УДК 343.3/.7 МРНТИ 10.77.51

Медет Сембайұлы Заркенов
Қазақстан Республикасы Бас прокуратурасының жанындағы
Құқық қорғау органдарының академиясы
Нұр-Сұлтан қ., Қазақстан Республикасы, e-mail: zarkenov@gmail.com

АҚПАРАТТАНДЫРУ ЖӘНЕ БАЙЛАНЫС САЛАСЫНДАҒЫ ШЕТЕЛДЕРДІҢ ҚЫЛМЫСТЫҚ ЗАҢНАМАЛАРЫН САЛЫСТЫРМАЛЫ-ҚҰҚЫҚТЫҚ ТАЛДАУ

Аннотация. Аталмыш мақалада ақпараттық-коммуникациялық технологиялар саласындағы қылмыстық құқық бұзушылықтар мәселесін зерттеу, нәтижелі және ең тиімді шараларды әзірлеу мақсатында ақпараттандыру және байланыс саласындағы қылмыстық құқық бұзушылықтарға қарсы шетелдік әрекет тәжірибесі талданған. Осы саладағы ғылыми әдебиетті талдау барысында, сонымен қоса жүйелі ықпал жасау мен танудың салыстырмалы-құқықтық әдісі негізінде ақпараттандыру және байланыс саласындағы Қазақстан Республикасының құқықтық жүйесіне ұқсас шетелдегі, оның ішінде Армения Республикасының және Әзірбайжан Республикасының нормаларына салыстырмалы талдау жасалынған. Белгіленген мәселелерді зерттеу нәтижесінде, оларды шешу жолдары ұсынылған және аргументтелген. Мақалада сонымен қоса терминологияға және ақпараттандыру және байланыс саласындағы қылмыстық құқық бұзушылықтардың квалификациялық белгілеріне жеке назар аударылған. Аталған шетелдердің қылмыстық-құқықтық нормаларын зерттеу ақпараттандыру және байланыс саласындағы қылмыстық құқық бұзушылықтарға қарсы әрекет етудің тиімділік деңгейін талдауға мүмкіндік береді.

Түйінді сөздер: киберқылмыс, киберқауіпсіздік, ақпараттық және телекоммуникациялық технологиялар, ақпараттық технологиялар, компьютерлік қылмыс, ақпараттандыру және байланыс саласындағы қылмыстық құқық бұзушылықтар.

Заркенов Медет Сембаевич
Академия правоохранительных органов
при Генеральной прокуратуре Республики Казахстан
г. Нур-Султан, Республика Казахстан, e-mail: zarkenov@gmail.com

СРАВНИТЕЛЬНО-ПРАВОВОЙ АНАЛИЗ УГОЛОВНОГО ЗАКОНОДАТЕЛЬСТВА ЗАРУБЕЖНЫХ СТРАН В СФЕРЕ ИНФОРМАТИЗАЦИИ И СВЯЗИ

Аннотация. В данной статье в целях исследования проблем уголовных правонарушений в сфере информационно-коммуникационных технологий, разработки эффективных и наиболее приемлемых мер проанализирован зарубежный опыт противодействия уголовным правонарушениям в сфере информатизации и связи. В ходе анализа научной литературы в данной области, а также на основе системного подхода и сравнительно-правового метода познания сделан сравнительный анализ норм в сфере информатизации и связи зарубежных стран со схожей правовой системой Республики Казахстан, а именно Республики Армении и Азербайджанской Республики. В результате изучения обозначенных проблем предложены и аргументированы пути их решения. В статье также отдельное внимание посвящено терминологии и квалифицирующим признакам уголовных правонарушений в сфере информатизации и связи. Данное исследование представляет возможность анализировать уровень эффективности противодействия уголовных правонарушений зарубежных стран.

Ключевые слова: киберпреступность, кибербезопасность, информационные и телекоммуникационные технологии, информационные технологии, компьютерная преступность, уголовные правонарушения в сфере информатизации и связи.

Medet Sembaevich Zarkenov
The Academy of Law Enforcement Agencies under the
Prosecutor General's Office of the Republic of Kazakhstan,
Nur-Sultan c., the Republic of Kazakhstan, e-mail: zarkenov@gmail.com

COMPARATIVE LEGAL ANALYSIS OF CRIMINAL LEGISLATION OF FOREIGN COUNTRIES IN THE FIELD OF INFORMATIZATION AND COMMUNICATION

Abstract. This article studies and provides the analysis of the problems of criminal offenses in the field of information and communication technologies, the development of effective and the most appropriate measures as well as foreign experience of countering criminal offenses in the field of informatization and communication.

The analysis of the scientific sources in this area as well as study based on using of the system approach and the comparative legal method of knowledge the norms in the sphere of informatization and communications of foreign countries with a similar legal system of the Republic of Kazakhstan such as the Republic of Armenia and the Republic of Azerbaijan has been prepared. As a result of the study the ways for solution of the discussed problems are proposed and argued. The article also focuses on the terminology and qualifying features of criminal offenses in the field of information and communication.

Key words: cybercrime, cybersecurity, information and telecommunication technologies, information technologies, computer crime, criminal offenses in the field of information and communication.

Информационно-коммуникационные технологии широко используются жителями любого государства. Во всем мире протекает процесс цифровизации, эти перемены коснулись и Республики Казахстан. В нашем государстве в период с 2018 по 2020 годы реализуется Государственная программа «Цифровой Казахстан». Комплексная программа направлена на ускорение темпов экономики и повышение уровня жизни жителей Республики Казахстан с использованием информационных технологий [1].

В условиях глобализации, страны мирового сообщества сталкиваются с некоторыми сложностями по защите информации, выявлению уголовных правонарушений и несовершенством уголовно-правовых норм в сфере информатизации и связи. Рассматриваемая сфера требует своевременной и постоянной модификации в силу быстрого развития информационных технологий и цифровизации в разных сферах услуг.

Игнорирование указанных мер может привести к колоссальным издержкам и нанести непоправимый ущерб, как государству, так и жителям страны.

Системы защиты информационных технологий Республики Казахстан находятся на стадии развития. Каждый житель страны имеет по несколько объектов информационно-коммуникационной инфраструктуры (персональный компьютер, смартфон, планшет и т.д.), постоянно находится в контакте с глобальной сетью Интернет, обширно пользуется государственными и частными электронными услугами, электронной торговлей, безналичным расчетом, облачными хранилищами, электронными почтами, носителями и т.д. Все эти обстоятельства создают условия для совершения уголовных правонарушений с использованием информационных технологий, поэтому уголовное законодательство, являясь последним рубежом, должно обеспечивать эффективное предупреждение данных уголовных правонарушений и применение в отношении виновных лиц соответствующих мер наказания.

Отличительной чертой уголовных правонарушений, совершенных с использованием информационных технологий, является сложность выявления и установления состава уголовного правонарушения, так как правонарушение, совершаемое с использованием информационных технологий, может осуществляться латентно и из другого государства. При этом, охраняемая законом информация легко поддается изменениям, копируется, передается, распространяется, блокируется и уничтожается. По этой причине возникают сложности по установлению источника и личности преступника, а также по доказыванию уголовных правонарушений в сфере информатизации и связи.

К примеру, согласно данным главы научно-образовательного центра Службы национальной безопасности Армении, вебсайты государственных органов Армении в течение 11 месяцев 2018 года подверглись 3 миллионам хакерских атак. Эти атаки исходили с территории разных стран мира, и важным фактором для Службы национальной безопасности Армении, явился не физический адрес, а их источник [2].

Отсюда мы видим, что уголовное правонарушение, совершаемое с использова-

нием информационных технологий, не привязано к границам какой-либо страны, в связи с чем сложно раскрыть все факты данных хакерских атак.

Так при совершении традиционного уголовного правонарушения преступник и потерпевший физически присутствуют в определенной географической точке. Поэтому принципы, регулирующие осуществление уголовной юрисдикции, основаны на предположении, что «преступление» является территориальным явлением. Однако, уголовное правонарушение, совершаемое с использованием информационных технологий делает эти принципы проблематичными. Лицо, совершившее такого рода уголовное правонарушение, может физически находиться в стране «А», в то время как его жертвы находятся в странах «Б», «В», «Г» и т.д. К тому же, преступник может усложнить ситуацию, направив свою атаку на жертву в стране «Б» через компьютеры в странах «Д» и «Е». Результатом этих и других сценариев уголовных правонарушений совершаемых с использованием информационных технологий является то, что они не совершаются на территории одного суверенного государства. Следовательно, на уголовное правонарушение может претендовать несколько разных суверенных государств [3, 189 стр.]. При этом, многие страны не желают сотрудничать друг с другом.

В свою очередь, транснациональный характер рассматриваемых преступлений несет угрозу национальным интересам из любой точки земного шара [4, 5 стр.].

К тому же, уголовных правонарушений в данной сфере с каждым днем становится больше, а принимаемые меры в большинстве случаев недостаточно эффективны. При таких обстоятельствах, одной из главных причин является «явное отсутствие эффективного законодательства против киберпреступности» [5, 104 стр.].

В силу высокого уровня развития информационно-коммуникационных технологий в развитых странах, противодействие уголовным правонарушениям совершенных с использованием информационных технологий началось намного раньше. При этом уголовно-правовое регулирование в сфере информатизации и связи Республики Казахстан находятся на стадии становления.

Следовательно, в целях исследования проблем уголовных правонарушений в сфере информационно-коммуникационных технологий, разработки эффективных и наиболее приемлемых мер с учетом национальных интересов, ценности, мировоззрения, менталитета и соответствия мировым стандартам необходимо проанализировать зарубежный опыт противодействия уголовным правонарушениям в сфере информатизации и связи.

На основе системного подхода и сравнительно-правового метода познания в статье представлен сравнительный анализ норм в сфере информатизации и связи зарубежных стран со схожей правовой системой Республики Казахстан, а именно Республики Армении и Азербайджанской Республики.

Исследование уголовно-правовых норм данных стран позволит анализировать уровень эффективности противодействия уголовным правонарушениям в сфере информатизации и связи, а также возможность внедрения этих правовых положений в законодательство Республики Казахстан.

Анализируя уголовные законодательства вышеуказанных стран, можно отметить различие некоторых норм уголовных правонарушений рассматриваемой сферы.

Для начала необходимо отметить, что название сферы информатизации и связи уголовных правонарушений в разных странах различаются, однако суть неизменна. Так, в Республике Казахстан оно именуется «Уголовные правонарушения в сфере информатизации и связи», в Республике Армении «Преступление против безопасности компьютерной информации», в Азербайджанской Республике «Киберпреступления».

Рассматривая данный вопрос, следует выделить, что в анализируемых странах понятие уголовных правонарушений в сфере информатизации и связи и ее единое определение на международной арене отсутствует.

Более того, статья 1 Конвенции о компьютерных преступлениях от 23.11.2001 года (Серия европейских договоров №185, г.Будапешт) ограничилась определением терминов, как «Компьютерная система», «Компьютерные данные», «Поставщик услуг», «Данные о потоках» [6].

Такие термины, как «Преступление в сфере компьютерной информации», «Компьютерная информация», «Вредоносная программа», «Неправомерный доступ» предусмотренные в Соглашение о сотрудничестве государств - участников Содружества Независимых Государств в борьбе с преступлениями в сфере компьютерной информации (г.Минск, 01.06.2001г.) не полностью раскрывают сущность термина, и используются не для всех стран мира [7].

Исходя из этого, необходимо на международном уровне согласовать единую терминологию для оперативного, слаженного и эффективного противодействия уголовным правонарушениям в сфере информатизации и связи.

Глава 7 «Уголовные правонарушения в сфере информатизации и связи» Уголовного кодекса Республики Казахстан (далее – УК РК) дополнена в редакции от 03.07.2014 года. В данную главу включены девять статей (ст.205 «Неправомерный доступ к информации, в информационную систему или сеть телекоммуникаций», ст.206 «Неправомерные уничтожение или модификация информации», ст.207 «Нарушение работы информационной системы или сетей телекоммуникаций», ст.208 «Неправомерное завладение информацией», ст.209 «Принуждение к передаче информации», ст.210 «Создание, использование или распространение вредоносных компьютерных программ и программных продуктов», ст.211 «Неправомерное распространение электронных информационных ресурсов ограниченного доступа», ст.212 «Предоставление услуг для размещения интернет-ресурсов, преследующих противоправные цели», статья 213 «Неправомерные изменение идентификационного кода абонентского устройства сотовой связи, устройства идентификации абонента, а также создание, использование, распространение программ для изменения идентификационного кода абонентского устройства»), устанавливающих ответственность за уголовные правонарушения совершенные с использованием информационных технологий [8].

Источником уголовного права Республики Армении является Уголовный кодекс, вступивший в силу 01.08.2003 года и заменивший Уголовный кодекс Армянской ССР 1961 года.

Естественно, Уголовный кодекс Республики Армении (далее - УК РА) по большей части схож с Уголовными кодексами государств-участников Содружества Независимых Государств (далее - СНГ).

Структура Особенной части УК РК раскрывает иерархию значимости, охраняемых уголовным законом: на первом месте преступления против жизни и здоровья; далее преступления против свободы, чести и достоинства личности; преступления против половой неприкосновенности и половой свободы; преступления против конституционных прав и свобод человека и гражданина; преступления против семьи и интересов ребенка; преступления против собственности; преступления против экономической деятельности; преступления против общественной безопасности; преступления против безопасности компьютерной информации; преступления против общественного порядка и нравственности; преступления против здоровья населения; преступления против безопасности окружающей среды; преступления против основ конституционного строя и безопасности государства; преступления против государственной службы; преступления против порядка управления; преступления против правосудия; преступления против порядка военной службы; преступления против мира и безопасности человечества.

Глава 24 УК РК «Преступления против безопасности компьютерной информации» состоит из семи статьей (ст.251 «Несанкционированный доступ (проникновение) к системе компьютерной информации»; ст.252 «Изменение компьютерной информации»; ст.253 «Компьютерный саботаж»; ст.254 «Неправомерное завладение компьютерной информацией»; ст.255 «Изготовление или сбыт специальных средств неправомерного доступа (проникновения) к компьютерной информации»; ст.256 «Разработка, использование и распространение вредоносных программ»; ст.257 «Нарушение правил эксплуатации компьютерной системы или сети»).

В данной главе объекты посягательств обозначены терминами «Компьютеры», «Компьютерные системы», «Сети» и «Компьютерные оборудования». При этом, определения данных терминов в УК РА не предусмотрены. Тем самым, использова-

ние вышеуказанных терминов при постоянном развитии информационных технологий и появлении новых устройств, оборудований приводит к проблемам в квалификации уголовного правонарушения.

В ст.251 УК РА «Несанкционированный доступ (проникновение) к системе компьютерной информации» предусмотрены квалифицирующие признаки преступления: то же деяние, с использованием должностного положения; группой лиц по предварительному сговору; повлекшее по неосторожности тяжкие последствия [9]. В аналогичной норме УК РК из данных квалифицирующих признаков предусмотрен признак – «повлекшее по неосторожности тяжкое последствие», а остальные охватываются в ст.54 УК РК в виде обстоятельств, отягчающих уголовную ответственность и наказание [8].

Норма об изменении компьютерной информации (ст.252 УК РА) отличается от аналогичных норм государств-участников СНГ тем, что в ней предусмотрено «причинение имущественного ущерба путем обмана или злоупотребления доверием, повлекшие значительный ущерб». Наряду с этим, содержание данной нормы недостаточно раскрывает различие между признаками мошенничества.

Также, приведены квалифицирующие признаки уголовного правонарушения за изменение компьютерной информации сопряженных с несанкционированным доступом (проникновением) к компьютерной системе или сети; совершенные с использованием должностного положения. При этом, в аналогичных нормах Республики Казахстан данные признаки не учтены.

Следует отметить, что ст.254 УК РА предусматривает в качестве разновидностей неправомерного завладения компьютерной информацией два самостоятельных состава уголовных правонарушений:

- неправомерное завладение информацией – основной и квалифицированный состав (ч.ч.1, 3, 4);

- принуждение к передаче информации - основной и квалифицированный состав (ч.ч.2, 3, 4).

Так, законодатель Республики Армении систематизировал два уголовных правонарушения в одной общей статье [9]. При сравнении аналогичных уголовных правонарушений УК РК следует заметить, что две близкие по сути нормы составляют две разные статьи (ст.208 «Неправомерное завладение информацией», ст.209 «Принуждение к передаче информации») [8].

По нашему мнению, систематизация в одной статье УК РК двух близких по смыслу норм обеспечит их согласованность и логичность. В этой связи, считаем целесообразным объединить ст.ст. 208 и 209 УК РК.

Объективные стороны ст.255 УК РК «Изготовление или сбыт специальных средств неправомерного доступа (проникновения) к компьютерной информации», 256 УК РА «Разработка, использование и распространение вредоносных программ» характеризуются альтернативными действиями в виде: разработки, использования, распространения носителей специальных вирусных программ; изготовления в целях сбыта или сбыт специальных программ. В данном случае, законодатель более оправдано подошел к пониманию термина «распространение носителей специальных вирусных программ» разграничив ее термином «сбыт специальных программ» [9]. Такое разграничение можно встретить, и в уголовных законодательствах Республики Беларусь и Азербайджанской Республики.

Вместе с тем, законодатель разделил терминологии «использование специальных вирусных программ» и «распространение носителей вирусных программ». Так как, без соответствующего определения термин «распространение вредоносных компьютерных программ» можно толковать, как сбыт (продажа), передача вредоносных программ другому лицу (может совершаться без участия автора программы), и как распространение (рассылка) вредоносных программ в сеть с целью поражения информационно-технологических систем (данная стадия деяния может считаться оконченным правонарушением за распространение вредоносной программы и покушением на использование вредоносной программы). Однако, в УК РК отсутствует определение понятия «использование, распространение вредоносных компьютерных программ и программных продуктов» и не предусмо-

трены альтернативные деяния, разграничивающие «использование, распространение вредоносных компьютерных программ и программных продуктов» от «сбыта (продажи), передачи вредоносных программ другому лицу» [8].

В качестве примера по распространению вредоносных программ приведем следующее.

В 2017 году появилась вредоносная программа под названием «WanaCrypt0r 2.0» (WannaCrypt, WCry, WannaCry). Программа распространилась с огромной скоростью и нанесла ущерб информационным системам множества стран, в частности испанской телекоммуникационной компании «Telefónica», медицинским учреждениям в Великобритании, американской компании «FedEx», французскому автопроизводителю «Renault», мобильному оператору «Мегафон» и Министерству внутренних дел Российской Федерации.

Принцип работы данной программы, заключался в шифровании информации компьютерных систем. После чего, запрашивалась определенная сумма денежных средств за разблокировку всех данных хранящихся на данной системе [10].

Исходя из приведенного, полагаем, что альтернативные действия совершаемые правонарушителями в указанных нормах УК РА более приемлемы и эффективны в применении уголовного закона. Таким образом, считаем, что в УК РК целесообразно ввести определение понятия «создание, использование и распространение вредоносных программ», а также внести дополнение в ст.210 УК РК в виде альтернативных действий: «сбыт (продажа») вредоносных программ», «передача вредоносных программ другому лицу».

Уголовный кодекс Азербайджанской Республики (далее – УК АР) вступил в силу 01.09.2000 года и заменил Уголовный кодекс Азербайджанской ССР 1960 года.

Структура Особенной части УК АР раскрывает иерархию следующих глав по значимости, охраняемых уголовным законом: на первом месте преступления против мира и безопасности человечности; далее военные преступления; преступления против жизни и здоровья; преступления против свободы и достоинства личности; преступления против половой неприкосновенности и половой свободы личности; преступления против конституционных прав и свобод человека и гражданина; преступления против несовершеннолетних и семейных отношений; преступления против собственности; преступления в сфере экономической деятельности; преступления против общественной безопасности; преступления, связанные с незаконным оборотом наркотических средств и психотропных веществ; преступления против общественной нравственности; экологические преступления; преступления против правил безопасности движения и эксплуатации транспортных средств; киберпреступления; преступления против основ конституционного строя и безопасности государства; преступления против правосудия; коррупционные преступления и иные преступления против интересов службы; преступления против порядка управления; преступления против военной службы.

Глава 30 УК АР «Киберпреступления» состоит из пяти статьей (ст.271 «Неправомерный доступ к компьютерной системе»; ст.272 «Неправомерное завладение компьютерной информацией»; ст.273 «Неправомерное вмешательство в компьютерную систему или компьютерную информацию»; ст.273-1 «Оборот средств, изготовленных для совершения киберпреступлений»; ст.273-2 «Фальсификация компьютерных данных»).

Азербайджанская Республика одно из первых государств-участников СНГ, предусмотревшая в своем УК разъяснение понятий «Компьютерная система», «Компьютерная информация», «Инфраструктурный объект общественного значения», «Серьезное препятствование работе компьютерной системы». Определение таких понятий, как «Компьютерная система», «Компьютерная информация» даёт точное понимание этих терминов, и расширяет круг объектов посягательств в ст.ст.271 - 273-2 УК АР [11].

Понятие по «Инфраструктурным объектам общественного значения» больше сходятся с термином «Критически важных объектов информационно-коммуникационной инфраструктур» используемое в УК РК. При этом, определение данного понятия предусмотрено только в п.24) ст.1 Закона РК «Об информатизации» от

24.11.2015 года [12]. В этой связи, в целях правильной квалификации уголовных правонарушений, считаем целесообразным раскрыть понятие «Критически важных объектов информационно-коммуникационной инфраструктуры» в УК РК.

К квалифицирующим признакам, предусмотренным в ст.ст.271-273, 273-1 УК АР («Неправомерный доступ к компьютерной системе», «Неправомерное вмешательство в компьютерную систему или компьютерную информацию», «Неправомерное завладение компьютерной информацией», «Оборот средств, изготовленных для совершения киберпреступлений») относятся те же деяния совершенные: повторно; группой лиц по предварительному сговору, организованной группой или преступным сообществом (организацией); должностным лицом с использованием своего служебного положения [11]. В рассматриваемой главе УК РК данные квалифицирующие признаки не предусмотрены и некоторые из них приводятся в ст.54 УК РК в виде обстоятельств, отягчающих уголовную ответственность и наказание [8].

Необходимо отметить, что в анализируемой главе УК АР законодателем отдельно выделена норма, направленная против фальсификации компьютерных данных, совершенных путем неправомерного введения, изменения, уничтожения или блокирования компьютерных данных (ст.273-2). Вместе с тем, норма, направленная против неправомерного вмешательства в компьютерную систему или компьютерную информацию (ст.273) регламентируется отдельной статьей [11]. В данном случае, для правильной квалификации деяния законодателю необходимо более точно разграничить эти нормы. В УК РК обе нормы УК АР охватываются ст.206 УК АР «Неправомерное уничтожение или модификация информации». По нашему мнению, выделение нормы, направленной против фальсификации компьютерных данных для Республики Казахстан очень актуальна в условиях цифровизации общественных отношений. Так, персональные данные каждого гражданина РК находятся в определенных базах данных и для получения тех, или иных государственных услуг правонарушители могут фальсифицировать компьютерные данные в угоду своих интересов.

В связи с чем, считаем целесообразным выделить норму, направленную против фальсификации компьютерных данных в отдельную статью УК РК.

Как показал анализ, нормы рассмотренной главы в большей части схожи с уголовно-наказуемыми деяниями указанными в Соглашении о сотрудничестве государств-участников СНГ в борьбе с преступлениями в сфере компьютерной информации (г.Минск, 01.06.2001г.), вступившие в силу 14.03.2002 года [7].

На основании изложенного, считаем целесообразным использовать успешный зарубежный опыт конструирования норм об ответственности за рассмотренные в статье уголовные правонарушения для совершенствования законодательства РК.

Список использованных источников:

1. Об утверждении Государственной программы «Цифровой Казахстан»: Постановление Правительства Республики Казахстан от 12 декабря 2017 года № 827. Режим доступа (http://adilet.zan.kz/rus/docs/P1700000827). Дата обращения: 30.10.2019.

2. Госсайты Армении подверглись около трем миллионам хакерских атак в 2018 году. Режим доступа (https://ru.armeniasputnik.am/society/20181215/16267579/gossajty-armenii-podverglis-okolo-trem-millionam-hakerskih-atak-v-2018-godu.html). Дата обращения: 30.10.2019.

3. Brenner, S. W. Cybercrime jurisdiction // Crime, Law, and Social Change, 46, - 2006, - 245 p. - journal.

4. Kellermann, T. Building a Foundation for Global Cybercrime law Enforcement // Computer Fraud and Security, 5, - 2010, - 245 p. - journal.

5. Schell, B. H., & Martin, C. Cyber crime: A Reference Handbook. - Santa Barbara, California: ABC-CLIO, 2004. – 247 p. - book.

6. Конвенции о компьютерных преступлениях: Будапешт, 23 ноября 2001 года, серия европейских договоров №185. Режим доступа (https://rm.coe.int/CoERMPublicCommonSearchServices/DisplayDCTMContent?documentId=0900001680081580). Дата обращения: 30.10.2019.

7. Соглашение о сотрудничестве государств - участников Содружества Независимых Государств в борьбе с преступлениями в сфере компьютерной информации: Минск, 1 июня 2001 года. Режим доступа (http://www.cis.minsk.by/page.php?id=866). Дата обращения: 30.10.2019.
8. Уголовный кодекс Республики Казахстан: от 3 июля 2014 года № 226-V ЗРК. Режим доступа (http://adilet.zan.kz/rus/docs/K1400000226). Дата обращения: 30.10.2019.
9. Criminal Code of the Republic of Armenia: of April 29, 2003 No. ZR-528. Access mode (https://www.legislationline.org/documents/action/popup/id/8872/preview). Access Data: 30.10.2019.
10. Крупнейшая атака программы-вымогателя WanaCrypt0r / Интернет IT журнал. Режим доступа (http://iteranet.ru/it-novosti/2017/05/13/krupnejshaya-ataka-programmy-vymogatelya-wanacrypt0r/). Дата обращения: 30.10.2019.
11. Criminal Code of the Republic of Azerbaijan: Approved by the Law of the Republic of Azerbaijan of 30 December, 1999, No. 787-IQ. Access mode (https://www.legislationline.org/download/id/8304/file/Azerbaijan_CC_am2018_en.pdf). Access Data: 30.10.2019.
12. Об информатизации: Закон Республики Казахстан от 24 ноября 2015 года № 418-V ЗРК. Режим доступа (http://adilet.zan.kz/rus/docs/Z1500000418). Дата обращения: 30.10.2019.

References:

1. Ob utverzhdenii Gosudarstvennoj programmy «Cifrovoj Kazahstan»: Postanovlenie Pravitel'stva Respubliki Kazahstan ot 12 dekabrja 2017 goda № 827. Rezhim dostupa (http://adilet.zan.kz/rus/docs/P1700000827). Data obrashhenija: 30.10.2019.
2. Gossajty Armenii podverglis' okolo trem millionam hakerskih atak v 2018 godu Rezhim dostupa (https://ru.armeniasputnik.am/society/20181215/16267579/gossajty-armenii-podverglis-okolo-trem-millionam-hakerskih-atak-v-2018-godu.html). Data obrashhenija: 30.10.2019.
3. Brenner, S. W. Cybercrime jurisdiction // Crime, Law, and Social Change, 46, — 2006, — 245 p. - journal.
4. Kellermann, T. Building a Foundation for Global Cybercrime law Enforcement // Computer Fraud and Security, 5, - 2010,- 245 p. - journal.
5. Schell, B. H., & Martin, C. Cyber crime: A Reference Handbook. –Santa Barbara, California: ABC-CLIO, 2004. - 247 p. - book.
6. Konvencii o komp'juternyh prestuplenijah: Budapesht, 23 nojabrja 2001 goda, serija evropejskih dogovorov №185. Rezhim dostupa (https://rm.coe.int/CoERMPublic CommonSearchServices/DisplayDCTMContent?documentId=0900001680081580). Data obrashhenija: 30.10.2019.
7. Soglashenie o sotrudnichestve gosudarstv - uchastnikov Sodruzhestva Nezavisimyh Gosudarstv v bor'be s prestuplenijami v sfere komp'juternoj informacii: Minsk, 1 ijunja 2001 goda. Rezhim dostupa (http://www.cis.minsk.by/page.php?id=866). Data obrashhenija: 30.10.2019.
8. Ugolovnyj kodeks Respubliki Kazahstan: ot 3 ijulja 2014 goda № 226-V ZRK. Rezhim dostupa (http://adilet.zan.kz/rus/docs/K1400000226). Data obrashhenija: 30.10.2019.
9. Criminal Code of the Republic of Armenia: of April 29, 2003 No. ZR-528. Access mode (https://www.legislationline.org/documents/action/popup/id/8872/preview). Access Data: 30.10.2019.
10. Krupnejshaja ataka programmy-vymogatelja WanaCrypt0r / Internet IT zhurnal. Rezhim dostupa (http://iteranet.ru/it-novosti/2017/05/13/krupnejshaya-ataka-programmy-vymogatelya-wanacrypt0r/). Data obrashhenija: 30.10.2019.
11. Criminal Code of the Republic of Azerbaijan: Approved by the Law of the Republic of Azerbaijan of 30 December, 1999, No. 787-IQ. Access mode (https://www.legislationline.org/download/id/8304/file/Azerbaijan_CC_am2018_en.pdf). Access Data: 30.10.2019.
12. Ob informatizacii: Zakon Respubliki Kazahstan ot 24 nojabrja 2015 goda № 418-V ZRK. Rezhim dostupa (http://adilet.zan.kz/rus/docs/Z1500000418). Data obrashhenija: 30.10.2019.