салтын, жалпы адамзаттық құндылықтар мен т. б. басымдықтарды қалыптастыру);

- ұйымдастырушылық (терроризмге қарсы бағыттағы қоғамдық және діни бірлестіктердің қызметіне жәрдемдесу; БАҚ-пен өзара іс-қимыл жасау, конференциялар, слайдтар, "дөңгелек үстелдер", терроризмге қарсы сипаттағы үздік материалдарға конкурстар және т. б. өткізу.);

- білім беру бағыты (терроризмге қарсы ақпараттық іс-қимыл саласында мамандарды даярлау жүйесін құру, оның ішінде азаматтық тұлғалар қатарынан).

- Жастар арасында экстремизм мен терроризмнің алдын алу, сондай-ақ қылмыстық сот ісін жүргізу саласында қалған аталған санаттағы адамдарды әлеуметтік оңалту жөніндегі шаралар кешенін іске асыру жөніндегі іс-шараларды көздейтін кәмелетке толмағандар мен жастар арасында тәрбие жұмысын жүргізу жөніндегі мемлекеттік бағдарлама қабылдау қажет;

- Экстремистік және террористік іс-әрекеттің алдын алу діни және өзге де қоғамдық бірлестіктердің, басқа да ұйымдардың, сондай-ақ жеке тұлғалардың экстремистік және террористік іс-әрекеттерін анықтау, олардың алдын алу және жолын кесу бойынша жүзеге асырылуға тиіс;

Қазақстанда қалыпты діни ахуалды қалыптастыру үшін экстремизм мен терроризмге қарсы күрес кешенді түрде қолға алынуы тиіс. Әлбетте, оның діни, әлеуметтік, психологиялық, экономикалық аспектілерімен қатар құқықтық негіздемесін жетілдіру бүгінгі күннің кезек күттірмейтін талабына айналып отыр. Елбасы Н. Назарбаевтың «Мәңгілік ел» идеясын іске асырып, қуатты мемлекетке айналу мақсатында ел қауіпсіздігіне қатер төндіретін әрбір шетін мәселенің дер шағында алдын алғанымыз абзал. Себебі, «Терроризм шекараны таңдамайды,елді бай және кедей деп бөлмейді».

Пайдаланылған әдебиеттер тізімі:

1. «Қазақстан-2050» Стратегиясы қалыптасқан мемлекеттің жаңа саяси бағыты // http://www.akorda.kz/kz/addresses/addresses_of_president/kazakstan-respublikasynyn-prezidenti-nenazarbaevtyn-kazakstan-halkyna-zholdauy-2012-zhylgy-14-zheltoksan.

2. Қазақстан Республикасының Конституциясы // 1995 жылы 30 тамызда республикалық референдумда қабылданды // http://adilet.zan.kz/kaz/docs/K950001000.

3. Қазақстан Республикасының Терроризмге қарсы іс-қимыл туралы Заңы // 1999 жылғы 13 шілдедегі N 416-I // http://adilet.zan.kz/kaz/docs/Z990000416.

4. Қазақстан Республикасының Қылмыстық кодексі // 2014 жылғы 3 шілдедегі № 226-V ҚРЗ // http://adilet.zan.kz/kaz/docs/K1400000226.

5. Сатпаев Д.А // Терроризм как явление политической жизни. Саясат // 1999. № 3. С. 10.

6. Ильинский И.М // О терроре и терроризме // Между будущим и прошлым. - М., - С. 239, 242.

Аманбекова Ә.Е., Карагандинский государственный университет имени академика Е.А.Букетова, юридический факультет, гр. МП-21, студент
(Научный руководитель — старший преподаватель Старожилова Н.П.)

ПРАВО НА ИНФОРМАЦИЮ В КОНТЕКСТЕ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ

В современном обществе одним из важных гражданских прав человека является право на информацию. Оно нашло закрепление в статье 19 Всеобщей декларации прав человека, а так же в статье 19 Международного Пакта о гражданских и политических правах человека.[1] В Конституции Республики Казахстан право на информацию закреплено и выражено в двух статьях: в статье 20 и в пункте 3 статьи 18. Анализ указанных статей в названных документах позволяет выделить в содержании данного права следующие элементы: 1) свободно искать, получать и распространять информацию; 2) использовать любые формы и способы выражения по своему выбору; 3) это право не зависит от государственных границ; 3) если какая-либо информация затрагивает права и интересы гражданина, то государственные органы, должностные лица и СМИ обязаны предоставить ему возможность ознакомиться с документами, решениями и указать источники такой информации (при условии, что речь идет о законных правах и интересах человека); 4) допускается возможность законного ограничения этого права в целях недопущения нарушения прав, интересов и репутации других лиц, обеспечения государственной безопасности, охраны общественного порядка, здоровья и нравственности народа. Например, в решении Европейского суда по правам человека по этому

поводу сказано, что «плюрализм и демократия основаны на компромиссе и требуют от людей и социальных групп различных уступок, чтобы гарантировать права всему обществу в целом»[2].

В эпоху глобализации обеспечение информационной безопасности приобретает все более важное значение для системы обеспечения национальной безопасности. Это объясняется существенным прогрессом в развитии информационно-коммуникационных технологий и средств, а также огромным масштабом информационного пространства. Информационная безопасность осознается как социально значимая проблема по мере развития общества, смены технологической основы связи, передачи и использования информации. Информация сегодня является важнейшим ресурсом, имеющим такую же большую ценность, как природные финансовые, трудовые и иные ресурсы. Информация стала товаром, который продается и покупается. Информация превратилась в оружие, возникают и прекращаются информационные войны.

Международная информационная безопасность является одним из элементов системы международной безопасности. Однако, в современном информационном законодательстве Казахстана определения термина «информация» нет. Недостатки в терминологии отражаются на качестве законодательной техники. Отсутствует определение понятия «информация» и в Законе РК «О средствах массовой информации»[3]. Используется термин «данные» применительно к персональным данным как к виду электронных информационных ресурсов (статья 36). Анализ действующего законодательства Республики Казахстан позволяет выделить следующие виды. Массовая информация (Закон РК «О средствах массовой информации»); информация о гражданах (персональные данные) (ст. 1 Закона РК «О персональных данных и их защите») [4], «информация об управлении правами (ст. 1 Закона РК «Об авторском праве и смежных правах»); электронные информационные ресурсы ограниченного доступа (конфиденциальная информация) (ст. 32 Закона РК «Об информатизации»)[5]; государственная тайна (ст. 1 Закона РК «О государственных секретах»); реклама (ст. 1 Закона РК «О рекламе»). На основании проведенного анализа предлагается следующее определение термина: «информация» - это объективно существующий вид материи, представляющий собой субъективно осознанные сведения, т.е. знания, данные, выраженные в сигналах, сообщениях, известиях, уведомлениях об окружающем объективном мире, которые являются объектом хранения, преобразования, передачи и использования и защиты.

Сравнительный анализ законодательства об информатизации и о национальной безопасности показал, что действующие законы не содержат положений о соотношении угроз информационной безопасности и их источников. В Законе «Об информатизации» отсутствуют нормы, перечисляющие виды угроз и источников информационной безопасности. Из содержания рассмотренных правовых актов не ясно в чем различие между угрозами и источниками угроз. Считаем, что при подготовке проекта Кодекса об информатизации в части определения угроз и их источников для информационной безопасности можно имплементировать положения Соглашения ШОС.

Копылов В.А. выделяет три основных направления правового обеспечения информационной безопасности:

1. защита чести, достоинства, деловой репутации от угроз воздействия вредной, опасной, недоброкачественной, недостоверной информации, нарушение порядка распространения информации;

2. защита информации и информационных ресурсов ограниченного доступа от угроз несанкционированного и неправомерного воздействия посторонних лиц;

3. защита информационных прав и свобод личности на передачу и использование информации в условиях информатизации.[6]

Конвенция «Об обеспечении международной информационной безопасности» содержит достаточно обширный перечень способов нарушений информационной безопасности.[7, с.240]

В Великобритании, например, проблемам правового обеспечения безопасности персональных данных стали уделять внимание еще в восьмидесятых годах прошлого века. В этой стране правовое регулирование неприкосновенности частной жизни и персональных данных осуществляется на национальном и универсальном уровнях. Великобритания ратифицировала Конвенцию «О защите частных лиц в отношении автоматизированной обработки персональных данных» 1981 года. К основным правовым актам национального характера относятся Закон о защите данных 1998 года [8], Закон о свободе информации 2000 года. Под «данными» в Законе о защите данных понимается информация, которая

обрабатывается и записывается с помощью автоматизированного оборудования и является частью системы или записью, находящегося в распоряжении государственного органа. Стоит отметить один недостаток этой формулировки. Данные могут находиться не только в распоряжении и пользовании государственного органа [9, с.72]. Очень часто такими данными обладают частные лица и организации, которые предоставляют какие-либо услуги, например, коммунальные, услуги связи. Этот же закон, например, делает различия между понятиями «конфиденциальные персональные данные» и «персональные данные». К конфиденциальным персональным данным относится информация о расовом иди этническом происхождении субъекта данные о политических взглядах, о религиозных убеждениях, о членстве в профсоюзах, о физическом или психическом здоровье человека, о совершенных правонарушениях. Основным субъектом обеспечения конфиденциальности персональных данных является контролер данных – лицо, которое определяет цели и средства обработки персональных данных. Персональные данные могут обрабатываться и использоваться только в законных целях, которые определил контролер.

Конституционной основой правового обеспечения информационной безопасности является пункт 3 статьи 20 Конституции РК. Одним из важнейших нормативных правовых актов, направленных на реализацию информационной безопасности, является Закон РК «О средствах массовой информации». Перечень оснований, по которым можно приостановить деятельность СМИ, закреплен в пункте 3 статьи 13 Закона. Статья 15 особо посвящена защите интересов несовершеннолетних при размещении рекламы от злоупотребления их доверием и отсутствием у них опыта.

Информация о личной, индивидуальной или семейной жизни человека также обладает особой ценностью. В соответствии со статьей 18 Конституции Республики Казахстан закреплено, что каждый имеет право на неприкосновенность частной жизни, личную и семейную тайну, защиту своей чести и достоинства. Однако, в условиях Интернета часто совершаются правонарушения, связанные с использованием персональных данных, не соответствующим целям операторами данных. Например, поисковые системы собирают информацию обо всех действиях своих пользователей, осуществляемых в Интернете, без их согласия, и в дальнейшем эту информацию используют для рассылки рекламы или предоставления дополнительных услуг. Свои действия поисковые системы объясняют тем, что информация о совершаемых действиях пользователей не относится к персональным данным. Такие действия операторами поисковых систем совершаются практически во всех странах. Поэтому актуальным становится вопрос о понятии персональных данных. Так, Закон Великобритании о защите данных 1998 года определяет их как «любые данные, которые относятся к живому человеку и на основании которых этот человек может быть идентифицирован, или информацию, которая находится в распоряжении контролера данных или может поступать к нему для обработки, в том числе любые выражения мнения об индивидуальных особенностях человека или его личности (ч.1 статьи 1).

Статья 1 Закона РК «О персональных данных» определяет их как сведения, относящиеся к определенному или определяемому на их основании субъекту персональных данных, зафиксированные на электронном, бумажном и (или) ином материальном носителе. Полагаем, что данная формулировка требует уточнения и дополнения применительно к целевому использованию персональных данных, а именно: сведения, на основании которых физическое лицо может быть идентифицировано, в том числе любые выражения мнения об индивидуальных особенностях субъекта». С января 2016 г. вступили в силу изменения в Закон «О персональных данных», предусматривающий, что запись, накопление и хранение персональных данных казахстанцев разрешаются только на территории Республики Казахстан. Принятие указанных актов свидетельствует об особом внимании к качеству программного обеспечения парка ИКТ Казахстана с учетом того, что Интернет-среда все более насыщается информацией, опасной для человека и используемой в целях массового поражения. Жатканбаева А.Е. отмечает, что «проблема обеспечения конфиденциальности сведений о личности является очень актуальной и болезненной. Так, например, в МВД РК создана единая компьютерная база со всей необходимой информацией о всех гражданах Республики Казахстан, ставится задача всеобщей дактилоскопии… Минздрав готов создать свою базу данных о здоровье всех и каждого в Казахстане…, но «наибольших успехов» добилось министерство финансов, присвоив каждому гражданину ИНН, зная который можно получить практически любую информацию о человеке». [10, с.144]

Информационные угрозы планируются и реализуются в таких социальных сетях, как Facebook, Twitter, «В контакте» и «Одноклассники». Достаточно просмотра новостей в Интернете. США увеличивают расходы на информационную пропаганду. Как заявил заместитель помощника Госсекретаря США по делам Европы и Евразии Зифф на слушаниях в Сенатском комитете по иностранным делам Конгресса США, расход на эти цели предусматривает рост на 86 млн долларов. Мовкебаева Г.А., например, считает, что военные операции в кибепространстве, доктринальные разработки ведения информационной войны в США начались после ведения войны в Персидском заливе.[11, с.238] Для этого в США создано Командование совместных информационных операций. Информационная операция – это комплекс мероприятий по манипулированию информацией в целях достижения и удержания всеобъемлющего превосходства над противником посредством воздействия на информационные процессы, происходящие в системах управления.

В связи с нарастающим глобальным процессом активного формирования и широкомасштабного использования информационных ресурсов особое значение приобретает информационная безопасность детей. Причиной этому стали с участившиеся случаи интернет-мошенничества, вовлечения подростков в совершение преступлений и склонения их к суицидам. Это явление уже получило свое название, которое пришло из английского языка – кибербуллинг. Так называется одна из форм психологического воздействия, травли, запугивания, насилия подростков и младших детей при помощи информационно-коммуникационных технологий, а именно Интернета и мобильных телефонов. Этот вид терроризма в виртуальном пространстве имеет разные формы проявления. Первая стадия воздействия – шутки, насмешки. На более тяжелых стадиях – сильное психологическое влияние, приводящее к суицидам и смертям. Сегодня по всей территории СНГ активно распространяются интернет-игры «Синий кит» и «Тихий дом», в которые втягивают подростков. По данным СМИ, с ноября 2015-го по апрель 2016-го года покончили с собой более 120 подростков, которые почти все были участниками одних и тех же групп смерти в социальных сетях. [12, с.41; 13, с.159] Обеспечение государством информационной безопасности детей, защита физического, умственного и нравственного развития несовершеннолетних – требование международного права. Международные стандарты в области информационной безопасности детей пока не нашли отражение в казахстанском законодательстве.

Кроме этого, появился новый вид бизнеса – так называемые информационные брокеры, лица, которые ведут сбор и обобщение информации о пользователях, которую они оставляют в общем свободном доступе. Эта информация продается компаниями, которые ее используют по своему усмотрению. Все мы сталкиваемся с такой практикой в условиях Интернета, когда сайтами совершаются действия, связанные с обработкой наших персональных данных, не соответствующих целям, заявленным оператором персональных данных, законодательству. Например, поисковые системы собирают информацию обо всех действиях своих пользователей в Интернете без их согласия (какие сайты посещаются чаще всего, чем интересуется пользователь). В дальнейшем эта информация используется для рассылки рекламы или предоставления дополнительных платных услуг.

Террористические преступления также совершаются с использованием информационных технологий. Сегодня все новые угрозы несут в себе возможности использования киберпространства террористическими организациями и различными экстремистскими группировками, осуществляющими через Всемирную сеть вербовку новых членов, в том числе в молодежной среде. В Нормативном постановлении Верховного Суда Республики Казахстан от 8 декабря 2017 года №11 «О некоторых вопросах судебной практики по применению законодательства о террористических и экстремистских преступлениях» сказано, способ распространения не имеет значения для квалификации данных преступлений, что под пропагандой терроризма следует понимать распространение любым способом материалов или информации, содержащих идеологию насилия и практику терроризма, посредством воздействия на сознание и волю человека (людей) с целью возбуждения в нем (них) стремления к осуществлению террористической деятельности либо обосновывающих или оправдывающих необходимость осуществления такой деятельности. Публичные призывы к осуществлению акта терроризма включают в себя использование средств массовой информации или сетей телекоммуникаций (периодического печатного издания, теле-радиоканала, интернет-ресурсов и других средств). [14]

Рост уровня доступности глобальной сети Интернет неизбежно приводит к увеличению числа инцидентов информационной безопасности. Лаборатория Kaspersky Security Network сообщает сведения, что 85% интернет атак в Центральной Азии приходится на Казахстан. Для сравнения: на Узбекистан приходится 8%, на Кыргызстан 4%, на Туркменистан 2%, на Таджикистан 1%.[15] Если раньше крупным кибераратакам подвергались в основном правительственные сайты, причем их рост шел одновременно с ростом цифровизации управления. То в последнее время значительно выросла угроза со стороны кибератак в отношении крупного бизнеса. Источником угрозы информационной безопасности для систем государственного управления и социальной стабильности в стране является также утрата данных национальных и государственных информационных систем.

В деле обеспечения информационной безопасности очень важно соблюдение принципа баланса интересов граждан, общества и государства. Поэтому мы предлагаем:

1 В Конституции Республики Казахстан право на информацию имеет различную субъектную принадлежность. При формулировке права на поиск, получение и распространение информации используется слово «каждый» (и гражданин РК, и иностранец). Требовать от государственных органов и должностных лиц предоставления информации, затрагивающей права и интересы, могут только граждане. В редакцию п.3 статьи 18 Конституции необходимо внести изменения и заменить слово «гражданин» на слово «каждый».

2 Большое число нормативных правовых актов в сфере информационного права, возросшая в современном обществе роль информационных ресурсов, необходимость защиты информации и обеспечения информационной безопасности государства требуют систематизации и качественного правового обеспечения. Все это обусловливает необходимость принятия Кодекса Республики Казахстан «Об информатизации».

3 Сравнительный анализ законодательства об информатизации и о национальной безопасности свидетельствует, что действующие законы не устанавливают положений о соотношении угроз информационной безопасности и их источников. В Законе «Об информатизации» не установлены нормы, перечисляющие виды угроз и источников информационной безопасности. Из содержания рассмотренных правовых актов не ясно в чем различие между угрозами и источниками угроз. Считаем, что при подготовке проекта Кодекса об информатизации в части определения угроз и их источников для информационной безопасности можно имплементировать положения Соглашения между правительствами государств – членов ШОС о сотрудничестве в области обеспечения международной информационной безопасности (2010).

4 Для защиты нравственного здоровья несовершеннолетних от негативного влияния информации ввести законодательный запрет на регистрацию в социальных сетях Facebook, В Контакте, Twitter для лиц младше 18 лет без согласия родителей. Компании должны разработать специальный механизм запрашивания согласия родителей на регистрацию в той или иной сети.

5 Дополнить Главу 2 «Уголовные правонарушения против семьи и несовершеннолетних» Уголовного кодекса Республики Казахстан статьей, предусматривающей уголовную ответственность за преступления против несовершеннолетних с использованием информационно-коммуникативных технологий (вовлечение в преступные игры, доведение до самоубийства и др.).

Литература:

1. Международный Пакт о гражданских и политических правах от 16 декабря 1966 / Международные акты о правах человека. Сборник документов по международному праву. – М.: Норма-Инфра, 1998. -784с.

2. Refah Partisi (the Welfare Party) and Others v. Turkey [GC] no 41340/98, 41342/98, 41343/98 et al. (ECtHR, Judgment 13 February 2003) -[Электронный ресурс] – Режим доступа - http://europeancourt.ru/uploads/ The Welfare Party and others v. Turkey.pdf.

3. Закон Республики Казахстан от 23 июля 1999 года № 451-I «О средствах массовой информации» (с изменениями и дополнениями по состоянию на 28.12.2017 г.) – Электронный ресурс – [Режим доступа] -https://online.zakon.kz/document/?doc_id=31396226.

4. Закон Республики Казахстан от 21 мая 2013 года № 94-V «О персональных данных и их защите» (с изменениями и дополнениями по состоянию на 28.12.2017 г.) – Электронный ресурс – [Режим доступа] -https://online.zakon.kz/document/?doc_id=31396226.

5. Закон Республики Казахстан от 24 ноября 2015 года № 418-V «Об информатизации» (с изменениями и дополнениями по состоянию на 28.12.2017 г.) – Электронный ресурс – [Режим доступа] - https://online.zakon.kz/document/.

6. Копылов В.А. Информационное право. –М.: Юрист, 2002. – 612с.
7. Конвенция об обеспечении международной информационной безопасности (концепция) – Электронный ресурс – [Режим доступа] — http://www.scrf.gov.ru/documents/6/112.html.
8. Data Protection Act 1998 – Электронный ресурс – [Режим доступа] - https://www.legislation.gov.uk/ukpga/1998/36/contents.
9. Жарова А.К. Опыт правового обеспечения безопасности персональных данных в Великобритании // Государство и право. – 2017. -№6. –С.70-79.
10. Приоритеты национальной безопасности в условиях глобализации. / Жатканбаев Е.Б. и др.- Алматы: Қазақ университеті, 2006. -329с.
11. Мовкебаева К.А., Карманов А. Информационные операции США в контексте обеспечения кибербезопасности //Вестник КазНУ. Серия м.о. и м.п. -2016.-№2. –С.236-242.
12. Строева Ю. О. Информационная безопасность детей в телекоммуникационных сетях // Молодой ученый. — 2017. — №50.1. — С. 41-43. — URL https://moluch.ru/archive/184/47336/.
13. Танекова М.О. К вопросу о распространении порнографических материалов в социальных сетях // Вестник КазНУ. Серия м.о. и м.п.- 2016. - №4. –С.158-164.
14. Нормативное постановление Верховного Суда Республики Казахстан от 8 декабря 2017 года №11 «О некоторых вопросах судебной практики по применению законодательства о террористических и экстремистских преступлениях» – Электронный ресурс – [Режим доступа]- https://online.zakon.kz/Document/?doc_id=355366.
15. Государственная программа «Цифровой Казахстан». Утверждена Постановлением Правительства Республики Казахстан № 827 12 декабря 2017 года. – Электронный ресурс – [Режим доступа]- https://zerde.gov.kz/activity/management-programs/the-state-program-d.

Амангелдинова З.Ж., Тәңірберген С.С., академик Е.А.Бөкетов атындағы Қарағанды мемлекеттік университеті, экономика факультеті, топ. Фн-21, студенттер
(Ғылыми жетекші – э.ғ.м., аға оқытушы Топшахова Г.Р.)

ТӨЛЕМ КАРТАЛАРЫНА ҚАТЫСТЫ АЛАЯҚТЫҚ МӘСЕЛЕЛЕРІН ШЕШУ ЖОЛДАРЫ

Қазіргі уақытта төлем карточкалары қаржы құралдарының арасында төлем жүйелерінің ең көп бөлігін қамитиды . Алайда бұл қаржылық құралдың өзіне тән кемшіліктері де аз емес оның ішінде осы құралдар арқылы жасалатын түрлі алаяқтық әрекеттер.Карточкалық алаяқтықтың біріншіжәне қазіргі кезде ең көп таралған түрі - «ақ карталар» немесе «клон карталары» деп аталатын карталар жасау. Алаяқтар пайдаланушының картасының магниттік жолағындағы құпия ақпаратты оқиды, содан кейін магниттік жолағы бар пластиктен және ұрланған ақпараттан «ақ карточкалар» жасайды. Осыдан кейін, шабуылдаушылар қолданыстағы картаның иесінің шотын еркін қолдана алады, бұл жағдайда олардың «бөтен» төлемдерге қатыспайтындығын дәлелдеу өте қиын болады.

Картада сақталған құпия ақпаратты оқу әр түрлі жолмен жасалуы мүмкін. Олардың ішіндегі ең көп тарағаны - алаяқтардың дүкендер, қонақүйлер, мейрамханалар және басқа да сауда-ойын-сауық кәсіпорындарының қызметкерлерімен жасырын келіссөздері. Мұндай қастандықтың нәтижесі - қылмыстық құрылымдардың өкілдеріне карточкалардың деректемелері туралы ақпаратты беру. Карта алаяқтардың қолында болса, төлем картасы арнайы құрылғы (скиммер) арқылы өтіп, оның магниттік жолағында сақталған мәліметтерді скимминг арқылы оқи алады. Осылайша, алаяқтар картаның маңызды ақпараттарын аладыжәне оған қажетті соманы енгізерде, қол қою қажет болмайды, ал операция үшін барлық есептерді картаның заңды иесіне бағыттайды.

Қылмыстық құрылымдар өздерінің сауда дүкендерін құруда.Осындай «сауда нүктелерінің» мақсаты қарапайым - клиенттердің пластикалық карталары туралы мүмкіндігінше көп ақпарат алу. Алаяқтар Интернет-сайттарды бұл үшінжиі пайдаланады. Осындай сайттың қызметін бір рет пайдаланып (мысалы, тауарды сатып алған немесе бейне роликті жүктеп алған), карта иесі оның жазылушысы болғанын таң қаларлық түрде анықтайды және осылайша, ай сайын жазылым үшін төлем алынып отырады , одан бас тарту қиын болады.

Карточкалық алаяқтықтың тағы бір түрі фишинг деп аталады. Ол қолданушыдан пластикалық карта туралы мәліметтерді алады. Зиянкестер қолданушыларға өзінің қауіпсіздік жүйесінде болған өзгерістер туралы банктің атынан есеп беретін электрондық пошталарды жібереді. Сонымен бірге, алаяқтар сенімсіз пайдаланушылардан карточка туралы ақпаратты,