на наказанието. Проблемът придобива още по-голямо значение от гледна точка на наказуемостта на престъпленията по чл. 319а НК, тъй като по основния състав законът предвижда като единствено наказание налагането на глоба, докато при квалифицираните състави като алтернатива на глобата е предвидено и наказание лишаване от свобода.

3.3.1. Квалифицирани състави във връзка със субекта на престъплението

НК предвижда два квалифицирани състава с оглед субекта на престъплението – когато деянието е извършено от две или повече лица, сговорили се предварително за извършване на такова деяние (чл. 319а, ал. 2 НК) и когато е извършено повторно (чл. 319а, ал. 3 НК)

Чл. 319а, ал. 2 НК предвижда по-тежко наказание за случаите, когато престъплението е извършено от две или повече лица, сговорили се предварително за извършване на такова деяние. Според чл. 93, т. 12 НК едно престъпление е извършено от две или повече лица, когато в самото изпълнение са участвали най-малко две лица. Това означава, че най-малко две лица осъществяват елементи на изпълнителното деяние. Ако едното лице само улеснява извършването на престъплението без да осъществява елемент от изпълнителното деяние (например предоставя дискета, на която извършителят копира данните), ще е налице помагачество.

Необходимо е освен това съизвършителите да са действали при предварителен сговор за осъществяване на такова деяние. Сговорът е предварителен, когато лицата са взели решението за извършване на престъплението и са съгласували престъпната си воля известно време преди деянието, в сравнително спокойно състояние и с обсъждане на мотивите "за" и "против".[19] Предварителният сговор трябва да има за предмет извършването престъпление по чл. 319а НК, без значение дали лицата са определели предварително конкретния предмет на посегателството (конкретна компютърна информационна система или конкретни компютърни информационни данни).

---

[18] За значението на тези обстоятелства за степента на обществена опасност на деянието може да се съди и по предоставената от Конвенцията възможност страните да не инкриминират във вътрешното си законодателство случаите на незаконен достъп въобще, а само тези, при които са налице посочените квалифициращи обстоятелства (член 2 от Конвенцията).

[19] Вж. по-подробно относно предварителния сговор – Стойнов, Ал., *Наказателно право. Особена част. Престъпления против собствеността.* Изд. Сиела. София, 1997 г., стр. 34-35.

Чл. 319а, ал. 3 НК предвижда квалифициран състав, ако деянието е извършено повторно. По смисъла на чл. 28, ал. 1 НК престъплението е извършено повторно, ако деецът го е извършил, след като е бил осъден с влязла в сила присъда за друго такова престъпление. Според практиката на Върховния съд "еднакви по вид престъпления по смисъла на чл. 28 НК са тези, с които се осъществяват едни и същи или различни състави на едно и също престъпление, включително когато то е квалифицирано или привилегировано".[20]

3.3.2. Квалифицирани състави във връзка с предмета на престъплението

Квалифицираният състав във връзка с предмета на престъплението е уреден в чл. 319, ал. 4 НК. Особеният предмет на престъплението са сведения, съставляващи държавна тайна.

Държавната тайна е легално дефинирана в новия Закон за защита на класифицираната информация (ЗЗКИ). Според чл. 25 ЗККИ държавна тайна е информацията, определена в списъка по приложение № 1, нерегламентираният достъп до която би създал опасност за или би увредил интересите на Република България, свързани с националната сигурност, отбраната, външната политика или защитата на конституционно установения ред.[21]

В наказателно-правната доктрина се приема, че определението на държавната тайна по чл. 104, ал. 3 НК включва два кумулативно дадени белега – формален и материален. Формалният белег е, че информацията, представляваща държавна тайна, трябва да бъде включена в списък под формата на приложение към закона. Материалният белег се изразява в обстоятелството, че нерегламентираният достъп до съответната информация би създал опасност за или би увредил интересите на Република България.

От субективна страна престъплението е умишлено, като деецът знае, че сведенията, по отношение на които извършва съответните действия, съставляват държавна тайна.

С оглед все по-широкото използване на електронни подписи в различни сфери на обществения живот е необходимо да бъде разширено приложното поле на разпоредбата на чл. 319а, ал. 4 НК, като към сведенията, съставляващи държавна тайна, се добавят и данните за създаване на електронен подпис, съответно частният ключ при усъвършенстваните електронни подписи. Обществената опасност на посегателствата срещу тайната на тези данни, която е изрично регламентирана в чл.

---

[20] Вж. Пост. 2-70-Пл., т. 1.

[21] Дефиниция на държавната тайна дава и чл. 104, ал. 3 НК, според който държавна тайна са факти, сведения и предмети от военно, политическо, стопанско или друго естество, узнаването на които от друга държава или чужда организация може да увреди интересите на републиката и особено нейната безопасност; списъкът на фактите, сведенията и предметите, които съставляват държавна тайна, се приема от Народното събрание и се обнародва в Държавен вестник. С приемането на ЗЗКИ тази разпоредба не беше отменена, нито беше актуализирана в съответствие с новата уредба на държавната тайна. По този начин определението на държавната тайна по чл. 104, ал. 3 НК ще продължи да се прилага, но само по отношение на престъпните състави по чл. 104, ал. 1 и 2 НК. Този извод се подкрепя и от систематичното място на това определение, което е в особената, а не в общата част на НК. За останалите престъпления, които имат за предмет сведения, съставляващи държавна тайна, включително компютърните престъпления, приложение ще намери новото определение по чл. 25 ЗЗКИ.

14, съответно чл. 18 ЗЕДЕП, е изключително висока и не съответства на предвиденото по основния състав наказание глоба до 3 000 лв. В този смисъл е препоръчително *de lege ferenda* разпоредбата на чл. 319а, ал. 4 НК да бъде променена, като към сведенията, съставляващи държавна тайна, се добави и всяка информация, съставляваща друга защитена от закона тайна.

3.3.3. Квалифицирани състави във връзка с престъпния резултат

Престъпният резултат е квалифициращо обстоятелство по чл. 319а, ал. 5 НК. Това е единственият състав по глава 9а от НК, по който е налице тежко престъпление по смисъла на чл. 93, т. 7 НК. Особеното в този случай е наличието на две квалифициращи обстоятелства. На първо място квалифициращо обстоятелство е престъпният резултат, който в закона е определен като настъпване на тежки последици. На второ място в текста на разпоредбата е изрично е посочено, че тя се прилага единствено по отношение на деяния по чл. 319а, ал. 4 НК, т.е. необходимо е деянието да е извършено по отношение на сведения, съставляващи държавна тайна. Следователно съставът по чл. 319а, ал. 5 НК е квалифициран по два кумулативно дадени признака – особен предмет (сведения, съставляващи държавна тайна) и престъпен резултат (настъпване на тежки последици).

От обективна страна настъпването на тежките последици трябва да бъде пряк и непосредствен резултат от изпълнителното деяние. Квалификацията на настъпилите последици като тежки ще се извършва от съда във всеки конкретен случай. Доколкото, обаче, квалифицираният състав визира единствено посегателства срещу сведения, съставляващи държавна тайна, при определянето на тежестта на последиците съдът ще следва да се ръководи преди всичко от степента на застрашаване или увреждане на държавния интерес.

Квалифицираният състав по чл. 319а, ал. 5 НК има субсидиарен характер. Той ще намери приложение единствено в случаите, когато деецът не подлежи на по-тежко наказание. По-тежки наказания са предвидени например за шпионство по чл. 104, ал. 1 НК (издаване или събиране с цел издаване на чужда държава или чужда организация на сведения, съставляващи държавна тайна) и за разгласяване на сведения от военен характер, съставляващи държавна тайна, по чл. 393 НК.

4. Престъпни посегателства срещу компютърни програми или данни

Чл. 319б. (1) Който без разрешение на лицето, което администрира или ползва компютър, добави, промени, изтрие или унищожи компютърна програма или данни, в немаловажни случаи, се наказва с лишаване от свобода до една година или глоба до две хиляди лева.

(2) Ако с деянието по ал. 1 са причинени значителни вреди или са настъпили други тежки последици, наказанието е лишаване от свобода до две години и глоба до три хиляди лева.

(3) Ако деянието по ал. 1 е извършено с цел имотна облага, наказанието е лишаване от свобода от една до три години и глоба до пет хиляди лева.

Чл. 319в. (1) Който извърши деяние по чл. 319б по отношение на данни, които се дават по силата на закон, по електронен път или на магнитен носител, се наказва с лишаване от свобода до две години и с глоба до три хиляди лева.

(2) Ако деянието по ал. 1 е с цел да се осуети изпълнение на задължение, наказанието е лишаване от свобода до три години и глоба до пет хиляди лева.

4.1. Добавяне, промяна, изтриване или унищожаване на компютърна програма или данни

Непосредствен обект на престъпните посегателства срещу компютърни програми и компютърни данни са обществените отношения, осигуряващи неприкосновеността на компютърните програми и данни и защита срещу неправомерно въздействие върху тях.

От обективна страна престъплението се характеризира с особен предмет – компютърна програма или компютърни данни.

Компютърните данни са легално определени в чл. 93, т. 22 НК като всяко представяне на факти, информации 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.

НК не дава легално определение на понятието компютърната програма.[22] Компютърната програма представлява поредица от инструкции, които могат да бъдат изпълнение от компютърната система за постигане на определен резултат.[23]

Изпълнителното деяние по основния състав е дадено в четири различни форми – добавяне, променяне, изтриване и унищожаване. И при четирите форми изпълнителното деяние може да бъде осъществено единствено чрез действие.[24]

Добавяне на компютърна програма или компютърни данни означава въвеждане на нова програма или данни в компютърна система. Начинът, по който програмата или данните са въведени, е без значение. Така например въвеждането може да стане посредством периферните устройства на компютъра (чрез клавиатурата), посредством прехвърлянето им от преносим носител на информация (компакт диск, дискета), чрез използването на друга компютърна система и т.н. Само по себе си добавянето на компютърна програма или данни по начало не уврежда вече съществуващите в компютърната система програми и данни. В някои случаи обаче такова увреждане е възможно, например когато чрез добавената програма или данни се нарушава нормалното функциониране на останалите

[22] В един от първоначалните варианти на проекта беше предвидена легална дефиниция на това понятие, според която компютърната представлява комбинация от команди и свързана информация, които, когато са изпълнени в определена форма, карат компютър, компютърна система или компютърна мрежа да изпълнят зададени функции.

[23] Българският НК неоснователно прави разлика между понятията компютърна програма и софтуер, като в чл. 172а, ал. 2 НК, който регламентира престъпленията против интелектуалната собственост, е инкриминирано незаконното използване на софтуер или компютърна програма. Двете понятия имат идентично съдържание и се използват като синоними. Основание за такова тълкуване дава и Законът за авторското право и сродните му права, който посочва като обект на авторското право само компютърните програми.

[24] Вж. по-подробно за отделните форми на изпълнителното деяние и отношението между тях – Дончева, Д., *Компютърни престъпления по глава девета "а" от Наказателния кодекс*, Правна мисъл, кн. 2, 2003 г.

програми или се накърнява целостта на други данни, намиращи се в компютърната система.[25]

Променяне на компютърна програма или компютърни данни означава изменение на съществуващи програми или данни. Изменението обикновено води до промяна във функционирането на програмата и до изменение в данните без да ги прави негодни за използване.

Изтриването на компютърна програма или компютърни данни представлява заличаване на съответната програма или данни. За съставомерността на деянието е без значение дали изтритата програма или данни могат да бъдат възстановени.[26]

Унищожаването на компютърна програма или данни означава увреждане на целостта или функционалността на програмата или данните, което ги прави абсолютно негодни за използване.

Престъплението е уредено като резултатно. При отделните форми на изпълнителното деяние резултатът е съответно появата на нова програма или данни (при добавянето), настъпването на промяна в съществуваща програма или данни (при променянето), и заличаването или увреждането на съществуваща програма или данни (при изтриването, съответно унищожаването).

От обективна страна е необходимо изпълнителното деяние да е осъществено без разрешението на лицето, което ползва или администрира компютъра. Лицето, което администрира компютъра, е лицето на което е поверена поддръжката на компютъра. Лицето, което ползва компютъра, е лицето, което на практика осъществява определени действия с него.

От обективна страна е необходимо случаят да е немаловажен. Според чл. 93, т. 9 НК маловажен случай е този, при който извършеното престъпление с оглед на липсата или незначителността на вредните последици или с оглед на други смекчаващи обстоятелства представлява по-ниска степен на обществена опасност в сравнение с обикновените случаи на престъпление от съответния вид. Дали случаят е маловажен подлежи на преценка от съда във всеки конкретен случай

Субект на престъплението може да бъде всяко наказателно отговорно лице с изключение на лицата, които администрират или ползват компютъра. От

---

[25] Типичен случай на добавяне на компютърна програма, която нарушава нормалното функциониране на компютърната система, е въвеждането на компютърен вирус, което е обособено като самостоятелно престъпление по чл. 319г НК.

[26] В много случаи изтриването не означава цялостно заличаване на програмата или данните от компютърната система. Когато една програма или данни бъдат изтрити от компютъра, компютърът унищожава информацията, указваща местоположението на съответната програма или данни върху твърдия диск. Тази информация се използва от операционната система за изграждането на структурата на директориите в компютъра. Когато тази информация е унищожена, съответната програма или данни стават невидими за операционната система. Те съществуват, но операционната система не знае как да достигне до тях. С възстановяването на тази информация, което може да стане сравнително лесно и за което има създадени специални програми, на практика се възстановява и изтритата програма или данни. На практика единственият начин за пълно заличаване на определена информация от компютъра е записването на нови данни върху вече съществуващите. По начало операционната система периодично записва нова информация върху данните, за които информацията къде се намират е унищожена. Това означава, че колкото повече време е изминало от изтриването на определени данни (от заличаването на информацията за тяхното местоположение), толкова по-голяма е вероятността операционната система да запише други данни върху тях и те да бъдат окончателно заличени.

субективна страна престъплението е умишлено. Деецът съзнава, че няма необходимото разрешение, но въпреки това добавя, променя, изтрива или унищожава компютърната програма или данни.

4.2. Квалифицирани състави на престъпните посегателства срещу компютърни програми и компютърни данни

НК регламентира няколко квалифицирани състава на престъплението по чл. 319б, ал. 1 НК. Квалифициращи обстоятелства са престъпният резултат (причиняване на значителни вреди или настъпване на други тежки последици), престъпната цел (користна цел, осуетяване изпълнението на задължение) и предмета на престъплението (данни, които по силата на закон се предоставят по електронен път или на магнитен носител).

4.2.1. Квалифицирани състави във връзка с престъпния резултат

Престъпният резултат е квалифициращо обстоятелство по чл. 319б, ал. 2 НК. Законът посочва два възможни престъпни резултата – причиняване на значителни вреди или настъпване на други тежки последици.

Според съдебната практика значителните вреди обхващат само имуществените вреди от престъплението. Имуществените вреди от престъплението се изразяват в намаляване на имуществото (намаляване на активите или увеличаване на пасивите) на определено лице. Дали вредите са обикновени или значителни се определя въз основа на два критерия – абсолютната стойност на вредата и нейната относителна стойност в сравнение със стойността на цялото имущество.[27]

Що се отнася до настъпването на други тежки последици те следва да се тълкуват преди всичко като причиняване на неимуществени вреди, защото имуществените вреди се обхващат от понятието значителни вреди. Кога тези последици са тежки е фактически въпрос и ще подлежи не преценка от съда във всеки конкретен случай.

Двата възможни престъпни резултата са посочени алтернативно. При всички случаи е необходимо наличието на причинно-следствена връзка между престъпния резултат и изпълнителното деяние.

4.2.2. Квалифицирани състави във връзка с предмета на престъплението

Предметът на престъплението е квалифициращо обстоятелство по чл. 319в, ал. 1 НК и е определен като данни, които се дават по силата на закон, по

[27] Вж. ТР № 6 от 15.11.1973 г. на ОСНК по н. д. № 2/73 г. Според решението ако относителната стойност на вредата е голяма, а по абсолютния си размер е незначителна, няма да има значителна вреда по смисъла на закона. Обратно, когато абсолютният размер на вредата е значителен, но в сравнение със стойността на ощетения патримониум е незначителна, ще е налице вреда, която ще квалифицира престъплението като по-тежко. Вж. също ТР № 2 от 09.08.1993 г. на ОСНК по н.д. № 2 от 1993 г. Според това решение значителни имуществени вреди означава преди всичко, че вредите по абсолютния си размер са такива, т.е. че паричният еквивалент на причинените вреди е значителен.

електронен път или на магнитен носител. От обективна страна е достатъчно изрична законова разпоредба да предвижда задължение за предоставяне на определени данни, както и възможност тези данни да бъдат предоставени по електронен път или на магнитен носител. Не е необходимо законът да предвижда задължение данните да се предоставят само по електронен път или на магнитен носител. Достатъчно е да е предвидена възможност данните да бъдат предоставени по този начин. Предоставянето на данни по електронен път може да включва изпращането им чрез електронната поща, през Интернет и т.н. Що се отнася до магнитните носители те могат да бъдат магнитни дискове (дискети), магнитни ленти и др.[28]

Чл. 319в, ал. 1 НК не съдържа ограничения относно това кой и на кого предоставя съответните данни. По-специално няма изискване тези данни да се предоставят от или на държавен орган. От обективна страна е достатъчно единствено съществуването на законова разпоредба, регламентираща задължение за предоставяне на определена информация.

Понастоящем няколко закона предвиждат възможност за предоставяне на определена информация по електронен път или на магнитен носител.

На първо място такава възможност е предвидена в данъчното законодателство. Данъчният процесуален кодекс предоставя възможност на данъчните субекти, които са свързани с електронна система със съответната данъчна дирекция, да изпращат по електронен път на данъчните органи декларациите и справките, които са длъжни да представят в определените за това срокове (чл. 56, ал. 4 ДПК). По Закона за данъка върху добавената стойност регистрираните по закона лица са длъжни да водят специални регистри (т.нар. дневник за покупките и дневник за продажбите) и да предоставят ежемесечно информация от тези регистри на данъчните органи на магнитен носител (чл. 106, ал. 5 ЗДДС). Освен това законът дава възможност на регистрираните лица да подават справки-декларации за съответния данъчен период по електронен път при условията и по реда на Данъчния процесуален кодекс (чл. 104, ал. 6 ЗДДС).

На второ място възможност за подаване на информация по електронен път е предвидена в митническото законодателство. Законът за митниците предвижда, че декларирането пред митническите учреждения може да се осъществява по електронен път (чл. 67, ал. 1, т. 2 ЗМ), като условията и редът за такова деклариране са уредени в Правилника за приложение на Закона за митниците (чл. 134 – 136 ППЗМ).

На трето място са законите, уреждащи правото на достъп до информация. Законът за достъп до обществена информация предоставя възможност на лицата да

[28] Освен магнитните носители широко разпространени в практиката са и оптичните носители на информация (оптични дискове). Нещо повече, оптичните носители придобиват все по-широко разпространение, тъй като имат по-голям капацитет за съхраняване на информация и са по-надеждни в сравнение с магнитните. Буквалното тълкуване на текста на чл. 319в, ал. 1 НК води до извода, че когато е налице посегателство срещу определени данни, които се дават по силата на закон и са предоставени не на магнитен, а на оптичен носител, деянието няма да се квалифицира като по-тежко наказуемо. Подобно тълкуване е нелогично, тъй като двете деяния разкриват една и съща степен на обществена опасност и следва да бъдат еднакво наказуеми. За да се преодолее това положение е необходимо *de lege ferenda* определението магнитен да отпадне от текста на разпоредбата.

подават заявления за предоставяне на достъп до обществена информация по електронен път (чл. 24, ал. 2 ЗДОИ) и да получават такава информация под формата на копие на технически носител (чл. 26, ал. 1, т. 4 ЗДОИ). Законът за защита на личните данни също предвижда възможност за подаване на заявления за предоставяне на достъп до лични данни по електронен път (чл. 29, ал. 2 ЗЗЛД) и за предоставяне на данните също по електронен път (чл. 31, ал. 2 ЗЗЛД).

Други закони, които предвиждат възможност за предаване на данни по електронен път, са Законът за здравното осигуряване относно задължението на изпълнителите на медицинска помощ да предоставят на районните здравно-осигурителни каси определени данни и документация само на електронен или магнитен носител в съгласуван с Националната здравно-осигурителна каса формат (чл. 66, ал. 3 ЗЗО), Законът за обществените поръчки относно възможността възложителят на обществени поръчки да уведомява кандидатите по електронен път при условията и по реда на Закона за електронния документ и електронния подпис (чл. 12, ал. 2 ЗОП), Законът за Сметната палата относно правото на органите на Сметната палата да изискват справки и друга информация на електронен носител във връзка с извършваните от тях предварителни проучвания или одити (чл. 31, ал. 2 ЗСП) и др.

4.2.3. Квалифицирани състави във връзка с особената цел на дееца

НК регламентира два квалифицирани състава с оглед особената престъпна цел на дееца – когато престъплението е извършено с цел имотна облага (чл. 319б, ал. 3 НК) и когато е извършено с цел да се осуети изпълнение на задължение (чл. 319в, ал. 2 НК).

По чл. 319б, ал. 3 НК особената цел на дееца е посочена в закона като имотна облага. Става дума за т.нар. користна цел. Деецът цели настъпването на благоприятни изменения в своето имущество или в имуществото на трето лице. Действителното постигане на целта е без значение за съставомерността на деянието, но ще може да се преценява при индивидуализацията на наказанието.

По чл. 319в, ал. 2 НК особената цел на дееца се изразява в осуетяване изпълнението на задължение. Текстът на чл. 319в, ал. 2 НК се прилага само по отношение на деяния по чл. 319в, ал. 1 НК, т.е. необходимо е кумулативно да е налице и особеният предмет на престъплението – данни, които се дават по силата на закон, по електронен път или на магнитен носител. Особената цел сама по себе си не е основание за прилагане на по-тежко наказуемия състав. Става дума, следователно, за посегателство срещу компютърни данни, които се дават по силата на закон и предоставянето на които е свързано с пораждането на задължение за определено лице. Тук се включват преди всичко случаите на подаване на справки и декларации по данъчното и митническото законодателство, които са предпоставка за възникването на определени данъчни или митнически задължения за съответните лица.

Осуетяването означава създаване на пречки за изпълнението на определено задължение. Не е необходимо деецът да е длъжник по задължението, чието изпълнение се стреми да осуети. Видът и размерът на задължението са без значение.

Квалифициращото обстоятелство е единствено намерението на дееца да осуети изпълнението на определено задължение. Реализацията на тази цел е без значение за съставомерността на деянието. Действителното осуетяване на изпълнението на задължението обаче може да се преценява от съда при индивидуализацията на наказанието.

5. Компютърни вируси

Чл. 319г. (1) Който въведе компютърен вирус в компютър или информационна мрежа, се наказва с глоба до три хиляди лева.

(2) Ако от деянието по ал. 1 са настъпили значителни вреди или е извършено повторно, наказанието е лишаване от свобода до три години и глоба до хиляда лева.

5.1. Въвеждане на компютърен вирус

Непосредствен обект на престъплението въвеждане на компютърен вирус са обществените отношения осигуряващи нормалното функциониране на компютърните информационни системи, включително компютърните мрежи.

От обективна страна престъплението се характеризира преди всичко с особено средство – компютърен вирус. Съществен пропуск на законодателя е отсъствието на легално определение на понятието "компютърен вирус".[29] Компютърният вирус представлява компютърна програма, която се разпространява автоматично и против волята или без знанието на ползващите компютърните системи лица и е предназначен за привеждане на компютърни системи или компютърни мрежи в изпълнение на нежелани от ползващите ги състояния или резултати.[30]

Компютърните вируси следва да са разграничават от някои други видове компютърни програми, които притежават само някои от характерните особености на вирусите. Най-често срещаните такива програми са т.нар. троянски коне (Trojan horses) и червеи (worms). Троянският кон представлява компютърна програма, чието изпълнение води до желан от потребителя резултат, но едновременно с това, без знанието на потребителя, осъществява и втори резултат, който е нежелан за него, като например повреждане на файлове, осигуряване на достъп до чужда компютърна система, дори в някои случаи въвеждане на компютърен вирус. Троянският кон сам по себе си не е вирус, тъй като не се разпространява автоматично и против волята или без знанието на лицето. Червеите представляват компютърни програми, които се разпространяват автоматично и без знанието или против волята на лицето, което ползва системата, без да оказват въздействие върху

[29] Определение на понятието компютърен вирус беше предвидено в един от първоначалните варианти на проекта и според него компютърният вирус представлява група от компютърни инструкции, които се саморазмножават и са в състояние да заразят компютърни програми или компютърни данни, да погълнат компютърни ресурси, да променят, унищожат данни или по някакъв друг начин да попречат за нормалната работа на компютър, компютърна система или компютърна мрежа.

[30] Вж. Димитров, Г., *Предложения до работната група към Министерството на правосъдието по проект за изменение на НК*, София, 2002 г.

останалите компютърни програми или данни. Единственият нежелан резултат, който тези програми могат да причинят, е претоварване на системата вследствие на тяхното неконтролируемото разпространение.

Липсата на легално определение на понятието компютърен вирус може да създаде сериозни затруднения в практиката при преценката дали определена програма представлява компютърен вирус. Въпросът придобива особено значение от гледна точка на съществуването и разпространяването на програми, които не отговарят на критериите за компютърен вирус, но въпреки това са еднакво опасни за потребителите на компютърни информационни системи. Такива програми са например програмите за отдалечен контрол (известни още като "троянски коне") и т.нар. "червеи".[31]

Един от най-често срещаните начини за разпространяване на вируси са файловете, прикрепени към съобщения по електронната поща.

Изпълнителното деяние е определено в закона като въвеждане. Въвеждането представлява инкорпориране на вируса в определен компютър или информационна мрежа.[32] Законът не изисква вирусът да бъде въведен в чужд компютър или информационна мрежа. Подобно решение има известно основание, тъй като поради специфичните особености на компютърните вируси, много често въвеждането им в който и да е компютър създава сериозна опасност за разпространението им и в други компютри и информационни мрежи.

Престъплението е резултатно. Компютърният вирус трябва да е въведен в определена компютърна информационна система (компютър или мрежа).[33]

Субект на престъплението може да бъде всяко наказателно отговорно лице. От субективна страна е налице умисъл. Деецът цели да въведе компютърния вирус в определен компютър или информационна мрежа. Вината като елемент от субективната страна на престъплението е от особено значение при въвеждането на компютърни вируси поради специфичната характеристика на компютърните вируси да се саморазмножават. Съставомерно ще е единствено деянието, при което деецът съзнава, че инструкциите, които въвежда в компютъра, представляват компютърен вирус и въпреки това цели тяхното въвеждане. Няма да е налице престъпление следователно, когато лицето не знае, че програмата или данните, които въвежда в компютъра съдържат компютърен вирус. Същото важи и за случаите, когато поради активирането на вируса системата на съответното лице

---

[31] Троянският кон представлява компютърна програма, която позволява достъп до чужда компютърна информационна система без знанието на лицето, което я ползва. Троянският кон не се саморазмножава, поради което не се приема за компютърен вирус. Червеите (worms) от друга страна се саморазмножават, но не причиняват други вредни последици (освен претоварване на паметта вследствие на саморазмножаването), поради което също не попадат в определението за компютърен вирус.

[32] Редакцията на текста разкрива известна непоследователност от гледна точка на използваните понятия, тъй като термините компютър и информационна мрежа не са легално определени. По-прецизно би било изпълнителното деяние да бъде формулирано като въвеждане на компютърен вирус в компютърна информационна система.

[33] Вж. Дончева, Д., *Компютърни престъпления по глава девета "а" от Наказателния кодекс*, Правна мисъл, кн. 2, 2003 г. Престъплението е довършено с достигането на вируса до определен компютър или информационна мрежа, без значение дали се е активирал или е бил неутрализиран от специална антивирусна програма.

автоматично въвежда вируса в други компютърни системи или мрежи или го изпраща по електронна поща.

В първоначалния вариант на проекта беше предвидена наказателна отговорност за по-широк кръг деяния, свързани с разпространението на компютърни вируси, включително за тяхното създаване, но в приетия вариант като форма на изпълнителното деяние остана единствено въвеждането. Когато обаче компютърният вирус е създаден от едно лице, а е въведен в компютър или информационна мрежа от друго лице, създателят на вируса ще носи наказателна отговорност като съучастник (помагач), ако са налице съответните елементи от субективна страна.

5.2. Квалифицирани състави

Чл. 319г, ал. 2 НК регламентира два квалифицирани състава на престъплението въвеждане на компютърен вирус. В първия случай деянието е квалифицирано с оглед на обективната страна, като квалифициращ признак е престъпният резултат, посочен в закона като настъпване на значителни вреди.[34] Във втория случай деянието е квалифицирано с оглед на особеното качество на субекта на престъплението, когато е извършено повторно.

6. Разпространяване на компютърни или системни пароли

Чл. 319д. (1) Който разпространи компютърни или системни пароли и от това последва разкриване на лични данни или държавна тайна, се наказва с лишаване от свобода до една година.

(2) За деяние по ал. 1, извършено с користна цел, или ако с него са причинени значителни вреди, наказанието е лишаване от свобода до три години.

6.1. Основен състав

Непосредствен обект на престъплението са обществените отношения, осигуряващи поверителността и неприкосновеността на информацията в електронна форма, съставляваща лични данни или държавна тайна.

От обективна страна престъплението се характеризира с особен предмет – компютърни или системни пароли. Паролата представлява поредица от символи, която позволява на определен потребител да има достъп до определен файл, програма, компютърна система или мрежа. За да може системата да изпълнява зададените от съответния потребител команди или да му предостави достъп до определени данни, той трябва предварително да въведе своята парола. Паролите са едно от най-често срещаните средства за защита на компютрите и компютърните системи срещу осъществяване на неправомерен достъп до тях. Преди всичко те

[34] Пропуск на законодателя е включването в престъпния резултат на настъпването на други тежки последици. По този начин неимуществените вреди неоснователно са изключени от квалифициращите обстоятелства. От гледна точка на особеностите на компютърните вируси обаче може да се предположи, че вредите от тяхното разпространение ще имат предимно имуществен характер.

намират приложение при компютърни системи, които се ползват едновременно от множество потребители. Освен това паролите се използват и при други компютърни системи, които, макар да не предоставят достъп на множество потребители по едно и също време, могат да бъдат използвани от различни потребители последователно във времето.

Разделянето на паролите на компютърни и системни излишно утежнява редакцията на разпоредбата, доколкото липсва ясен критерий кои пароли се квалифицират като компютърни и кои – като системни.[35] Разпространяването на всяка парола, независимо от нейния вид, когато е довело до разкриване на лични данни или държавна тайна, разкрива еднаква степен на обществена опасност и следва да се квалифицира като престъпление по чл. 319д НК.

От обективна страна изпълнителното деяние на престъплението по чл.319д, ал. 1 НК се изразява в разпространяване. Разпространяването означава довеждане на определена информация, в случая на съответните пароли, до знанието на трети лица. Изпълнителното деяние може да бъде извършено само чрез действие. Паролите могат да бъдат разпространени както чрез използване на компютър или компютърна система, така и по друг начин, включително на хартиен носител.

От обективна страна престъплението е резултатно. Резултатът е посочен като разкриване на лични данни или държавна тайна. Разкриването означава довеждане на определена информация до знанието на лице или лица, които нямат право на достъп до такава информация.

Личните данни са определени в Закона за защита на личните данни. Според чл. 2, ал. 1 ЗЗЛД лични данни са информация за физическо лице, която разкрива неговата физическа, психологическа, умствена, семейна, икономическа, културна или обществена идентичност.

За да е налице съставомерно деяние по чл. 319д, ал. 1 НК, е необходимо наличието на причинна връзка между изпълнителното деяние и престъпния резултат. Причинната връзка също е елемент от обективната страна на престъплението и означава, че разкриването на личните данни или държавната тайна трябва да е пряка и непосредствена последица от разпространяването на компютърните или системните пароли.

Субект на престъплението може да бъде всяко наказателно-отговорно лице. За съставомерността на деянието няма значение дали деецът е знаел съответните пароли правомерно. От субективна страна е налице умисъл, който обхваща както изпълнителното деяние (разпространяването на паролите), така и престъпния резултат (разкриването на личните данни или държавната тайна).

6.2. Квалифицирани състави

Чл. 319д, ал. 2 НК регламентира два квалифицирани състава. Първата хипотеза е когато деянието е извършено с користна цел. Това е квалифициран състав с оглед на субективната страна, като квалифициращо обстоятелство се явява

[35] *De lege ferenda* е препоръчително разпоредбата да бъде формулирана като разпространяване на пароли за достъп до компютърна информационна система или компютърни информационни данни. По този начин от една страна се обхващат едновременно всички видове пароли, а от друга страна текстът се привежда в съответствие с легалните определения по чл. 93 НК.

особената цел на дееца. Деянието е извършено с користна цел, когато деецът желае чрез него да набави за себе си или за другиго имотна облага.

Втората хипотеза е когато с деянието са причинени значителни вреди. Престъплението е квалифицирано с оглед на обективната страна, а квалифициращо обстоятелство е особеният резултат. Според съдебната практика значителните вреди обхващат само имуществените вреди, а не и неимуществените такива.[36] Дали вредите са обикновени или значителни се определя въз основа на два критерия – относителната стойност на вредата в сравнение със стойността на цялото имущество и нейната абсолютна стойност.[37]

7. Престъпления във връзка със Закона за електронния документ и електронния подпис

Чл. 319е. Който при доставяне на информационни услуги наруши разпоредбите на чл. 6, ал. 2, т. 5 от Закона за електронния документ и електронния подпис, се наказва с глоба до пет хиляди лева, ако не подлежи на по-тежко наказание.

Непосредствен обект на престъплението по чл. 319е НК са обществените отношения, осигуряващи нормалното изпращане, получаване, записване и съхраняване на електронни изявления. Тези обществени отношения са регламентирани в ЗЕДЕП.

Нормата на чл. 319е НК е бланкетна норма, защото препраща за един от елементите на престъплението (изпълнителното деяние) към друг нормативен акт – Закона за електронния документ и електронния подпис (чл. 6, ал. 2, т. 5 ЗЕДЕП).

От обективна страна изпълнителното деяние се изразява в нарушаване на задължението за съхраняване на информацията за времето и източника на предаваните електронни изявления за срок от 6 месеца. То може да бъде осъществено както чрез действие (унищожаване на съответната информация), така и чрез бездействие (непредприемане на необходимите действия за запазване на информацията). Престъплението е формално – достатъчно е да е било осъществено изпълнителното деяние.

Престъплението по чл. 319е НК се характеризира с особен субект. Това е лице, което има качеството посредник при електронно изявление по смисъла на чл. 6, ал. 1 ЗЕДЕП. Изискването субектът на престъплението да има такова качество произтича от препращането към нормата на чл. 6, ал. 2, т. 5 ЗЕДЕП, която се прилага само по отношение на посредниците при електронни изявления. Понятието посредник при електронното изявление е легално дефинирано в чл. 6, ал. 1 ЗЕДЕП като лице, което по възлагане от титуляра изпраща, получава, записва или съхранява електронно изявление или извършва други услуги, свързани с него.

---

[36] И в този случай законодателят е пропуснал да посочи другите тежки последици като квалифициращо обстоятелство, оставяйки неимуществените вреди извън обстоятелствата, обуславящи приложението на по-тежко наказуемия състав. Решението не е удачно, тъй като в много случаи, особено при разкриването на лични данни, причинените вреди могат да имат неимуществен характер.

[37] Вж. ТР № 6 от 15.09.1973 г. на ОСНК по н. д. № 2/73 г.

При определянето на субекта на престъплението по чл. 319е НК следва да се има предвид основният наказателно-правен принцип, че наказателната отговорност е лична и наказателно-отговорни могат да бъдат само физически лица. Следователно субект на престъплението по чл. 319е НК ще бъде посредникът - физическо лице. Когато посредникът при електронното изявление е юридическо лице (например доставчик на Интернет услуги), субект на престъплението по чл. 319е НК ще бъде физическото лице – служител на доставчика, което съгласно вътрешните правила на доставчика е задължено да осигури съхраняването посочената информация.

От обективна страна законът изисква изпълнителното деяние да е осъществено при доставяне на информационни услуги. НК не дава легално определение на дейността по доставяне на информационни услуги. Доставянето на информационни услуги представлява предоставянето (възмездно или безвъзмездно) на услуги на трети лица за осъществяване на свързаност за предаване на компютърни данни чрез компютърни системи, както и обработването и/или съхраняването на компютърни данни от името на предоставящия услугите във връзка с предоставянето им.[38]

Изискването изпълнителното деяние да е осъществено при доставяне на информационни услуги е до голяма степен излишно. Напълно достатъчно за съставомерността на деянието е лицето да има качеството посредник при електронно изявление и да не е изпълнило задължението си да съхранява посочената информация в законово определения срок.

От субективна страна престъплението е умишлено. Деецът съзнава, че е длъжен да съхранява посочената информация за определения срок, но въпреки това нарушава това свое задължение.

Разпоредбата на чл. 319е НК има субсидиарен характер. Тя се прилага в случаите, когато деецът не подлежи на по-тежко наказание.

8. Компютърна измама

Чл. 212а. (1) 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 от една до шест години и глоба до шест хиляди лева.

(2) 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.

8.1. Компютърна измама по чл. 212а, ал. 1 НК

[38] Вж. за определението на доставчик на информационни услуги Димитров, Г., *Предложения до работната група към Министерството на правосъдието по проект за изменение на НК*, София, 2002 г.

Компютърната измама е уредена като престъпление против собствеността. Нейното систематично място е в раздел четвърти "Измама" на глава пета "Престъпления против собствеността" от особената част на НК.

Непосредствен обект на престъплението са от една страна обществените отношения, осигуряващи неприкосновеността и нормалното упражняване на правото на собственост.

От обективна страна компютърната измама по чл. 212а, ал. 1 НК се характеризира с няколко предмета на посегателство. На първо място предмет на престъплението са компютърни информационни данни. Компютърните информационни данни са определени в чл. 93, т. 21 НК. Същият е и предметът на престъплението в хипотезата на компютърна измама чрез използване на чужд електронен подпис, защото електронният подпис според ЗЕДЕП представлява именно компютърни информационни данни. На второ място предмет на компютърната измама могат да бъдат и материалните носители, върху които тези данни се съхраняват. Това могат да бъдат магнитни и оптични носители, компютърни информационни системи и т.н.[39]

Изпълнителното деяние на престъплението включва два взаимно свързани елемента. Първият елемент е посочен в закона като възбуждане или поддържане на заблуждение у друго лице. Заблуждението представлява неправилна представа за факти и обстоятелства от обективната действителност. При компютърната измама, както и при обикновената измама по чл. 212 НК, това са факти и обстоятелства, свързани по определен начин с правното действие, което измаменото лице предприема или не предприема. Възбуждането на заблуждение представлява първоначално създаване у лицето на неправилна представа за определени факти и обстоятелства, докато поддържането на заблуждение се изразява в утвърждаване на вече формирана без участието на дееца неправилна представа.

Вторият елемент на изпълнителното деяние е посочен в закона като внасяне, изменение, изтриване или заличаване на компютърни информационни данни или използване на чужд електронен подпис.

Въпреки терминологичните несъответствия, внасянето, изменението, изтриването и заличаването на компютърни информационни данни са същите изпълнителни деяния, както и на престъплението по чл. 319б НК, и са подробно разгледани при анализа на тази разпоредба.[40]

Под използване на чужд електронен подпис се има предвид използване на данните за създаване на електронния подпис (съответно частния ключ в хипотезата на усъвършенстван или универсален електронен подпис) от лице, различно от автора. Съгласно чл. 14 ЗЕДЕП само авторът има достъп до данните за създаване на електронния подпис (съответно до частния ключ) и следователно само той може правомерно да ги използва.[41]

---

[39] Вж. Стойнов, Ал., *Компютърната измама*, Съвременно право, кн. 4, 2002 г. Според автора компютърната измама има за предмет още физическото лице, върху което деецът въздейства, както и имуществото, намиращо се във фактическа власт на измаменото лице.

[40] Терминологичното разминаване между двете разпоредби (внасяне/добавяне, промяна/изменение, заличаване/унищожаване, компютърни данни/компютърни информационни данни) е необосновано и следва *de lege ferenda* да бъде коригирано.

[41] Редакцията на разпоредбата е неточна и може да създаде сериозни затруднения в практиката, поради което е наложително *de lege ferenda* тя да бъде прецизирана като се посочи

Вторият елемент на изпълнителното деяние се явява начин или средство за осъществяване на първия елемент – възбуждане или поддържане на заблуждение.

Компютърната измама по чл. 212а, ал. 1 НК е резултатно престъпление. Престъпните резултати са два – на първо място резултат е настъпилата промяна в компютърните информационни данни, а на второ място резултат е настъпването на вреди за измаменото лице или за друго лице. [42]

Субект на компютърната измама по чл. 212а, ал. 1 НК може да бъде всяко наказателно отговорно лице. В хипотезата на компютърна измама чрез използване на чужд електронен подпис субект на престъплението може да бъде всяко наказателно-отговорно лице с изключение на автора на подписа.

От субективна страна престъплението е умишлено. Деецът извършва посегателството като съзнава, че възбужда или поддържа заблуждение у измаменото лице. Освен това законът изисква и наличието на особена цел. Става дума за користна цел – деецът цели да набави имотна облага за себе си или за другиго.

8.2. Компютърна измама по чл. 212а, ал. 2 НК

Компютърната измама по чл. 212а, ал. 2 НК се различава от престъплението по чл. 212а, ал. 1 НК по няколко белега.[43]

На първо място разлика има в изпълнителното деяние. По чл. 212а, ал. 2 НК изпълнителното деяние е посочено само като неправомерно внасяне, изменение, изтриване или заличаване на компютърни информационни данни. Липсва възбуждането или поддържането на заблуждение у друго лице.

От обективна страна при компютърната измама по чл. 212а, ал. 2 НК законът изрично изисква посегателството да е извършено без деецът да има право на това.

Престъплението по чл. 212а, ал. 2 НК също е резултатно, но резултатът обхваща единствено настъпилата промяна в компютърните информационни данни. Съставомерността на деянието не зависи от настъпването на вреди за измаменото лице или за други лица.

Субект на престъплението по чл. 212а, ал. 2 НК може да бъде всяко наказателно-отговорно лице с изключение на лицата, които имат право да извършват посочените действия спрямо конкретните компютърни информационни данни.

От субективна страна престъплението по чл. 212а, ал. 2 НК също е умишлено престъпление, но се характеризира с различна цел – получаване от самия деец на нещо, което не му се следва. Ако деецът цели не той, а трето лице да

изрично, че става дума за използването не на чужд електронен подпис, а на чужди данни за създаване на електронен подпис.

[42] Вж. Стойнов, Ал., *Компютърната измама*, Съвременно право, кн. 4, 2002 г. Според автора вредата от компютърната измама може да бъде или само имуществена, или съчетание от имуществени и морални увреждания.

[43] Вж. по-подробно за отношението между съставите на чл. 212а, ал. 1 и 2 НК, както и за отношението между компютърната измама и другите видове измама – Стойнов, Ал., *Компютърната измама*, Съвременно право, кн. 4, 2002 г.

получи в резултат на деянието нещо, което не му се следва, деянието няма да е съставомерно по чл. 212а, ал. 2 НК

9. Други компютърни престъпления

9.1. Престъпления срещу неприкосновеността на кореспонденцията

Чл. 171. (1) Който противозаконно:

1. отвори, подправи, скрие или унищожи чуждо писмо, телеграма, запечатани книжа, пакет или други подобни;

2. вземе чуждо, макар и отворено, писмо или телеграма с цел да узнае тяхното съдържание или пък със същата цел предаде другиму чуждо писмо или телеграма;

3. узнае неадресирано до него съобщение, изпратено по електронен път, или отклони от адресата му такова съобщение,

се наказва с лишаване от свобода до една година или с глоба от сто до триста лева.

(2) Ако деянието е извършено от длъжностно лице, което се е възползувало от служебното си положение, наказанието е лишаване от свобода до две години, като съдът може да постанови и лишаване от право по чл. 37, точка 6.

(3) Който чрез използуване на специални технически средства противозаконно узнае неадресирано до него съобщение, предадено по телефон, телеграф, чрез компютърна мрежа или по друго далекосъобщително средство, се наказва с лишаване от свобода до две години.

С измененията на НК от 2002 г. бяха внесени съществени допълнения в правната уредба на престъпленията против неприкосновеността на кореспонденцията, продиктувани от все по-широкото използване на информационните технологии за размяна на информация между лицата. Непосредствен обект на тези престъпления са обществените отношения, които осигуряват неприкосновеността и тайната на кореспонденцията въобще и в частност на тази, която се предава по електронен път.[44]

9.1.1. Узнаване съдържанието на чуждо съобщение, изпратено по електронен път

Неправомерното узнаване на съдържанието на чуждо съобщение, изпратено по електронен път, е уредено в чл. 171, ал. 1, т. 3 НК.

Непосредствен обект на това престъпление са обществените отношения, гарантиращи тайната на кореспонденцията.

От обективна страна предмет на престъплението е съобщение, изпратено по електронен път. Съобщението представлява определена информация. То е изпратено по електронен път, когато е използвано електронно средство за

[44] Вж. по-подробно относно престъпленията против неприкосновеността на кореспонденцията – Стойнов, Ал. *Наказателно право. Особена част. Престъпления против правата на човека.* Изд. Сиела. София, 1997 г., стр. 205 и сл.

комуникация. Съобщение, изпратено по електронен път, е например изпращането на съобщение по електронна поща, на sms от мобилен телефон и т.н. За разлика от традиционните престъпления срещу неприкосновеността на кореспонденцията, които имат два предмета – от една страна самата информация, а от друга – носителят на тази информация (например писмо, телеграма и др.), при неправомерното узнаване на съобщение, изпратено по електронен път, е възможно деецът да узнае съдържанието на съобщението и без да е необходимо да има физически достъп до материалния носител на информацията. Такава ще бъде например хипотезата, когато едно лице проникне в електронната поща на друго лице през Интернет.

Изпълнителното деяние е формулирано в закона като узнаване. От обективна страна е необходимо съобщението да не е адресирано до дееца. Престъплението е резултатно – резултатът е неправомерното узнаване на съдържанието на съобщението.

Субект на престъплението може да бъде всяко наказателно-отговорно лице с изключение на титуляра, автора и адресата на съобщението. От субективна страна е налице умисъл. Деецът съзнава, че съобщението е чуждо (че не е адресирано до него) и въпреки това узнава неговото съдържание.

9.1.2. Отклоняване на съобщение, изпратено по електронен път, от неговия адресат

Отклоняването на съобщение, изпратено по електронен път, е второто престъпление по чл. 171, ал. 1, т. 3 НК.

Непосредствен обект на това престъпление са обществените отношения, които гарантират сигурността на предаването на информацията, предмет на кореспонденцията, от изпращача на адресата.

Предмет на престъплението отново е съобщение, изпратено по електронен път. Изпълнителното деяние обаче се изразява в отклоняване на съобщението от неговия адресат. Отклоняването на съобщението означава възпрепятстване на неговото получаване от адресата, за когото то е предназначено. Престъплението е резултатно – необходимо е адресатът да не е получил изпратеното до него съобщение.

Субект на престъплението е всяко наказателно-отговорно лице с изключение на адресата на съобщението. За разлика от хипотезата на узнаване на чуждо съобщение, при отклоняването теоретично е възможно субект на престъплението да бъдат титулярът и авторът на съобщението, когато те отклоняват собственото си съобщение.

От субективна страна е налице умисъл. Деецът съзнава, че съобщението не е адресирано до него и въпреки това възпрепятства получаването му от адресата.

9.1.3. Противозаконно узнаване на чуждо съобщение предадено чрез компютърна мрежа

С измененията на НК от 2002 г. беше допълнен текстът на чл. 171, ал. 3 НК, инкриминиращ противозаконното узнаване на чуждо съобщение чрез използване

на специални технически средства. Преди измененията законът изискваше от обективна страна престъплението да е извършено по отношение на съобщение, изпратено по телефон, телеграф или друго далекосъобщително средство. С измененията към примерното изброяване на далекосъобщителните средства бяха изрично добавени компютърните мрежи.

Компютърната мрежа представлява свързаност на две или повече компютърни информационни системи за обмен на компютърни данни. Начинът на осъществяване на връзката може да бъде различен, например наземна връзка (чрез кабел), безжична връзка (чрез радио вълни, инфрачервени лъчи, сателит) и т.н. Една мрежа може да бъде географски ограничена до малка територия (локални мрежи) или да се разпростира върху по-голяма територия (мрежи, свързващи отделни области). Отделните мрежи от своя страна също могат да се свързват помежду си. Интернет представлява глобална мрежа, състояща се от множество свързани помежду си мрежи, всички използващи едни и същи протоколи. Съществуват и други видове мрежи, свързани или не с Интернет, посредством които могат да предават компютърни данни между компютърни системи. Компютърните системи могат да бъдат свързани към мрежата като крайни точки или като средства за опосредяване на комуникацията по мрежата. От значение в случая е, че данните се обменят по мрежата.

От обективна страна престъплението трябва да е извършено чрез използване на специални технически средства. В хипотезата на съобщение, изпратено чрез компютърна мрежа, тези технически средства могат да бъдат специален хардуер или софтуер, позволяващ свързване към компютърна мрежа и осигуряващ достъп до информацията, обменяна по нея.

9.2. Унищожаване и повреждане на чуждо имущество

Чл. 216. (3) Който, като осъществи нерегламентиран достъп до компютър от значение за предприятие, учреждение, юридическо или физическо лице, и по този начин унищожи или повреди чуждо имущество, се наказва с лишаване от свобода от една до шест години и глоба до десет хиляди лева.

Унищожаването и повреждането на чуждо имущество посредством осъществяването на нерегламентиран достъп до компютър е уредено като квалифициран състав на престъплението унищожаване и повреждане.

От обективна страна изпълнителното деяние на престъплението включва два елемента. Първият елемент е осъществяване на нерегламентиран достъп до компютър. Този елемент наподобява изпълнителното деяние на престъплението по чл. 319а, ал. 1 НК. В хипотезата на чл. 216, ал. 3 НК обаче става дума за различен предмет на посегателство – компютър от значение за предприятие, учреждение, юридическо или физическо лице. Компютърът представлява компютърна информационна система по смисъла на чл. 93, т. 21 НК.[45] Кога определен компютър е от значение за предприятие, учреждение, юридическо или физическо лице е фактически въпрос, който ще се преценява от съда във всеки конкретен

[45] Предметът на нерегламентирания достъп по чл. 319а, ал. 1 НК са ресурсите на компютъра, които представляват компютърни информационни данни по смисъла на чл. 93, т. 22 НК.

случай. При тази преценка съдът следва да изхожда както от характеристиките на самия компютър, така и от информацията и данните, които се съхраняват в него.

Вторият елемент на изпълнителното деяние е същият както по основния състав на унищожаването и повреждането по чл. 216, ал. 1 НК – унищожаване и повреждане на чуждо имущество.[46] Следва да се има предвид, че за да е налице престъпление по чл. 216, ал. 3 НК от обективна страна между двете деяния трябва да е налице функционална връзка – осъществяването на нерегламентирания достъп е начин, средство за унищожаването или повреждането на чуждото имущество.

9.3. Лъжливо документиране

Чл. 313. (1) Който потвърди неистина или затаи истина в писмена декларация или съобщение, изпратено по електронен път, които по силата на закон, указ или постановление на Министерския съвет се дават пред орган на властта за удостоверяване истинността на някои обстоятелства, се наказва с лишаване от свобода до три години или с глоба от сто до триста лева.

(2) Когато деянието по ал. 1 е извършено с цел да се избегне заплащане на дължими данъци, наказанието е лишаване от свобода от една до шест години или глоба от сто до двеста и петдесет лева.

(3) Наказанието по ал. 1 се налага и на онзи, който потвърди неистина или затаи истина в частен документ или съобщение, изпратено по електронен път, в които по изрична разпоредба на закон, указ или постановление на Министерския съвет е специално задължен да удостовери истината, и употреби този документ като доказателство за невярно удостоверените обстоятелства или изявления.

(4) Който във връзка с публично предлагане на ценни книги в проспект или обзор за икономическо състояние използва неистински благоприятстващи данни или премълчава неблагоприятни такива, които са от съществено значение при вземане на решение за придобиване на ценни книги, се наказва с лишаване от свобода до три години и глоба до петстотин лева.

Измененията в съставите на лъжливото документиране по чл. 313, ал. 1 и 3 НК се изразяват в добавянето на съобщението, изпратено по електронен път, като предмет на престъплението заедно с писмената декларация по чл. 313, ал. 1 НК и частния документ по чл. 313, ал. 3 НК.

Промените в съставите на лъжливото документиране са практически ненужни. Съобщението, изпратено по електронен път, ще бъде документ по смисъла на НК, единствено ако отговаря на изискванията за електронен документ по ЗЕДЕП. В този случай обаче по силата на чл. 3, ал. 2 ЗЕДЕП това съобщение ще бъде приравнено на писмен документ, с което попада в приложното поле на чл. 313 НК и преди промяната. От друга страна, ако съобщението, изпратено по електронен път, не отговаря на изискванията за електронен документ, то няма правно значение, защото не автентифицира изявлението.

[46] Вж. по-подробно относно престъпленията против неприкосновеността на кореспонденцията – Стойнов, Ал. *Наказателно право. Особена част. Престъпления против собствеността.* Изд. Сиела. София, 1997 г., стр. 115 и сл.