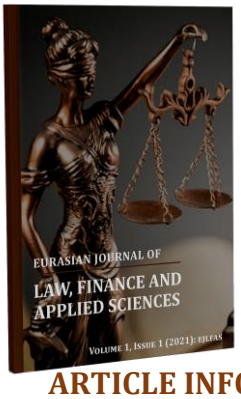
EURASIAN JOURNAL OF LAW, FINANCE AND APPLIED SCIENCES
Innovative Academy Research Support Center
UIF = 8.3 | SJIF = 5.961 www.in-academy.uz



УГОЛОВНАЯ ОТВЕТСТВЕННОСТЬ ЗА ПРЕСТУПЛЕНИЯ В СФЕРЕ ИНФОРМАЦИОННЫХ ТЕХНОЛОГИЙ

Р. Кабулов
Профессор кафедры Уголовного права
Академии МВД Республики Узбекистан
доктор юридических наук, профессор
https://doi.org/10.5281/zenodo.8166479

ARTICLE INFO

Received: 10th July 2023
Accepted: 15th July 2023
Online: 19th July 2023

KEY WORDS

ABSTRACT

В новом Узбекистане формирование национальной системы информатизации, массового внедрения и использования во всех сферах экономики и жизни общества современных информационных технологий, средств компьютерной техники и телекоммуникаций, наиболее полного удовлетворения растущих информационных потребностей граждан, создания благоприятных условий для вхождения в мировое информационное сообщество и расширения доступа к мировым информационным ресурсам являются приоритетными направлениями развития современного общества. И в силу этого Президент страны Шавкат Мирзиёев подчеркнул: «В целях устойчивого развития мы должны глубоко освоить цифровые знания и информационные технологии, что это даст нам возможность идти по самому короткому пути к достижению всестороннего прогресса. В современном мире цифровые технологии играют решающую роль во всех сферах». А также далее указал: «Широкое внедрение цифровых технологий способствует эффективности государственного и общественного управления, развитию социальной сферы, одним словом, кардинальному улучшению жизни людей»[1].

Вместе с тем, с развитием определенной сферы жизни общества появляются желающие воспользоваться новыми технологиями и нелегальным способом удовлетворить свои потребности. Это, в свою очередь, способствует появлению такого нового вида преступной деятельности, как преступления в сфере информационных технологий, которые на современном этапе достигли достаточно высокого уровня. Так, в мире киберпреступники средном в год причиняет ущерб на 113 млрд. долларов. По оценкам Сбербанка ущерб ежегодно от киберпреступности во всех сферах деятельности, например в Российской Федерации составляет около 1,5 млрд. долларов, в Великобритании 48,5 млрд. долларов. За 2017 год было совершено 241.123 хакерских атак, 16643 вандализма сайтов, 176602 случаев распространения вирусов и взлома

[1] Послание Президента Республики Узбекистан Шавката Мирзиёева Олий Мажлису (24 января 2020 года) https://nrm.uz/contentf?doc=612860_

информационных систем и сетей[2]. Приведенные статистические данные свидетельствуют о повышенной опасности преступлений в сфере информационных технологий. Дело еще стоит хуже тем, что с ростом совершенства компьютерной техники возрастает изощренный характер компьютерной преступности.

В Республике Узбекистан до недавнего времени считалось, что компьютерная преступность — явление, свойственное только зарубежным развитым странам, и по причине слабой компьютеризации нашего общества данная преступность не имела места. Теперь в современном Узбекистане складывается иная ситуация. Компьютеризация общества, затрагивающщая практически все стороны деятельности людей, предприятий и организаций, государства, породила новую сферу общественных отношений, которая, к сожалению, нередко становится объектом противоправных деяний. Следовательно компьютерная информационная система являясь объективным отражателем состояния различных отраслей хозяйства, а также обороноспособности страны, остро нуждается в средствах обеспечения правовой безопасности от несанкционированного проникновения в эту систему криминальных элементов, которые могут нанести ей громадный финансово-материальный ущерб. Учитывая эти обстоятельства, Законом Республики Узбекистан «О внесении изменений и дополнений в некоторые законодательные акты Республики Узбекистан в связи с усилением ответственности за совершение незаконных действий в области информатизации и передачи данных» от 30 ноября 2007 г опасные деяния, связанные с незаконным использованием компьютерных систем, криминализованы и действующий Уголовный кодекс дополнен новой главой XX' «Преступления в сфере информационных технологий», которая отнесена законодателем к разделу шестому Особенной части УК «Преступления против общественной безопасности и общественного порядка».

Реалии современного общественного развития, переход на методы электронного управления технологическими процессами, придание юридической силы актам, осуществляемым с помощью ЭВМ, создали предпосылки использования этих процессов для совершения преступлений в сфере информационных технологий. Противоправное вмешательство в работу компонентов телекоммуникационных сетей, функционирующих в их среде компьютерных программ, несанкционированная модификация и уничтожение компьютерной информации может дезорганизовать работу критически важных элементов инфраструктуры государства и создает опасность гибели многих людей, причинение невосполнимого имущественного ущерба или иные общественно опасные последствия. Более того, компьютерная телекоммуникация и сеть Интернет сами могут быть использованы в качестве орудие или средство совершения тяжких и особо тяжких преступления. В этой связи Президент страны Шавкат Мирзиёев предупреждая нас отметил, что: «Сейчас во всем мире терроризм, экстремизм и другие угрозы перешли в интернет-пространство и адаптировались в нем. Поэтому бороться с ними все сложнее. К сожалению, у

[2] Расулев А.К., Некоторые вопросы совершенствования уголовно-правовых и криминологических мер борьбы с преступлениями в сфере информационных технологий и безопасности. Ташкент, ТГЮУ, 2017. С. 6-7.

некоторых юношей и девушек низки культура и навыки правильного пользования Интернетом. Правда и то, что некоторые юноши и девушки воспринимают Интернет не источником знаний и просвещения, а средством для развлечений. В таком идеологическом противостоянии наша молодежь должна быть бдительной, в любой ситуации принимать решения исходя прежде всего из интересов Родины»[3].

Преступления в сфере информационных технологий — это не только нарушение неприкосновенности интеллектуальной собственности, но и разглашение сведений о частной жизни граждан, причинение имущественного ущерба в виде прямых убытков и неполученных доходов, потеря репутации фирмы, различные виды нарушений правомерной деятельности организаций, предприятий, учреждений и тд. На основании этого можно утверждать, что преступления данного вида посягают на отношения, обеспечивающие правомерное, безопасное использование информационных технологий,

Общим объектом преступного посягательства, связанным с неправомерным использованием информационных тсхнологий, будет выступать совокупность всех общественных отношений, охраняемых уголовным законом; родовым — общественная безопасность и общественный порядок и совокупность общественных отношений по правомерному и безопасному использованию информационных технологий; непосредственный объект определяется исходя из названия и диспозиции конкретной статьи. Чаще всего этот вид объекта основного состава преступления в сфере информационных технологий сформулирован альтернативно, в квалифицированных составах их количество, естественно, увеличивается.

В уголовно-правовом понимании компьютерная информация являются предметом преступления в сфере информационных технологий, на что законодатель в одних случаях прямо указывает в диспозициях ст.ст. 278^1, 278^2, 278^4, 278^6 УК, а в других случаях - установление предмета связывается с определением других обязательных элементов состава преступления - ст.ст. 278^3, 278^5 и 278^7 УК.

В соответствии со ст. 3 Закона Республики Узбекистан «О принципах и гарантиях свободы информации» под информацией понимаются сведения о лицах, предметах, фактах, событиях, явлениях и процессах независимо от формы их представления. Специфика главы Особенной части УК о преступлениях в сфере информационных технологий состоит в том, что в ней речь идет об отдельном виде информации — о компьютерной информации.

Представляется, что компьютерная информация — это информация, обработанная и используемая при помощи ЭВМ (компьютера), содержащая сведения о лицах, предметах, фактах, явлениях и процессах, а также программы для ЭВМ и базы данных, имеющая идентификационные атрибуты собственника, установившего режим (правила) ее использования. Также уголовно-правовой защите подлежат программы для ЭВМ и базы данных. Следует отметить особенность программ для ЭВМ: с одной

[3] Выступление Президента Республики Узбекистан Шавката Мирзиёева на форуме молодежи Узбекистана 26 декабря 2020 года, https://yuz.uz/ru/news/vstuplenie-prezidenta-respubliki-uzbekistan-shavkata-mirziyoeva-na-forume-molodeji-uzbekistana

стороны, они — инструмент воздействия на информацию, с другой же — они сами информация ввиду совокупности команд и данных, т.е. им присуща определенная двойственность. Эта двойственность дает основания для толкования программы для ЭВМ как одного из видов информации. Ст. 1 Закона Республики Узбекистан «О правовой охране программ для электронновычислительных машин и баз данных» дает следующее определение программы для ЭВМ:

«Программа для ЭВМ - это объективная форма представления совокупности данных и команд, предназначенных для функционирования ЭВМ и других компьютерных устройств с целью получения определенного результата. Под программой для ЭВМ подразумеваются также подготовительные материалы, полученные в ходе ее разработки, и порождаемые ею аудиовизуальные отображения».

Что же понимается под базой данных? Та же статья говорит, что «база данных — это объективная форма представления и организации совокупности данных (например: статей, расчетов), систематизированных Таким образом, чтобы эти данные могли быть найдены и обработаны с помощью ЭВМ».

Как уже было сказано, компьютерная информация может находиться на машинном носителе, в ЭВМ, системе ЭВМ или сети ЭВМ.

Машинные носители — устройства, предназначенные для постоянного хранения и переноса компьютерной информации.

Электронно-вычислительная машина (ЭВМ) состоит из системного блока, включающего в себя микропроцессор, который и являются ее «мозгом», клавиатуры (устройство, позволяющее вводить в ЭВМ печатные символы) и монитора — устройства для изображения различной информации.

К системному блоку компьютера могут подключаться различные дополнительные устройства. Эти устройства предназначены для расширения функциональных возможностей ЭВМ. К таким устройствам относятся принтер, сканер, модем и другие. Систему ЭВМ образует сам компьютер и все периферийные устройства.

Сеть ЭВМ представляет собой соединение нескольких компьютеров. Такое соединение образуется с помощью специальных кабелей.

С технической точки зрения, компьютерная информация действительно являются средством действия (и не только преступного) в рамках компьютерной системы, но мы тогда не должны отделять ее от самой ЭВМ. То есть средством в техническом и юридическом смысле информация будет только в совокупности с компьютером, а не отдельно от него. В связи с этим, вопрос можно считать исчерпанным и при квалификации преступлений, где электронно-вычислительная машина являются средством, воспринимать ЭВМ как комплекс аппаратного и программного обеспечения. С учетом этого, когда имеет место оплата покупки при помощи поддельной пластиковой карточки или незаконный и безвозмездный перевод денежной суммы с одного счета в банке на другой, содеянное подлежит квалификации как хищение в зависимости от формы последнего.

Объективная сторона составов преступлений в сфере информационных технологий в большинстве случаев сконструирована как материальная, поэтому предполагают не только совершение общественно опасного деяния, но и наступления общественно

опасных последствий, а также установления причинной связи между деянием и наступившим последствием. Отдельные составы преступлений (ст.ст. 278[3], 278[6] и 278[7] УК) сформулированы законодателем как формальные, момент окончания которых определяется моментом совершения действия или бездействия независимо от времени наступления последствий. Сами же общественно опасные деяния применительно к рассматриваемым преступлениям выступают в форме действий и лишь иногда как бездействие. В одном случае такой признак объективной стороны состава преступления, как способ его совершения, сформулирован в качестве обязательного признака основного и квалифицированного составов. В остальных он, а также место, время, орудие, средства, обстановка совершения преступления могут быть учтены судом в качестве смягчающих или отягчающих обстоятельств.

Преступления в сфере информационных технологий совершаются с использованием различных электронно-вычислительных машин, аппаратных средств, периферийных устройств и линий связи. Использование таких средств совершения данных преступлений обусловливает постановку вопроса о месте совершения преступления. Создание мировых информационных сетей, объединивших пользователей практически из всех стран мира (Интернет), дает возможность совершать деяния далеко от места наступления вредных последствий.

Субъективная сторона преступлений в сфере информационных технологий характеризуется умышленной формой вины в виде прямого или косвенного умысла. Лишь один состав преступления, предусмотренный ст. 2781 УК, устанавливающий ответственность за нарушение правил информатизации может быть совершен как умышленно, так и по неосторожности. *Цель* как обязательный признак субъективной стороны преступления указана законодателем в трёх составах преступлений, предусмотренные ст.ст. 278[3], 278[6] и 278[7] УК. В остальных случаях, *мотив и цель* не предусматриваются в качестве обязательных признаков рассматриваемых преступлений, но их установление имеет большое значение для индивидуализации наказания. Эти преступления могут совершаться из корысти, хулиганских побуждений, мести, «ради спортивного интереса», т.е. исследовательского интереса, политических мотивов и тд. Цель может быть также самой разнообразной: стремление достичь мнимого превосходства, желание получить наживу, совершение этих деяний с целью скрыть другое преступление и т.п.

Субъектом преступлений в сфере информационных технологий может быть вменяемое лицо, достигшее шестнадцатилетнего воз. раста, в обязанности которого входит соблюдение правил хранения информации, либо лицо, противоправно получившее доступ к компьютерной информации или в или телекоммуникаций

С точки зрения психофизиологических характеристик - это, как правило, творческая личность, профессионал, способный идти на технический вызов, риск. В настоящее время крупные компании стремятся привлечь наиболее опытных хакеров на работу с целью создания систем защиты информации и компьютерных систем.

Исходя из этого, круг лиц, совершающих преступления в сфере информационных технологий, являются относительно широким. Как следует из вышеуказанных данных о возрасте и личности субъекта преступления, рассматриваемая группа преступлений

совершается представителями различных слоев общества, причем возраст правонарушителей колеблется от 16 до 60 лет, а их уровень подготовки -от новичка до профессионала. Потенциальным преступником в области компьютерной техники являются лицо любого возраста, имеющее хотя бы минимальные знания в эгой области.

Таким образом, анализ объективных и субъективных признаков составов преступления позволяет констатировать, что определения место расположения общество опасных деяний в структуре Особенной части действующем УК, посягающих на отношения, обеспечивающие правомерное, безопасное использование информационных технологий и сети телекоммуникаций и установление ответственности за их совершение, является социально-обусловленными и продиктовано релями новых угроз направленных на объекты уголовно-правовой охраны.