УДК 343.3/.7
МРНТИ 10.77.51

М.С. Заркенов
Академия правоохранительных органов при Генеральной прокуратуре Республики Казахстан, г. Нур-Султан, Республика Казахстан

АКТУАЛЬНЫЕ ВОПРОСЫ СУБЪЕКТИВНОЙ СТОРОНЫ ОТДЕЛЬНЫХ ПРАВОНАРУШЕНИЙ В СФЕРЕ ИНФОРМАТИЗАЦИИ И СВЯЗИ

Аннотация. В статье рассматриваются признаки субъективной стороны неправомерного доступа к информации, в информационную систему или сеть телекоммуникаций, неправомерного уничтожения или модификации информации, неправомерного завладения информацией, имеющие большое теоретическое и практическое значение. Исследованы формы вины рассматриваемых уголовных правонарушений, в результате чего предложена административная ответственность за аналогичные виды уголовных правонарушений, совершенных в форме неосторожности. Учитывается интернет-зависимость пользователя информационных технологий, которой следует уделять больше внимания и принимать соответствующие меры.

Помимо того, в рассматриваемых уголовных правонарушениях предлагаются такие квалифицирующие признаки, как корыстный мотив, сокрытие другого преступления или облегчение его совершения, проанализирован зарубежный опыт противодействия уголовным правонарушениям в сфере информатизации и связи.

Ключевые слова: субъективная сторона; неправомерный доступ к информации; уничтожение информации; модификация информации; неправомерное завладение информацией; цифровизация; интернет-зависимость; уголовные правонарушения в сфере информатизации и связи.

М.С. Заркенов
Қазақстан Республикасы Бас прокуратурасының жанындағы Құқық қорғау органдары академиясы, Нұр-Сұлтан қ., Қазақстан Республикасы

АҚПАРАТТАНДЫРУ ЖӘНЕ БАЙЛАНЫС САЛАСЫНДАҒЫ ЖЕКЕЛЕГЕН ҚҰҚЫҚ БҰЗУШЫЛЫҚТАРДЫҢ СУБЪЕКТИВТІ ЖАҒЫНЫҢ ӨЗЕКТІ МӘСЕЛЕЛЕРІ

Аннотация. Мақалада ақпаратқа, ақпараттық жүйеге немесе телекоммуникация желісіне заңсыз қол жеткізудің, ақпаратты заңсыз жоюдың немесе түрлендірудің, үлкен теориялық және практикалық маңызы бар ақпаратты заңсыз иеленудің субъективті жағының белгілері қарастырылады. Қаралып отырған қылмыстық құқық бұзушылықтардың кінә нысандары зерттелді, соның нәтижесінде абайсызда жасалған қылмыстық құқық бұзушылықтардың ұқсас түрлері үшін әкімшілік жауапкершілік ұсынылды. Ақпараттық технологияларды пайдаланушының интернетке тәуелділігі ескеріледі, оған көп көңіл бөліп, тиісті шаралар қабылдау керек.

Бұдан басқа, қарастырып отырған қылмыстық құқық бұзушылықтарда пайдакүнемдік себеп, басқа қылмысты жасыру немесе оны жасауды жеңілдету сияқты белгілері ұсынылады, ақпараттандыру және байланыс саласындағы қылмыстық құқық бұзушылықтарға қарсы іс-қимылдың шетелдік тәжірибесі талданды.

Түйінді сөздер: субъективті тарап; ақпаратқа заңсыз қол жеткізу; ақпаратты жою; ақпаратты түрлендіру; ақпаратты заңсыз иелену; цифрландыру; интернет-тәуелділік; ақпараттандыру және байланыс саласындағы қылмыстық құқық бұзушылықтар.

M.S. Zarkenov
The Law Enforcement Academy under the Prosecutor General's Office of the Republic of Kazakhstan, Nur-Sultan c., the Republic of Kazakhstan

TOPICAL ISSUES OF THE SUBJECTIVE SIDE OF SOME OFFENSES IN THE FIELD OF INFORMATIZATION AND COMMUNICATION

Abstract. This article examines the signs of the subjective side of illegal access to information, to an information system or telecommunications network, illegal destruction or modification of information, illegal acquisition of information, which are of great theoretical and practical importance. The forms of guilt of the considered criminal offenses are deeply studied, as a result of which the administrative responsibility for similar types of criminal offenses committed in the form of negligence is proposed. The Internet dependence of the information technology user is also taken into account, which should be

given great attention and appropriate measures taken. In addition, in the criminal offenses we are considering, such qualifying features as a selfish motive, concealment of another crime or facilitation of its commission are offered. In order to study individual criminal offenses in the field of information technology, the foreign experience of countering criminal offenses in the field of informatization and communications is analyzed.

Keywords: subjective side; illegal access to information; destruction of information; modification of information; illegal acquisition of information; digitalization; internet addiction; criminal offenses in the field of information and communications.

DOI: 10.52425/25187252_2021_20_38

В статье 19 Уголовного кодекса Республики Казахстан (далее – УК РК), лицо привлекается к уголовной ответственности лишь за те общественно опасные деяния и последствия, в отношении которых установлена его вина[1]. Соответственно, вина выражает психическое отношение субъекта к совершенному уголовному правонарушению в форме умысла и неосторожности.

Так, субъективная сторона неправомерного доступа к информации, в информационную систему или сеть телекоммуникаций (ч.1, 2 ст.205 УК РК) характеризуется умышленной формой вины по отношению к деянию и последствиям. Между тем, данное уголовное правонарушение может быть совершено в виде прямого или косвенного умысла. В таком случае, виновный осознает общественную опасность своего неправомерного доступа к информации, в информационную систему или сеть телекоммуникаций, предвидит наступление общественно опасных последствий, предусмотренных статьей 205 УК РК, и желает (с прямым умыслом) или допускает их наступление, либо относится к ним безразлично (с косвенным умыслом). Ученые-юристы И.Ш. Борчашвили, С.М. Рахметов, И.И. Рогов, А.Б. Бекмагамбетов, В.П. Ревин, В.В. Ревина, А.Т. Исмагулова, А.М. Галиаскарова придерживаются такого же мнения о субъективной стороне исследуемого уголовного правонарушения.

В соответствии со статьей 19 УК РК форма неосторожности может быть специально предусмотрена только в статьях Особенной части УК РК. Однако в диспозиции основного деяния статьи 205 УК РК форма неосторожности не установлена. Таким образом, если деяние, предусмотренное частями 1,2 статьи 205 УК РК совершено по неосторожности, то такое деяние не будет являться уголовным правонарушением, то есть признается совершенным невиновно (ст.23 УК РК).

Вместе с тем, существует немало интересных высказываний ученых о неосторожной форме вины, однако эти суждения о ее сущности и особенностях остались лишь на уровне науки уголовного права.

В.В. Воробьев отмечает, что ученые испытывают трудности в разграничении уголовных правонарушений в области информационных технологий, совершенных умышленно от совершенных по неосторожности, а также неосторожных действий от невиновных, формально содержащих признаки аналогичных уголовных правонарушений [1, 112 стр.]. Например, при работе с компьютерными системами одни и те же действия могут привести к разным последствиям [2, 10 стр.], а именно: в одних случаях лицо может сознательно совершить определенные действия с ожидаемыми вредными последствиями, в других случаях лицо, совершающее действие, получает непредвиденные негативные последствия. В связи с этим, В.А. Усманов считает, что рассматриваемое уголовное правонарушение может совершаться не только умышленно, но и по неосторожности [3, 365 стр.].

Форма неосторожности имеет место в случаях, когда лица, обладающие специальными навыками и знаниями в работе с компьютерными системами, в результате чрезмерной самоуверенности могут допустить непредвиденные последствия в работе вычислительной системы, либо когда лицо, создавшее программу не предвидело, что в результате ее использования произойдет неконтролируемое проникновение в систему или иные противоправные действия (т.е. виновник не всегда способен

[1] Уголовный кодекс Республики Казахстан: от 03 июля 2014 г. № 226-V ЗРК [Электронный ресурс] – Режим доступа: http://adilet.zan.kz/rus/docs/K1400000226 (дата обращения: 18.02.2021).

полностью контролировать процесс воздействия). Например, студент Корнельского университета (США) с целью эксперимента разработал программу, которая могла самопроизвольно размножаться в сетях телекоммуникаций, обходя меры безопасности. Однако, эта программа содержала ошибку из-за которой скорость размножения была превышена, чем ожидалось. В итоге программа вышла из-под контроля и за несколько часов поразила более 6 тысяч компьютеров в университетах, исследовательских центрах и военных объектах, что привело к блокировке последних и нарушению связи между компьютерами [4, С. 7–20][2]. В то же время у виновного не было преступного умысла блокировать компьютерные технологии и нарушать связь между компьютерами. Этот случай четко указывает на то, как действия могут совершаться без контроля.

Также вредные последствия могут быть вызваны лицом из-за незнания компьютерной системы или ее мельчайших функций, то есть вследствие поступка, который он не осознавал. Наряду с этим в компьютерной системе могут возникать различные последствия из-за неисправности системы от различных факторов, не зависящих от ее пользователя. Такие обстоятельства допускают совершение рассматриваемого уголовного правонарушения по неосторожности (например, если виновный должен и мог предвидеть возможность наступления последствий).

По мнению С.А. Пашина неосторожная форма вины может проявляться при оценке лицом правомерности своего доступа к электронной информации, а также в отношении неблагоприятных последствий доступа [5, 418 стр.]. Например, чувство законности доступа может возникнуть, когда лицо, случайно получив ссылку с доступом к охраняемой законом информации через приложение WhatsApp, не осознавая характера общественно опасного вреда совершает незаконный доступ к информации или иные действия в отношении информации с вредными последствиями.

С точки зрения С.В. Озерского, Ю.Н. Лазарева, А.Ю. Лаврова уголовное правонарушение может быть совершено с умыслом, а неосторожность может проявиться в том случае, если лицо неверно оценит законность своего доступа к электронной информации, а также в отношении негативных последствий [6, 24 стр.].

Подобной позиции придерживается и А.Е. Шарков, отмечая, что лицо, совершающее незаконный доступ по неосторожности, либо осознает опасность своего поступка и действует легкомысленно, либо не предвидит возможных вредных последствий, но мог и должен был их предвидеть [7, 149 стр.].

Д.Г. Малышенко в работе предлагает ввести в рассматриваемый вид преступлений уголовного закона неосторожную форму вины [8, 94 стр.].

Кроме того, И.А. Сало приводит ряд действий, совершенных по неосторожности, а именно копирование информации в результате автоматических действий программных средств, модификация информации в результате изменения статистики на сервере новых учетных записей о логине пользователя, передаваемом клиентской программой для проверки подлинности, дате, времени и продолжительности доступа [9, 144 стр.] и другие последствия, вызванные независимо от воли пользователя. В связи с этим, по мнению И.А. Сало, «рассмотрение исследуемого деяния только в пользу умысла приведет к ошибкам в оценке поведения виновного с точки зрения наличия состава преступления в его действиях и, как следствие, безнаказанности за его совершение» [9, 146 стр.].

Несомненно, позиция вышеприведенных ученых о фактическом наличии неосторожной формы вины при совершении рассматриваемого деяния заслуживает особого внимания. Однако, несмотря на возможность действительного существования вреда от этой формы вины, мы не разделяем эту позицию по следующим причинам.

Во-первых, законодатель не предусматривает в УК неосторожной формы вины за деяние рассматриваемого уголовного правонарушения.

Во-вторых, могут возникнуть проблемы с разграничением неосторожности и неви-

[2] The Morris Worm: 30 Years Since First Major Attack on the Internet // FBI [Electronic resource] – Access mode: https://www.fbi.gov/news/stories/morris-worm-30-years-since-first-major-attack-on-internet-110218 (Access date: 01.10.2020).

новного причинения вреда, при этом расширяется охват уголовной ответственности за неосторожность и сужается область применения невиновного причинения вреда. Согласно статьи 23 УК РК, если уголовная ответственность за неосторожную форму вины не предусмотрена, то деяние и последствие, не охватываемые умыслом виновного считаются невиновным причинением вреда. В этом случае, с позиции вышеназванных ученых, преступная неосторожность не будет признана невиновной.

Вызывает интерес статья 16 УК Китайской Народной Республики, которая устанавливает, что деяния, не являющиеся результатом умышленной или неосторожной вины, а вызванные обстоятельствами непреодолимой силы или невозможностью ее предвидеть, признаются невиновными[3]. Например, это может быть связано с возникающим пробелом в системах защиты компьютера от различных программных процессов и их конфликтов с другой системой, в результате чего обычный пользователь компьютера, не подозревая об этом и не будучи в состоянии (не имея возможности) предвидеть это, может получить несанкционированный доступ к электронной информации. Таким образом, сужается область невиновного причинения вреда, что противоречит правовой политике Казахстана, направленной на гуманизацию системы уголовного правосудия.

Разумеется, криминализация неосторожных преступлений характеризуется, с точки зрения последствий, способами и средствами причинения этих последствий, а также сферой деятельности, в процессе которой они причиняются. В этой связи, рассмотрим возможность применения неосторожной формы вины по отношению к последствиям.

Как известно, совершение только рассматриваемого деяния без вытекающих из него вредных последствий не является уголовным правонарушением. Следовательно, общественная опасность уголовного правонарушения выражается в общественно опасном последствии. Такие последствия могут быть вызваны неосторожностью, то есть существует возможность причинения вредных последствий по неосторожности. Исходя из этого, целесообразно, чтобы уголовная ответственность за деяния, предусмотренные частями 1, 2 статьи 205 УК РК, состояла из двух форм вины. Таким образом, следовало бы полагать, что форма вины по неосторожности должна определяться именно применительно к общественно опасным последствиям.

Однако возникает вопрос о том, насколько соразмерной будет уголовная ответственность за неосторожную форму вины по отношению к лицу, совершившему одно нажатие клавиши компьютерной техники и причинившему значительный вред, за исключением тяжких последствий. Действительно, в результате использования компьютерных технологий люди часто совершают ошибочные действия или не воспринимают свои действия всерьез, а также совершают множество различных бессознательных действий. В таком случае криминализация неосторожной формы вины за деяния, предусмотренные частями 1, 2 статьи 205 УК РК, также противоречит принципам гуманизации уголовного законодательства и международным стандартам в области прав человека.

Кроме того, во всех уголовно-правовых мерах, предложенных в международной Конвенции о преступности в сфере компьютерной информации от 23 ноября 2001 года не предусмотрена неосторожная форма вины[4]. В соответствии с Соглашением о сотрудничестве государств-участников Содружества Независимых Государств (далее - СНГ) в борьбе с преступлениями в сфере компьютерной информации от 01 июня 2001 года противоправными деяниями являются только общественно опасные деяния, совершенные с умыслом[5]. Соответственно в Модельном уголовном кодексе государств-участников

[3] Criminal Law of the People's Republic of China (Adopted at the Second Session of the Fifth National People's Congress on July 1, 1979, Revised at the Fifth Session of the Eighth National People's Congress on March 14, 1997) [Electronic resource] – Access mode: https://www.cecc.gov/resources/legal-provisions/criminal-law-of-the-peoples-republic-of-china (Access date: 18.02.2021).

[4] Convention on Cybercrime. European Treaty Series – No. 185. Budapest, 2001 [Electronic resource] – Access mode: https://rm.coe.int/1680081561 (Access date: 18.02.2021).

[5] Соглашение о сотрудничестве государств-участников Содружества Независимых Государств в борьбе с преступлениями в сфере компьютерной информации. Минск, 2001 [Электронный ресурс] – Режим доступа: http://www.cis.minsk.by/page.php?id=866 (дата обращения: 18.02.2021).

СНГ за рассматриваемое уголовное правонарушение форма вины установлена как умышленная, за исключением ее квалифицированного состава[6]. Следовательно, в международных актах форма вины за неправомерный доступ к электронной информации указывается только в виде умысла, что также свидетельствует о правильности нашей точки зрения.

Между тем процесс цифровизации в нашей стране все еще находится на начальной стадии, а население страны еще не достигло достаточного уровня компьютерной грамотности и кибергигиены, и не осознало всю опасность угрозы в сфере информационных технологий. Рано требовать от граждан страны соблюдения дополнительных репрессивных и ужесточающих уголовно-правовых мер, пока в стране не создано систематизированное информационное право, полноценная, доступная, защищенная среда в информационном пространстве, а также устойчивая информационная культура. Таким образом, криминализация неосторожной формы вины за деяния, предусмотренные частями 1, 2 статьи 205 УК РК, должна быть заменена менее социально опасной мерой, такой как административное наказание.

С.Д. Бражник совершенно справедливо отмечает, что большая часть уголовных правонарушений в области электронной информации должны быть установлены как умышленные. Деяния, наносящие ущерб по неосторожности в большинстве случаев не имеют степени общественной опасности присущей уголовным правонарушениям [10, 124 стр.]. Так, ученый допускает низкую общественную опасность от деяния, причинившего вред в неосторожной форме вины.

Следует отметить, что в аналогичном уголовном правонарушении, предусмотренном частью 1 статьи 349 УК Республики Беларусь, форма вины характеризуется неосторожностью. Санкция этой статьи предусматривает штраф и арест[7], которые больше всего схожи с административными взысканиями. Общественная опасность такого деяния (ч.1 ст.349 УК РБ) ниже по сравнению с его умышленной формой (ч.2 ст.349 УК РБ). Такой подход в уголовном законодательстве также подтверждает низкую степень общественной опасности исследуемого деяния по неосторожности.

Учитывая вышеизложенное, за совершение исследуемых противоправных деяний, предусмотренных частями 1, 2 статьи 205 УК РК и последствия по неосторожности целесообразно предусмотреть административную ответственность. В этой связи, главу 10 «Административные правонарушения, посягающие на права личности» Кодекса Республики Казахстан «Об административных правонарушениях» следует дополнить следующей новой нормой «неправомерный доступ к охраняемой законом информации, содержащейся на электронном носителе, в информационную систему или сеть телекоммуникаций, повлекший по неосторожности значительное нарушение прав и законных интересов граждан, организаций либо охраняемых законом интересов общества или государства, если это действие не содержит признаков уголовно наказуемого деяния». Таким образом, считаем, что предлагаемая мера будет эффективна в противодействии неосторожным деяниям, связанным с неправомерным доступом к информации, в информационную систему или сеть телекоммуникаций.

Кроме того, в качестве дополнительной меры за причиненный ущерб могут выступать установленные нормы Гражданского кодекса РК (гражданско-правовая ответственность), которые влекут за собой обязательства по восстановлению первоначального положения и возмещению ущерба. Например: уплата неустойки, компенсационные меры, меры оперативного воздействия, приостановление или прекращение работы вычислительной техники и других объектов информатизации, приводящие к негативным воздействиям и др.

---

[6] Модельный уголовный кодекс для государств-участников Содружества Независимых Государств. Рекомендательный законодательный акт от 17 февр. 1996 г. [Электронный ресурс] – Режим доступа: https://www.icrc.org/ru/doc/assets/files/other/crim.pdf (дата обращения: 30.12.2020).

[7] Постатейный комментарий к Уголовному кодексу Республики Беларусь: Судебная практика [Электронный ресурс] – Режим доступа: https://bypravo.ru/postatejnyj-kommentarij-k-ugolovnomu-kodeksu-respubliki-belarus-osobennaya-chast-razdel-xii-prestupleniya-protiv-informatsionnoj-bezopasnosti-glava-31-prestupleniya-protiv-informatsionnoj-bezopas/ (дата обращения: 01.08.2020).

Часть 3 статьи 205 УК РК специально предусматривает форму неосторожности применительно к тяжким последствиям. В данном случае уголовная ответственность возникает только в том случае, если лицо предвидело возможность наступления последствий, но без достаточных оснований самонадеянно полагалось на их предотвращение (по самонадеянности), либо не предвидело, но должно и могло предвидеть возможность наступления последствий (по небрежности), предусмотренных статьей 205 УК РК. Тем не менее, это положение охватывает две формы вины: умысел и неосторожность. Согласно статьи 22 УК РК такое общественно опасное деяние признается совершенным умышленно.

Следующими исследуемыми уголовными правонарушениями являются деяния, предусмотренные статьями 206, 208 УК РК. Как показывает анализ, субъективная сторона неправомерного уничтожения, модификации, ввода в информационную систему заведомо ложной информации, а также неправомерного копирования или иного завладения информацией характеризуется умышленной формой вины. Эти уголовные правонарушения также могут быть совершены как с прямым, так и с косвенным умыслом. Так, форма вины в этих противоправных деяниях аналогична субъективной стороне деяний, предусмотренных частями 1 и 2 статьи 205 УК РК.

О внесении в информационную систему заведомо ложных сведений, доктор юридических наук И.Ш. Борчашвили совершенно верно отмечает, что заведомость подразумевает знание лица о ложности вводимой информации [11, 385 стр.]. При этом незнание и заблуждение лица в истинности введенных сведений исключает ответственность за исследуемое деяние. Такое понимание признака заведомости определяет интеллектуальный момент вины.

Кроме того, неосторожная форма вины, часто обсуждаемая среди ученых, рассматривается по аналогии с предыдущими деяниями, предусмотренными частями 1 и 2 статьи 205 УК РК. За совершение неправомерного уничтожения, модификации, ввода в информационную систему заведомо ложной информации, а также неправомерного копирования или иного завладения информацией по неосторожности предлагается административная ответственность. В этой связи, Кодекс Республики Казахстан «Об административных правонарушениях» следует дополнить административной ответственностью за неправомерное воздействие на информацию и ее завладение, а именно: «неправомерное уничтожение, модификация, копирование или иное завладение охраняемой законом информацией, хранящейся на электронном носителе, содержащейся в информационной системе или передаваемой по сетям телекоммуникаций, а равно внесение в информационную систему заведомо ложной информации, повлекшее по неосторожности значительное нарушение прав и законных интересов граждан, организаций или охраняемых законом интересов общества или государства, если это действие не содержит признаков уголовно наказуемого деяния».

На наш взгляд, предложенная норма будет эффективна при противодействии неосторожным деяниям по совершению неправомерного уничтожения, модификации или завладения информацией.

Кроме того, В.В. Воробьев в своей научной работе учитывает такое отклонение в психике человека, как маниакальную компьютерную или интернет-зависимость, что не позволяет с полной уверенностью утверждать о наличии вины в уголовном поступке данного лица [1, С. 117–118]. Виртуальная реальность новых технологий усиливает агрессию, стирает черту между разрешенным и незаконным. Этот вид зависимости появляется при чрезмерном использовании компьютерных технологий или интернета. При этом двигательные навыки человека нарушаются уже с 2-3 минут пребывания в виртуальной реальности, а нарушения двигательных рефлексов появляются через 25-30 минут[8].

По мнению А. Альтера, если раньше люди становились зависимыми от сигарет, алкоголя и наркотиков, то сейчас в цифровую эпоху появилось намного больше так называемых крючков: Instagram, Facebook, интернет-магазины, компьютерные игры и т.д. Доступность этих программных продуктов приводит к быстрому развитию зависимости.

[8] Интерактивная виртуальность // Современное образование. - 2000. - № 7. – С. 15-23.

А. Альтер также считает, что в последнее время аддиктивное поведение становится все более разнообразным и сопротивляться ему становится все сложнее [12, 55 стр.].

Возросшее признание его негативных психосоциальных (прерывистое взрывное расстройство, клептомания, патологическая азартная игра и пиромания) и медицинских последствий привело к включению интернет-зависимости в качестве нового заболевания в редакцию DSM (Американской психиатрической ассоциации) [13, 757 стр.]. Интернет-наркомания проявляется как в физических, так и в эмоциональных симптомах, однако эти особенности могут отличаться у каждого человека. Когда зависимость выходит из-под контроля больные люди могут навредить себе или совершить другие преступные действия. Так, компьютерная или интернет-зависимость фактически проявляется в различных формах, таких как нежелание отрываться от компьютерной техники (компьютерной игры), игнорирование домашних дел, отказ от общения с друзьями и т.д.

В нашем случае негативная сторона обсуждаемой зависимости может быть реализована в виде неосознанного совершения уголовно наказуемых деяний, предусмотренных статьями 205, 206, 208 УК РК, например, для того, чтобы получить компьютерную игру или другие программы. В связи с этим, данный вид психического расстройства требует дальнейшего исследования и должен учитываться при проведении экспертного обследования психического заболевания судебно-психиатрическими экспертами.

Учитывая, что подростки находятся в процессе психологического созревания, было отмечено, что они особенно уязвимы к развитию аддиктивного поведения. В связи с этим растет популярность и распространенность интернет-зависимости среди детей и молодежи. Фактически каждый четвертый ребенок зависим от интернета, и это тревожная статистика [14, 272 стр.]. Таким образом, целесообразно принять меры по исключению интернет-зависимости среди детей и молодежи, а также совершения ими противоправных действий в сфере информационных технологий или по защите их от подобных противоправных действий.

Вместе с тем, факультативные признаки субъективной стороны, как мотив и цель не имеют значения для квалификации рассматриваемых уголовных правонарушений и могут повлечь только отягчающее или смягчающее обстоятельство в пределах наказания, предусмотренных статьями 205, 206, 208 УК РК. Практически невозможно описать типичный стереотип злоумышленника в области информационных технологий и его мотивы, главным образом потому, что они действуют на основе одного или нескольких мотивов. Некоторые мотивы включают любопытство, развлечения, удовлетворение, рекламу (публичность), манипуляцию, разрушение, месть, удовлетворение эго, хактивизм, национализм, радикализм, религию, политику и финансовую выгоду [15, 167 стр.]. Мотивами и целями совершения деяний, предусмотренных статьями 205, 206, 208 УК РК, выступают в основном любопытство, хулиганское побуждение, корысть, исследование, самоутверждение, сокрытие другого преступления, чувство мести. Так, некоторые ученые считают, что определенные мотивы и цели повышают степень общественной опасности уголовного правонарушения.

В.Г. Степанов-Егиянц совершенно справедливо предлагает дополнить уголовную ответственность за неправомерный доступ к информации квалифицирующим признаком, включающим в себя цель сокрытия другого преступления или содействия его совершению [16, 74 стр.]. Причина этого предложения заключается в его высокой общественной опасности.

К.Н. Евдокимов придерживается позиции, что отсутствие в уголовном законе непосредственного указания на обязанность анализировать мотивы и цели совершения уголовных правонарушений в сфере информационных технологий расценивается как пробел в законодательстве. В результате он предлагает ужесточить уголовную ответственность за неправомерный доступ к информации, дополнив в качестве квалифицирующего признака корыстные и хулиганские мотивы, а также сокрытие другого преступления [17, С. 113–114].

Разделяем позицию вышеуказанных ученых, поскольку действительно основное количество неправомерного доступа к информации или ее завладения, а также иных воздействий на нее совершается с целью получения выгоды и сокрытия другого преступления. Между тем, они представляют высокую общественную опасность. Исследования показывают, что 76% всех компьютерных атак имеют финансовую мотивацию [18, 5 стр.].

Это подтверждается и проведенным исследованием, где большинство проинтервьюированных (45,8%) считают, что уголовные правонарушения в сфере информатизации и связи чаще всего совершаются из корыстных побуждений. Остальные респонденты указали на хулиганство (34,6%), любопытство (5,4%), самоутверждение (5%), карьеризм (4,6%), эмоциональное напряжение (1,4%), ревность (1,2%), политическую неприязнь (0,8%), удовлетворение эго (0,6%), месть (0,4%), безработицу (0,2%). Например, завладение информацией зачастую сопряжено с финансовыми последствиями, а именно с помощью этих данных можно украсть деньги, шантажировать или продать их в «Даркнете».

Также результаты опроса показали, что уголовные правонарушения в рассматриваемой сфере чаще всего совершаются со следующими преступными целями: с целью сокрытия другого преступления или облегчения совершения преступления (40,4%); с целью хищения имущества или получения имущества в крупном размере (37,4%); с целью сбыта, распространения информации (8,6%); с целью передачи иностранному государству, международной или иностранной организации либо их представителям сведений, составляющих государственные секреты (8%); с целью последующего изобличения и привлечения к уголовной ответственности или шантажа (2,8%); с целью получения информации из критически важных объектов информационно-коммуникационной инфраструктуры (1,6%); с целью провокации войны или осложнения международных отношений (0,6%); с целью подрыва конституционного строя, безопасности и обороноспособности РК, нарушения унитарности и целостности РК (0,6%). Таким образом, данные результаты исследования свидетельствуют о высокой общественной опасности деяния в рассматриваемой сфере, совершенного с целью сокрытия другого преступления или облегчения совершения преступления.

В то же время, учитывая, что в нашей стране происходит дигитализация всей государственной деятельности, в том числе и переход уголовного производства в электронный формат, существует риск уничтожения электронных материалов уголовного дела или данных о судимости лица. В этой связи, предлагаем дополнить квалифицирующим составом деяния, предусмотренные статьями 205, 206, 208 УК РК, а именно: «2. Те же деяния, совершенные:

...) из корыстных побуждений или по найму;

...) с целью скрыть другое преступление или облегчить его совершение».

Подводя итог, следует отметить, что анализ субъективной стороны рассматриваемых уголовных правонарушений показывает целесообразность дальнейшего совершенствования не только уголовного законодательства, но и других нормативных правовых актов. Все рассмотренные в статье предложения направлены на противодействие отдельным уголовным правонарушениям в сфере информатизации и связи, а также на обеспечение охраны национальной безопасности.

Список использованной литературы:

1. Воробьев, В.В. Преступления в сфере компьютерной информации: дис. ... канд. юрид. наук / В.В. Воробьев. - Нижний Новгород, 2000. – 201 с.

2. Ляпунов, Ю.И. Ответственность за компьютерные преступления / Ю.И. Ляпунов // Законность. - 1997. - №1. - С.8-15.

3. Усманов, У.А. Комментарий к Уголовному кодексу Российской Федерации / У.А. Усманов. - М.: ПРИОР, 1999. – 496 с.

4. Моисеенков, И. Суета вокруг Роберта или Моррис-сын и все. все. все... / И. Моисеенков. - КомпьютерПресс, 1991. – 51 с.

5. Комментарий к Уголовному кодексу Российской Федерации: особенная часть; под общ. ред. Ю.И. Скуратова и В.М. Лебедева. - М.: Инфра-М: Норма, 1996. – 487 с.
6. Озерский, С.В. Компьютерные преступления: методы противодействия и защиты информации / С.В. Озерский, Ю.Н. Лазарев, А.Ю. Лавров. - Саратов: Саратовский юридический институт МВД России, 2004. – 114 с.
7. Шарков, А.Е. Неправомерный доступ к компьютерной информации: преступность деяния и проблемы квалификации: дис. … канд. юрид. наук / А.Е. Шарков. – Ставрополь, 2004. – 174 с.
8. Малышенко, Д.Г. Уголовная ответственность за неправомерный доступ к компьютерной информации: дис. ... канд. юрид. наук / Д.Г. Малышенко. - М., 2002. – 166 с.
9. Сало, И.А. Преступные действия с компьютерной информацией ограниченного доступа: дис. … канд. юрид. наук / И.А. Сало. – М., 2011. – 285 с.
10. Бражник, С.Д. Преступления в сфере компьютерной информации: проблемы законодательной техники: дис. … канд. юрид. наук / С.Д.Бражник. – Ижевск, 2002. – 189 с.
11. Борчашвили, И.Ш. Комментарий к Уголовному кодексу Республики Казахстан: особенная часть (том 2) / И.Ш. Борчашвили. - Алматы: Жеті Жарғы, 2015. – 1120 с.
12. Alter, A. Irresistible: The rise of addictive technology and the business of keeping us hooked / A. Alter. – New York, Penguin Books, 2017. – 368 p.
13. Müller, K.W. et al. Prevalence of internet addiction in the general population: results from a German population-based survey / K.W. Müller // Behaviour & Information Technology. – 2014. – T.33. – №.7. – P. 757-766.
14. Czincz, J. Internet addiction: Debating the diagnosis / J. Czincz, R. Hechanova // Journal of Technology in Human Services. – 2009. – T.27. – №4. – P. 257-272.
15. Sabillon, R. Cybercrime and cybercriminals: a comprehensive study / R. Sabillon, J. Cano, V. Cavaller, J. Serra // International Journal of Computer Networks and Communications Security. – 2016. - №4 (6). - P. 165-176.
16. Степанов-Егиянц, В.Г. Субъективная сторона компьютерных преступлений / В.Г. Степанов-Егиянц // Бизнес в законе. – 2013. – № 2. – С.72-74.
17. Евдокимов, К.Н. Уголовно-правовые и криминологические аспекты противодействия неправомерному доступу к компьютерной информации: дис. … канд. юрид. наук / К.Н. Евдокимов. – Иркутск, 2006. – 203 с.
18. Widup, S. 2018 Verizon Data Breach Investigations Report / S. Widup, M. Spitler, D. Hylender, G. Bassett // Verizon, 2018. - P. 68.

References:

1. Vorob'ev, V.V. Prestuplenija v sfere komp'juternoj informacii: dis. ... kand. jurid. nauk / V.V. Vorob'ev. - Nizhnij Novgorod, 2000. – 201 s.
2. Ljapunov, Ju.I. Otvetstvennost' za komp'juternye prestuplenija / Ju.I. Ljapunov // Zakonnost'. - 1997. - №1. - S.8-15.
3. Usmanov, U.A. Kommentarij k Ugolovnomu kodeksu Rossijskoj Federacii / U.A. Usmanov. - M.: PRIOR, 1999. – 496 s.
4. Moiseenkov, I. Sueta vokrug Roberta ili Morris-syn i vse. vse. vse... / I. Moiseenkov. - Komp'juterPress, 1991. – 51 s.
5. Kommentarij k Ugolovnomu kodeksu Rossijskoj Federacii: osobennaja chast'; pod obshh. red. Ju.I. Skuratova i V.M. Lebedeva. - M.: Infra-M: Norma, 1996. – 487 s.
6. Ozerskij, S.V. Komp'juternye prestuplenija: metody protivodejstvija i zashhity informacii / S.V. Ozerskij, Ju.N. Lazarev, A.Ju. Lavrov. - Saratov: Saratovskij juridicheskij institut MVD Rossii, 2004. – 114 s.
7. Sharkov, A.E. Nepravomernyj dostup k komp'juternoj informacii: prestupnost' dejanija i problemy kvalifikacii: dis. … kand. jurid. nauk / A.E. Sharkov. – Stavropol', 2004. – 174 s.
8. Malyshenko, D.G. Ugolovnaja otvetstvennost' za nepravomernyj dostup k komp'juternoj informacii: dis. ... kand. jurid. nauk / D.G. Malyshenko. - M., 2002. – 166 s.
9. Salo, I.A. Prestupnye dejstvija s komp'juternoj informaciej ogranichennogo dostupa: dis. … kand. jurid. nauk / I.A. Salo. – M., 2011. – 285 s.
10. Brazhnik, S.D. Prestuplenija v sfere komp'juternoj informacii: problemy zakonodatel'noj tehniki: dis. … kand. jurid. nauk / S.D.Brazhnik. – Izhevsk, 2002. – 189 s.
11. Borchashvili, I.Sh. Kommentarij k Ugolovnomu kodeksu Respubliki Kazahstan: osobennaja chast' (tom 2) / I.Sh. Borchashvili. - Almaty: Zheti Zharғy, 2015. – 1120 s.
12. Alter, A. Irresistible: The rise of addictive technology and the business of keeping us hooked / A. Alter. – New York, Penguin Books, 2017. – 368 p.

13. Müller, K.W. et al. Prevalence of internet addiction in the general population: results from a German population-based survey / K.W. Müller // Behaviour & Information Technology. – 2014. – T.33. – №.7. – P. 757-766.

14. Czincz, J. Internet addiction: Debating the diagnosis / J. Czincz, R. Hechanova // Journal of Technology in Human Services. – 2009. – T.27. – №4. – P. 257-272.

15. Sabillon, R. Cybercrime and cybercriminals: a comprehensive study / R. Sabillon, J. Cano, V. Cavaller, J. Serra // International Journal of Computer Networks and Communications Security. – 2016. - №4 (6). - P. 165-176.

16. Stepanov-Egijanc, V.G. Sub#ektivnaja storona komp'juternyh prestuplenij / V.G. Stepanov-Egijanc // Biznes v zakone. – 2013. – № 2. – S. 72-74.

17. Evdokimov, K.N. Ugolovno-pravovye i kriminologicheskie aspekty protivodejstvija nepravomernomu dostupu k komp'juternoj informacii: dis. … kand. jurid. nauk / K.N. Evdokimov. – Irkutsk, 2006. – 203 s.

18. Widup, S. 2018 Verizon Data Breach Investigations Report / S. Widup, M. Spitler, D. Hylender, G. Bassett // Verizon, 2018. - P. 68.