ҚЫЛМЫСТЫҚ ҚҰҚЫҚ
КРИМИНОЛОГИЯ, УГОЛОВНОЕ ПРАВО
CRIMINAL LAW CRIMINOLOGY

МРНТИ: 10.77.01 10.51889/2959-6181.2023.72.2.007
УДК: 343.2/.7

Б.Б.Досжанов[1]
[1] Казахский национальный педагогический университет имени Абая

ОБЪЕКТИВНЫЕ ПРИЗНАКИ УГОЛОВНЫХ ПРАВОНАРУШЕНИЙ В СФЕРЕ ИНФОРМАТИЗАЦИИ И СВЯЗИ

Аннотация

В статье освещаются вопросы, связанные с изменениями, происходящими в экономической жизни и финансово-кредитной системе предприятий различных форм собственности и т.п., оказывающие существенное влияние на вопросы защиты информации. Долгое время в нашей стране существовала только одна собственность - государственная, поэтому информация и секреты были тоже только государственные, которые охранялись спецслужбами.

В связи с открытостью национального информационного пространства и популярностью зарубежных средств массовой информации, в т. ч. телевидения и Интернет-ресурсов (почтовых служб, социальных сетей, блогов и видео порталов), возникает реальная угроза информационного влияния на общественное сознание населения. Информационное влияние может выражаться как в виде прямого навязывания идей, противоречащих национальным интересам Республики Казахстан, так и в виде создания определенного информационного фона, искусственно поддерживаемого путем манипулирования информацией или ее тенденциозным комментированием. Для противодействия подобным манипулирования общественным сознанием требуется серьезно улучшить эффективность государственной информационной политики, увеличить открытость государственных органов, повысить обеспеченность права граждан на информацию.

Ключевые слова: информатизация, связь, собственник, национальная безопасность, ЭВМ, перехват, компьютерные данные, уголовное правонарушение.

Б.Б.Досжанов [1]
[1]Абай атындағы Қазақ ұлттық педагогикалық университеті

АҚПАРАТТАНДЫРУ ЖӘНЕ БАЙЛАНЫС САЛАСЫНДАҒЫ ҚЫЛМЫСТЫҚ ҚҰҚЫҚ БҰЗУШЫЛЫҚТАРДЫҢ ОБЪЕКТИВТІК БЕЛГІЛЕРІ

Аңдатпа

Мақалада экономикалық өмірдегі, қаржы-несие жүйесіндегі, әртүрлі меншік нысанындағы кәсіпорындарда ақпаратты қорғауға айтарлықтай ықпал еткен және т.б. өзгерістерге байланысты мәселелер қарастырылады. Біздің елде ұзақ уақыт бойы тек бір ғана меншік - мемлекеттік меншік болған, сондықтан ақпарат пен құпиялар тек қана арнайы мемлекет тарапынан қорғалған.

Ұлттық ақпараттық кеңістіктің ашықтығы мен шетелдік БАҚ, соның ішінде телевизия және интернет ресурстары (пошта байланысы, әлеуметтік желілер, блогтар және бейне порталдар) танымалдығына байланысты халықтың қоғамдық санасына ақпараттық әсер етудің нақты

қаупі бар. Ақпараттық ықпал етуді Қазақстан Республикасының ұлттық мүдделеріне қайшы келетін идеяларды тікелей сол қалпында, сондай-ақ ақпараттық ақпаратты немесе оның үрдістік түсіндірмелерін жасанды түрде ұстап тұру арқылы белгілі бір ақпараттар қалыптастыру түрінде де көрсетуге болады. Қоғамдық сананы осындай манипуляциялауға қарсы тұру үшін мемлекеттік ақпараттық саясаттың тиімділігін арттыру, мемлекеттік органдардың ашықтығын арттыру және азаматтардың ақпаратқа деген құқығын қорғауды арттыру қажет.

Түйін сөздер: Ақпараттандыру, байланыс, меншік иесі, ұлттық қауіпсіздік, компьютер, ұстап қалу, компьютерлік деректер, қылмыстық құқық бұзушылық.

B.B. Doszhanov [1]
[1] Abai Kazakh National Pedagogical University

OBJECTIVE SIGNS OF CRIMINAL OFFENSES IN THE SPHERE OF INFORMATIZATION AND COMMUNICATION

Abstract

The article covers issues related to those changes occurring in the economic life and the financial and credit system, enterprises of various forms of ownership, etc. - having a significant impact on the protection of information. For a long time in our country there was only one property - state property, therefore information and secrets were also state only, which were guarded by special services.

In connection with the openness of the national information space and the popularity of foreign media, including television and Internet resources (postal services, social networks, blogs and video portals), there is a real threat of information impact on the public consciousness of the population.

Information impact can be expressed both in the form of direct imposition of ideas that contradict the national interests of the Republic of Kazakhstan, and in the form of creating a certain information background artificially maintained by manipulating information or its tendentious commenting. To counteract such manipulation of public consciousness, it is required to seriously improve the effectiveness of the state information policy, increase the openness of state bodies, and increase the security of citizens' right to information.

Keywords: Informatization, communication, owner, national security, computer, interception, computer data, criminal offense.

Введение

Всестороннее изучение объекта рассматриваемой главы 7 «Уголовные правонарушения в сфере информатизации и связи» УК РК позволяет выяснить юридическую и социальную сущность этих посягательств, определить границы действия уголовно-правовой нормы, установить общественно опасные последствия, что способствует правильной квалификации и разграничению данных уголовных правонарушений от других уголовных правонарушений и преступлений.

Закон РК «Об информации, информатизации и защите информации» дает ряд исходных определений, из которых вытекает, что: 1) информация (данные) - это любые сведения о лицах, предметах, фактах, событиях, явлениях и процессах независимо от формы их представления; 2) уголовным законом (как и законодательством, вообще) защищается документированная информация, т.е.: а) закрепленная на материальном носителе, б) имеющая реквизиты, позволяющие установить источник получения и передачи; 3) применительно к компьютерной информации речь идет о самостоятельном машинном ее носителе (магнитная лента, магнитный или оптический диск и т.д.) либо о носителе электронно-вычислительной машины (жесткий магнитный диск), в ее оперативной памяти, в коммуникациях системы или сети. Указание закона на способность информации к идентификации означает, что машинная

информация, предназначенная для операций в условиях, не дающих возможность установить источник возникновения и передачи, уголовно-правовой защите не подлежит [1, с.325].

Преступные действия с компьютерной информацией могут быть элементом деяний по незаконному прослушиванию телефонных переговоров и иных сообщений, по неправомерному контролю почтовых сообщений и отправлений, по нарушению неприкосновенности частной жизни, по нарушению неприкосновенности частной жизни, по нарушению изобретательских и патентных прав в части разглашения сведений, составляющих коммерческую или банковскую тайну. Использование компьютерной информации может быть связанно с государственной изменой, шпионажем, публичными призывами к развязыванию агрессивной войны, заведомо ложными сообщениями о готовящихся актах терроризма.

Законность операций с информацией вообще и компьютерной в частности определяется: а) инициативой или согласием собственника или иного частного владельца информации; б) наличием законного допуска к осуществлению операций; в) соблюдением правовых предписаний об операциях с конфиденциальной информацией различных видов; г) соблюдением правовых требований эксплуатации компьютеров, их систем и сетей.

Закон об информации имеет специальную главу о защите информации и прав субъектов, участвующих в работе с ней. Целями защиты провозглашаются:

- предотвращение утечки, хищения, утраты, искажения, подделки информации;

- предотвращение угроз безопасности личности, общества, государства, в том числе защита конституционных прав граждан, сохранение государственной, служебной, иной тайны, предусмотренной законом;

- обеспечение прав информационных процессов. Способы защиты информации и прав субъектов работы с нею различаются «с учетом специфики правонарушений и нанесенного ущерба». Этот критерий использован и при определении границ уголовно-правового регулирования борьбы с преступлениями в сфере компьютерной информации. А именно установление уголовной ответственности предполагает материальные составы, связанные с наличием существенного или тяжкого вреда.

Родовым объектом являются общественные отношения, нарушающие формирование и использование автоматизированных информационных ресурсов и средств их обеспечения. В родовой объект в свою очередь входят несколько объектов, охватывающих права и законные интересы: а) владельцев (в том числе собственников) и пользователей информации, компьютеров, их систем и сетей, средств обеспечения;

б) физических и юридических лиц, сведения о которых имеются в автоматизированных информационных ресурсах (банках данных);

в) общества и государства, в том числе интересы национальной безопасности. В частности, применительно к гражданам объектом посягательства могут быть здоровье (например, при нарушений работы информационной системы или сетей телекоммуникаций), имущественные права, право на личную тайну и тайну сообщений, честь и достоинства личности.

Проблемы информационной безопасности постоянно усугубляется процессами проникновения практически во все сферы деятельности общества технических средств обработки и передачи данных и прежде всего вычислительных систем. Это дает основание поставить проблему компьютерного права, одним из основных аспектов которой являются так называемые компьютерные посягательства. Об актуальности проблемы свидетельствует обширный перечень возможных способов компьютерных преступлений [2, с.176].

Объектами посягательств могут быть сами технические средства (компьютеры и периферия) как материальные объекты, программное обеспечение и базы данных, для которых технические средства являются окружением.

Таким образом, в соответствии со сложившимся на сегодня международным подходом, киберпреступность можно разделить на следующие категории:

- Преступления против конфиденциальности, целостности и доступности компьютерных систем и данных (так называемые «CIA-преступления»), включая;
- неправомерный доступ, например, путем взлома, обмана и иными средствами;
- неправомерный перехват компьютерных данных;
- воздействие на данные, включая повреждение, удаление, ухудшение качества, изменение или блокирование компьютерных данных;
- воздействие на функционирование системы, включая создание серьезных помех функционированию компьютерной системы, например, путем распределенных атак на ключевую информационную инфраструктуру типа отказ в обслуживании;
- противозаконное использование устройств, то есть, например, производство, продажа или иные действия, направленные на обеспечение доступности программ, устройств и иных средств, предназначенных для совершения «CIA-преступлений».
- Преступления, совершенные при помощи компьютерных систем, включая:
- подлог и мошенничество, совершенные с использованием компьютерных технологий;
- преступления, связанные с содержанием данных, в частности - детская порнография, детская эксплуатация и сексуальное насилие, расизм, ксенофобия, а также консультирование, подстрекательство, содействие путем указаний и предложение совершить преступление, начиная с убийства и кончая изнасилованием, пытками, диверсией и терроризмом. Под эту же категорию подпадают кибервымогательство, запугивание, клевета, распространение ложной информации в Интернете, азартные игры онлайн;
- преступления, связанные с нарушением авторских и смежных прав, например, незаконное воспроизводство и использованием компьютерных программ, аудио/видео и иных видов цифровой формы, а также баз данных и книг.

Обсуждение и результаты

При определении родового объекта уголовных правонарушений,посягающих на безопасность компьютерной информации,необходимио согласиться с мнением таких ученых как М.С.Строговича и Ю.М. Батурина, которые в своей работе «Компьютерная преступность и компьютерная безопасность» указывают, что правильно будет считать объектом значительной часть компьютерных правонарушений отношения общественной безопасности.

Отсутствие соответствующих потребностям государства, бизнеса и общества отечественных информационных технологий приводит к вынужденному использованию иностранного оборудования и информационных систем. В результате этого повышается вероятность несанкционированного доступа к базам и банкам данных, а также возрастает зависимость страны от иностранных производителей компьютерной и телекоммуникационной техники и программного обеспечения[3,с.354].

Общественная безопасность, будучи своего рода собирательным понятием, включает в себя различные составляющие. В этой связи юридическая природа уголовных правонарушений, посягающих на безопасность компьютерной информации, заключается в том что они объединяют действия, ставившие под угрозу причинения вреда другим общественным отношениям, в результате чего образуется качественно новое уголовное правонарушение в данной сфере.

Объектом неправомерного доступа к компьютерной информации, как указано в Комментарии к Уголовному Кодексу Республики Казахстан являются права на информацию ее владельца и третьих лиц.

Непосредственным объектом ее являются общественные отношения по обеспечению безопасности компьютерной информации и нормальной работы электронного носителя: информационной системы или сети телекоммуникаций. Предметом преступления будет компьютерная (машинная) информация: содержащаяся в информационной системе: в

электронном носителе: информационной системе или сети телекоммуникаций: охраняемая законом иными словами изъятая из открытого оборота на основании Закон Республики Казахстан «Об информатизации» иного нормативного правового акта, а также правил внутреннего распорядка: основанных на названных правовых актах.

Состав преступления сформулирован как материальный: причем если деяние в форме действия определено однозначно (неправомерный доступ к охраняемой законом компьютерной информации), то последствия хотя и обязательны, могут быть весьма разнообразны:

1) уничтожение информации:
2) ее блокирование:
3) модификация:
4) копирование:
5) нарушение работы информационной системы:
6) то же - для системы электронного носителя:
7) то же - для их сети.

Деяние: как видно из диспозиции статьи: предполагает наличие двух обязательных признаков - информация должна охраняться законом: а доступ к ней должен быть неправомерен: т.е. пользователь электронного носителя не имел права вызывать ее: знакомиться с ней: а тем более распоряжаться ею. Среди способов совершения такого доступа можно назвать: использование чужого имени: изменение физического адреса технического устройства: подбор пароля: нахождение и использование «пробелов» в программе: любой другой обман системы защиты информации. Вопрос о том: когда окончено данное деяние: должен решаться так. Моментом окончания его является момент отсылки пользователя компьютеру последней интерфейсной команды (голосовой: нажатием клавиши) вызова хранящейся информации: независимо от наступления дальнейших последствий. Однако преступлением это деяние станет только лишь при наличии последнего условия. Все действия: выполненные до подачи последней команды: будут образовывать состав неоконченного преступления. Что касается преступных последствий: то под уничтожением информации следует понимать такое изменение её состояния, при котором она перестает существовать в силу утраты основных качественных признаков. Под блокированием - невозможность доступа к ней со стороны законного пользователя. Под модификацией - видоизменение: характеризующееся появлением новых (очевидно: нежелательных) свойств. Под копированием - получение точного или относительно точного воспроизведения оригинала (опять-таки без соответствующей санкции). Под нарушением работы - остановку действия программы: ее зацикливание замедление работы, нарушение порядка выполнения команд, ущерб самой аппаратной части и другие последствия.

Непосредственным объектом данного преступного деяния являются общественные отношения, обеспечивающие безопасность информационных систем от внешних воздействий сточки зрения конфиденциальности содержащейся в них компьютерной информации. Конфиденциальность понимается как предотвращение возможности использования информации лицами, которые не имеют к ней отношения. Предметом преступления является компьютерная информация, охраняемая законом, находящаяся либо на машинном носителе, либо в информационной системе, либо в системе электронного носителя или в сети телекоммуникации. Объективная сторона данного преступления характеризуется деянием, последствием и причинной связи между ними. Деяние выражается в неправомерном доступе к компьютерной информации. Доступом к информационной системе является санкционированное и упорядоченное собственником информационной системы взаимодействие лица с устройствами электронного носителя и (или) ознакомление лица сданными, содержащимися на машинных носителях или в сети телекоммуникации. Регламентация порядка доступа к компьютерной информации устанавливается ее собственником в его внутренних нормативных актах, которые доводятся до сведения

пользователей информации. Такая регламентация может содержаться также в договорах или соглашениях с пользователями информационных ресурсов. Нарушение установленного собственником информации порядка образует неправомерность доступа к компьютерной информации. Существенно, что современные информационные системы, как правило, обладают инструментами разграничения доступа для различного круга пользователей. Это создает предпосылки для оценки действий как неправомерного доступа и для случаев, когда пользователи, имеющие доступ к строго определенной части информационной системы, вторгаются в иные ее элементы, не имея для этого прямо выраженного согласия собственника системы. Особо следует отметить компьютерную информацию, собственником которой является государство или его субъекты и образования. К государственной конфиденциальной информации относятся в частности служебная тайна, государственная тайна, данные предварительного следствия, сведения о мерах безопасности, применяемых в отношении судьи и участников уголовного процесса, сведения о мерах безопасности, применяемых в отношении должностного лица правоохранительного или контролирующего органа. Подобная информация охраняется государством непосредственно в силу соответствующего закона[4, с.245].

Мы выделили три общих признака, присущих неправомерному доступу:

1.Неправомерность доступа.

2.Проникновение к компьютерной информации.

3.Получение возможности ознакомления лица с компьютерной информации и последующего распоряжения ею.

Признак неправомерности предполагает под собой несоответствие определенных явлений социальной жизни требованиям и дозволения, в частности отсутствие у лица, осуществляющего доступ, разрешения (санкции) собственника или держателя компьютерной информации.

Второй признак неправомерного доступа характеризуется проникновением виновного лица к компьютерной информации. Проникновение к компьютерной информации будет иметь место в тех случаях, когда, например, лицо проникает в какое либо помещение, где электронный носитель находиться в рабочем режиме.

К третьему признаку неправомерного доступа можно охарактеризовать подобным образом - доступ характеризуется как деяние с момента начала фактического проникновения к компьютерной информации до получения реальной возможности манипулировать данной информацией.

Выделение определенного порядка, характеризующего неправомерный доступ, можно считать необоснованным, поскольку для установления определенного порядка доступа необходимо наличие нормативно-правового акта. Как правило, это присуще государственным органам, а также крупным частным хозяйствующим субъектам (акционерные общества, товарищества с ограниченной ответственностью и так далее).

Состав неправомерного доступа к охраняемой законом компьютерной информации сконструирован как материальный, то есть такой состав, в котором предусматривается либо фактическое наступление определенного последствия, либо возможного наступления.

Следует различать преступную деятельность по захвату информационной системы, систем телекоммуникаций и машинных носителей с целью завладения ими как имуществом, имеющим самостоятельную материальную ценность, в не связи с тем, какая информация на них находится, и деятельность, совершаемую с целью доступа к компьютерной информации, связанную с изъятием указанных предметов как носителей этой информации. В первом случае такую деятельность при известных условиях необходимо отнести к преступлениям в сфере экономики. Преступная деятельность, направленная на противоправное причинение ущерба компьютерной информации, является неправомерным доступом независимо от способа доступа. Поэтому утверждения о том, что «не образует объективной стороны... уничтожение или искажение компьютерной информации путем внешнего воздействия на машинные носители теплом, магнитными волнами, механическими ударами...» представляются не верными.

Состав неправомерные уничтожение или модификация информации (ст.206 УК РК) и носит материальный характер и предполагает обязательное наступление одного из последствий: а) уничтожение информации - это приведение информации или ее части в непригодное для использования состояние независимо от возможности ее восстановления. Уничтожением информации не является переименование файла, где она содержится, а также само по себе автоматическое «вытеснение» старых версий файлов последними по времени; б) блокирование информации - результат воздействия на компьютерную информацию или технику, последствием которого является невозможность в течение некоторого времени или постоянно осуществлять требуемые операции над компьютерной информацией полностью или в требуемом режиме, то есть совершение действий, приводящих к ограничению или закрытию доступа к компьютерному оборудованию и находящимся на нем ресурсам, целенаправленное затруднение доступа законных пользователей к компьютерной информации, не связанное с ее уничтожением; в) модификация информации - внесение изменений в компьютерную информацию (или ее параметры).

Законом установлены случаи легальной модификации программ (баз данных) лицами, правомерно владеющими этой информацией, а именно: модификация в виде исправления явных ошибок; модификация в виде внесения изменений в программы, базы данных для их функционирования на технических средствах пользователя; модификация в виде частной декомпиляции программы для достижения способности к взаимодействию с другими программами; г) копирование информации - создание копии имеющейся информации на другом носителе, то есть перенос информации на обособленный носитель при сохранении неизменной первоначальной информации, воспроизведение информации в любой материальной форме - от руки, фотографированием текста с экрана дисплея, а также считывания информации путем любого перехвата информации и т.п.

Объективная сторона преступления включает альтернативные действия, состоящие: а) в создании программ, заведомо предназначенных для несанкционированного уничтожения, блокирования, модификации, копирования компьютерной информации или нейтрализации средств ее защиты; б) в распространении таких программ или машинных носителей с такими программами; в) в использовании таких программ или машинных носителей с ними. Создание программ представляет собой деятельность, направленную на разработку, подготовку программ, способных по своему функционалу несанкционированно уничтожать, блокировать, модифицировать, копировать компьютерную информацию или нейтрализовать средства защиты компьютерной информации.

Более того, невозможно будет провести четкую грань между уничтожением компьютерной информации и ее модификации (изменением) как наступившими общественно опасными последствиями. Поэтому данный признак (изменение информации) необходимо относить к модификации компьютерной информации.

Нарушение работы информационной системы или сетей телекоммуникаций (ст.207 УК РК). Непосредственным объектом данного преступного деяния являются общественные отношения, обеспечивающие внутреннюю безопасность информационных систем, базирующихся на использовании информационной системы, системы электронных носителей или сети телекоммуникаций с точки зрения целостности и конфиденциальности, содержащейся в них компьютерной информации. Иными словами, интерес владельца компьютерной системы или сети относительно правильной эксплуатации системы или сети. Существует два вида правил эксплуатации информационной системы, которыми должны руководствоваться в своей деятельности лица, работающие с электроннными носителями. Первый вид правил - инструкции по работе с информационными системами и машинными носителями информации, разработанные изготовителем электронных носителей и периферийных технических устройств, поставляемых вместе с данным экземпляром

электронно-вычислительной машины. Эти правила обязательны к соблюдению пользователем электронного носителя под угрозой, как минимум, потери прав на гарантийный ремонт и обслуживание. Второй вид правил - правила, установленные собственником или владельцем информационных ресурсов, информационных систем, технологий и средств их обеспечения, определяющие порядок пользования информационной системой, системой электронного носителя и сети телекоммуникации, а также иными носителями информации.

Объективная сторона данного деяния заключается в действиях или бездействии лица, которое в соответствии с правилами, установленными собственником информационной системы, обязано было осуществлять операции с компьютерной информацией в определенном порядке, но не соблюдало эти правила, и это послужило причиной уничтожения, блокирования или модификации информации, понятия которых давались ранее. Понятие существенного вреда является оценочным и установление объема, причиненного собственнику информационной системы вреда в результате воздействия вредоносных программ или нарушения правил эксплуатации информационной системы будет осуществляться судом с учетом совокупности полученных данных. Следует правильно различать последствия воздействия на компьютерную информацию, причинившие вред информационным ресурсам, и вред, причиненный преступными действиями в целом. Так, например, при изменении данных в информационной системе (в частности, данных учета движения товарно-материальных ценностей) с целью совершения их хищения вред, наносимый информационной системе, определяется затратами собственника системы на восстановление правильного учета. Вред, нанесенный непосредственно хищением, является самостоятельным видом вреда, причиненного криминальной деятельностью.

При правильной оценке данной разновидности преступной деятельности как направленной на причинение ущерба компьютерной информации, не могут быть квалифицированы как нарушение правил эксплуатации электронного носителя действия, связанные с использованием средств и элементов информационного оборудования при совершении с ними или с их помощью действий, не относящихся к обработке информации. Как уже указывалось, доступом к информационной системе является санкционированное и упорядоченное собственником информационной системы взаимодействие лица с устройствами электронно-вычислительной машины и (или) ознакомление лица сданными, содержащимися на машинных носителях или в информационной системе. Совершение указанных действий лицом, имеющим доступ к информационной системе, рассматривается законодателем как отягчающее наказание обстоятельство, поскольку совершение преступления с использованием доверия, оказанного виновному в силу его служебного положения или договора, признается таковым[5, с.428].

Неправомерный доступ будет иметь место в случаях, когда лицо, не являясь собственником или иным законным владельцем компьютерной информации, имеет право на работу с ней либо имеет доступ к работе с данным банком информации, но ограничено в объеме операций и вторгается в ту часть банка данных, которая для него закрыта. Неправомерным проникновением к компьютерной информации будут действия лица, имеющего допуск к операциям соответствующего ранга, если доступ осуществлен с нарушением правил работы с данным компьютером, системой, сетью, обеспечивающими устройствами, например, с отключением систем безопасности, с игнорированием физических условий, создавшихся в месте работы (например, высокой температуры), которые заведомо угрожают сохранности информации. По мнению А.Шукан, объективная сторона преступления охватывает любой способ неправомерного проникновения к охраняемой законом компьютерной информации, который всегда связан с совершением определенных действий и может выражаться в проникновении в компьютерную систему путем: использования технических или программных средств, позволяющих преодолеть установленные системы защиты; незаконного использования паролей или кодов для проникновения в компьютер либо

совершение иных действий в целях проникновения в систему или сеть под видом законного пользователя; хищение носителей информации при условии, что были приняты меры к их охране, если это - деяние повлекло уничтожение или блокирование информации[6, с.71-77].

Закон указывает на следующие варианты действий виновного, которые повлекли: уничтожение, блокирование, модификацию, копирование информации, нарушение работы информационной системы, их системы или сети. Таким образом, неправомерный доступ - сложное понятие, включающее действия по: а) "физическому" проникновению, дающему возможность по своему усмотрению оперировать данным объемом компьютерной информации; б) несанкционированным операциям с компьютерной информацией.

Предметом преступного посягательства по статье 208 УК РК являются:

- Компьютерная информация, под которой в уголовно-правовом аспекте понимаются сведения (сообщения, данные), представленные в форме электрических сигналов, независимо от средств их хранения, обработки и передачи.

- Имущество, то есть совокупность вещей, которые находятся в собственности лица (включая деньги и ценные бумаги), а также имущественных прав на получение вещей или имущественного удовлетворения от других лиц.

- В случае если лицо оперировало сведениями, не относящимися к компьютерной информации (в понимании уголовного закона), либо его действия не были связаны с завладением имуществом, а преследовали иные цели, например, создание препятствий в реализации прав собственника, уголовная ответственность по статье 208 УК РК исключается.

- Уголовно-наказуемыми по статье 208 УК РК являются лишь нижеперечисленные способы завладения имуществом:

- Ввод компьютерной информации, то есть размещение сведений в устройствах электронного носителя информационной системы для их последующей обработки и (или) хранения.

- Удаление компьютерной информации, то есть совершение действий, в результате которых становится невозможным восстановить содержание компьютерной информации, и (или) в результате которых уничтожаются носители компьютерной информации.

- Блокирование компьютерной информации, то есть совершение действий, приводящих к ограничению или закрытию доступа к компьютерной информации, но не связанных с ее удалением.

- Модификация компьютерной информации, то есть совершение любых изменений сведений (сообщений, данных), представленных в форме электрических сигналов, независимо от средств их хранения, обработки и передачи.

- Вмешательство в функционирование:

- средств хранения,

- средств обработки,

- средств передачи компьютерной информации,

- информационно-телекоммуникационные сети.

Под вмешательством в функционирование следует понимать осуществление неправомерных действий, нарушающих установленный процесс обработки, хранения, использования, передачи и иного обращения с компьютерной информацией.

Следует отметить, что на практике конструкция статьи 208 УК РК не всегда будет охватывать собой «типичные» схемы хищения чужого имущества с использованием компьютерной техники и информации, а будет применяться к виновному лицу в совокупности с иными статьями Уголовного кодекса Республики Казахстан.

Понятие «вредоносная программа» для уголовного законодательства Рес-публики Казахстан и в целом для всего законодательства является новым. По смыслу диспозиции ст.210 УК РК вредоносная программа представляет собой программу для информационной системы,

заведомо проводящую к несакционированному уничтожению, блокированию, модификации либо копированию информации, нарушению работы информационной системы, систем электронного носителя или сетей телекоммуникаций. Понятие программы для электронного носителя информационной системы дается в законодательстве, в частности, в законе Республики Казахстан «Об авторском праве и смежных правах», как набор инструкций или правил, выраженных словами, цифрами, кодами, символами, знаками, диаграммами или в какой-либо другой форме, которые могут быть использованы в электронной вычислительной машине (ЭВМ) или другим компьютерным устройством с целью достижения желаемого результата, включая также подготовительные материалы, полученные в процессе разработки программы для информационной системы и порождаемые ею ауидиовизуальные отображения. «Компьютерный вирус» - термин, предложенный профессором Университета Южной Калифорнии Фредом Коэном, представляет собой программу, характеризующуюся способностью скрытого внедрения и саморазмножения с целью поражения (инициирования) программ, локализованных на винчестере компьютера или другом носителе информации.

Использование программы для информационной системы - это выпуск ее в свет, воспроизведение и иные действия по введению ее в хозяйственный оборот в изначальной или модифицированной форме, а также самостоятельное применение этой программы по назначению. Использование вредоносной программы для информационной системы, для личных нужд (например, для уничтожения собственной компьютерной информации) не наказуемо.

Распространение программы для информационной системы - это предоставление доступа к воспроизведенной в любой материальной форме программе для электронно-вычислительной машины, в том числе сетевыми и иными способами, а также путем продажи, проката, сдачи внаем, предоставления взаймы, а также создание условий для самораспространения программы.

Неправомерные изменение идентификационного кода абонентского устройства сотовой связи, устройства идентификации абонента, а также создание, использование, распространение программ для изменения идентификационного кода абонентского устройства (ст.213 УК РК), общественная опасность преступления определяется значимостью высоких технологий абонентского устройства сотовой связи в экономической деятельности общества, в результате чего причиняется значительный ущерб организациям или отдельным гражданам.

Законодательством Республики Казахстан предусматривается, что «физические и юридические лица, допустившие повреждения средств связи, сооружений и сетей телекоммуникаций, нарушение установленного порядка изготовления, приобретения, ввоза, использования и регистрации радиоэлектронных средств и высокочастотных устройств, использования радиочастот для работы радиоэлектронных средств всех назначений и высокочастотных устройств, а также создающие ненормированные помехи теле и радиоприему, несут ответственность в установленном законом порядке (ст.28 Закона РК «О связи» от 18 мая 2009 г. с целью снижения уровня хищения телефонов сотовой связи и исключения возможности беспрепятственного и неправомерного их использования была введена данная уголовно-правовая норма Законом РК от 8 января 2007 г. Объектом данного преступления являются общественные отношения, связанные с правом собственности производителя, а также отношения, складывающиеся в сфере регулирования прав и законных интересов пользователей услугами связи, уполномоченных органов и хозяйствующих субъектов, осуществляющих деятельность в области связи. Неправомерное изменения идентификационного кода абонентского устройства сотовой связи, создание дубликата карты идентификации абонента сотовой связи, создание, использование, распространение программ для указанных целей, безусловно нарушает порядок распределения ресурса нумерации и выделения номеров сотовой связи, оказывает разрушительное воздействие на установленные правила получения прав пользования номерами телефонов указанной связи. Под телефонами

сотовой связи (абонентское устройство, устройство сотовой связи) следует понимать оконечное сертифицированное оборудование абонента, подключенное к сетям радиосвязи для приема и передачи информации, имеющее идентификационный код абонентского устройства и устройства идентификации абонента.

Электрическая связь (телекоммуникация) - передача или прием знаков, сигналов, голосовой информации, письменного текста, изображений, звуков по проводной, радио, оптической и другим электромагнитным системам.

Абонент - пользователь услугами связи, с которым заключен договор об оказании таких услуг при выделении для этих целей абонентского номера или кода идентификации. Под идентификационным кодом абонентского устройства сотовой связи понимается IMEI, который расшифровывается как International Mobile Equipment Identifier, что в переводе означает «международный идентификатор мобильного оборудования». Иначе, идентификационным кодом абонентского устройства (IMEI), является число состоящее из 15 цифр, представляющее собой уникальный серийный номер каждого телефона формата GSM (Глобальная система мобильной связи), который автоматически передается аппаратом в сеть оператора при подключении. Он устанавливается на заводе при изготовлении и служит для точной и полной идентификации устройства в GSM сети.

Устройство идентификации абонента в сотовом телефоне (карта идентификации абонента) предназначено для индивидуализации аппарата сотовой связи и абонента, приобретается независимо от телефона, регистрируется на физическое лицо и устанавливается в корпус аппарата со строго установленным номером. Иначе, данное устройство именуются как Сим-карта.

Заключение

С объективной стороны данного преступления действия виновного выражаются в неправомерном изменении идентификационного кода абонентского устройства сотовой связи, устройства идентификации абонента, а также создание, использование, распространение программ для изменения идентификационного кода абонентского устройства. Несовпадение идентификационного кода абонентского устройства сотовой связи (IMEI) может быть только в двух случаях: либо он был изменен при «перепрошивке» телефона, либо была проведена полная замена корпуса (не сменных панелей, а именно корпуса). Замена корпуса сотового телефона равнозначна стоимости нового телефона. В то же время технические средства связи, используемые на единой сети телекоммуникаций Республики Казахстан, радиоэлектронные средства и высокочастотные устройства, являющиеся источником электромагнитного излучения, подлежат обязательной сертификации в соответствии с законодательством РК. Перечень средств связи, подлежащих обязательной сертификации, определяется уполномоченным органом по согласованию с органами национальной безопасности и уполномоченным органом по стандартизации, метрологии и сертификации. Таким образом, под неправомерным изменением без согласия производителя или законного владельца идентификационного кода абонентского устройства сотовой связи следует понимать самовольную с применением электронно-технических средств переустановку 15-значного серийного номера телефона формата GSM. Замена указанного номера может быть произведена полностью либо путем хаотичного внесения замены какой-то цифры из заданного числового ряда. Уполномоченный орган разрабатывает и утверждает правила, устанавливающие порядок получения прав пользования номерами, в том числе определяет основания присвоения номеров, ведет реестр распределенных и резервных ресурсов нумерации. Создание дубликата карты идентификации абонента сотовой связи виновным лицом в нарушении установленных правил путем подделки Сим-карты, сканирования профиля Сим-карты либо имитации ее действия под номер другого абонента также составляет объективную сторону рассматриваемого состава преступления. По конструкции состав

рассматриваемого деяния является формальным. Данное преступление считается оконченным с момента совершения действий, предусмотренных настоящей нормой, независимо от наступления преступных последствий.

Например, как показывает практика, наиболее распространенное преступное деяние в виде хищения «электронных денег» состоит из нескольких «технических стадий»:

- неправомерного завладения компьютерной информацией (ключ доступа, логин, пароль и т.п.);
- использование похищенной компьютерной информации в целях присвоения чужого имущества.

«Первая стадия», как правило, заключается в неправомерном копировании компьютерной информации, ответственность за которое предусмотрена ст. 206 УК РК, либо в неправомерном использовании вредоносного программного обеспечения, что преследуется по закону в соответствии со ст.207 УК РК.

«Вторая стадия» - это уже непосредственное использование полученной неправомерным путем компьютерной информации в целях хищения имущества потерпевшего.

Квалификация по объективной стороне невозможна без установления причинной связи. Причинная связь представляет собой объективно существующую категорию, которая выражает внутреннею связь и зависимость между общественно опасным действием и наступившим в результате этого вредными последствиями.

В странах зарубежья неправомерный доступ к компьютерной информации уже влечет самостоятельную уголовную ответственность, что мы считаем более верным исходя из того , что виновному лицу может быть достаточно лишь ознакомиться с находящиеся в компьютере информации.

Список использованной литературы:

1. Сеитов Т. Б. Правовые аспекты компьютерной преступности в зарубежных странах и в Казахстане: Учебное пособие. - Алматы: Данекер, 2013.-450 с.

2. Ткачев А. В. Правовой статус компьютерных документов: Основные характеристики. – М.: Городец-издат, 2010. -282 с.

3. Строгович М. С. Курс советского уголовного процесса. Т. 2. - М.: Наука, 1980. -1050 с.

4. Толеубекова Б. Х. Уголовно-процессуальное право Республики Казахстан. Часть общая: Учебник. - Алматы: Баспа, 2008.-705 с.

5. Уголовное право. Особенная часть: Учебник для вузов / Под ред. Н.И.Ветрова, Ю.И.Ляпунова. – М: Новый юрист, 2013.-1204 с.

6. Шукан Алия. Қылмыстық саясат және құқық қолдану үрдісін жетілдіру мәселелері. //Хабаршы-Вестник-Bulletin КазНПУ имени Абая №2 (48), Серия «Юриспруденция». - Алматы, 2017. - С.71-77.