На международном уровне контрольным механизмом Совета Европы по защите прав человека является Европейский суд по правам человека, за решениями которого осуществляет надзор Комитет министров - исполнительный орган Совета Европы.

Список литературы

1.Устав Организации Объединенных Наций, принят в г. Сан-Франциско 26.06.1945, с изм. и доп. от 20.12.1971.

2.Всеобщая декларация прав человека, принята резолюцией 217 А (III) Генеральной Ассамблеи ООН от 10 декабря 1948 года.

3.Конвенция о защите прав человека и основных свобод, заключена в г. Риме 04.11.1950. с изм. от 24.06.2013.

4.Американская конвенция о правах человека, заключена в г. Сан-Хосе, 22 ноября 1969 года.

5.Африканская Хартия прав человека и народов, заключена в г.Найроби, 26 июня 1981 года.

6.Арабская хартия прав человека, принята Советом Лиги арабских государств 22 мая 2004 года.

7.Конвенция Содружества Независимых Государств о правах и основных свободах человека, заключена в г.Минск, 26 мая 1995 г.

8. Водько Н.П., Воронцов Ю.С. Влияние европейского опыта борьбы с преступностью на формирование уголовной политики Российской Федерации // Вестник МГЭИ (он-лайн), 2-2021. // https://mgei.ru/upload/iblock/6b9/vestnik_mgei_2_2021_online.pdf

9. Декларация принципов и программа действий ООН в области предупреждения преступности и уголовного правосудия от 18.12.91 г.

10.Декларация ООН о преступности и общественной безопасности от 12.12.96 г.

11.Рекомендации Комитета Министров Совета Европы от 05.09.95 г. «По политике борьбы с преступностью в изменяющейся Европе»

12.Декларация тысячелетия ООН, принята 08.09.2000 года Резолюцией 55/2 на 8-м пленарном заседании 55-й сессии Генеральной Ассамблеи ООН.

13.Бангкокская декларация о взаимодействии и ответных мерах: стратегические союзы в области предупреждения преступности и уголовного правосудия, принята в апреле 2005 г. на 11-м Конгрессе ООН по предупреждению преступности и уголовному правосудию и одобрена резолюцией Генеральной Ассамблеи ООН от 16.12.05 г.

О МЕРАХ ПРЕДУПРЕЖДЕНИЯ ПРАВОНАРУШЕНИЙ, СОВЕРШАЕМЫХ ПОСРЕДСТВОМ ИНФОРМАЦИОННЫХ СИСТЕМ И СЕТЕЙ ТЕЛЕКОММУНИКАЦИЙ

Еспергенова Е.В., доктор философии PhD, старший научный сотрудник НИИ Карагандинской академии МВД Республики Казахстан им. Б. Бейсенова,
Манджиева Г.Р., магистр юридических наук, научный сотрудник НИИ Карагандинской академии МВД Республики Казахстан им. Б. Бейсенова

Преступность в сфере информационных систем и сетей телекоммуникаций является одной из наиболее актуальных и сложных проблем во всем мире. Анонимность правонарушителей, рост их числа, совершенствование информационных технологий, создающих новые возможности совершения указанных преступлений, создают угрозы для глобальных информационных сетей и общества в целом. Каждая из перечисленных проблем влияет на принятие соответствующих мер в области предупреждения преступлений в сфере информатизации и связи.

Мировая практика предупреждения преступности в информационной сети, в том числе сети Интернет имеет следующие направления: принятие соответствующих законов;

эффективное руководство, развитие потенциала правоохранительных органов и органов уголовного правосудия; информационно-просветительская деятельность; создание прочной базы знаний; взаимодействие между органами государственного управления, обществом, частным сектором; а также сотрудничество на международном уровне.

Ученые-правоведы Д.А. Вечеринский и И.И. Шалькевич выделяют 4 группы мер по противодействию правонарушениям, совершаемым посредствам информационно-коммуникационных технологий: правовые, международные, организационные и технические [1].

К правовым мерам следует отнести разработку норм, устанавливающих ответственность за правонарушения в сфере информатизации и связи, совершенствование уголовного, административного и гражданского законодательства, а также судопроизводства, вопросы контроля за поставщиками телекоммуникационных услуг (в т.ч. Интернета), кроме того наличие стратегий или программ по обеспечению информационной безопасности, либо противодействию киберпреступности.

Следует отметить, что в Республике Казахстан приняты соответствующие правовые меры по противодействию правонарушениям, совершенным посредством информационных систем и сетей телекоммуникаций.

Так Уголовный кодекс Республики Казахстан предусматривает отдельную главу, посвященную уголовным правонарушениям, совершаемым в сфере информатизации и связи. С учетом квалифицирующих обстоятельств, глава 7 «Уголовные правонарушения в сфере информатизации и связи» включает 38 составов уголовных правонарушений против электронных информационных ресурсов и систем или сетей телекоммуникаций.

Также в ряде норм УК РК (ст.188 «Кража», ст.190 «Мошенничество», ст.195 «Причинение имущественного ущерба путем обмана или злоупотребления доверием при отсутствии признаков хищения») содержатся следующие квалифицирующие признаки: «путем незаконного доступа в информационную систему либо изменения информации, передаваемой по сетям телекоммуникаций», «путем обмана или злоупотребления доверием пользователя информационной системы».

Кодекс Республики Казахстан «Об административных правонарушениях» также содержит ряд составов административных правонарушений, за совершение которых предусмотрены меры административной ответственности, в том числе на должностных лиц, не выполняющих обязанности по обеспечению информационной безопасности в виде нарушения требований по эксплуатации средств защиты электронных информационных ресурсов (ст.639 КоАП РК), невыполнения Единых требований, неосуществления или ненадлежащего осуществления собственником или владельцем информационных систем, содержащих персональные данные, мер по их защите (ст.641 КоАП РК).

Кроме того, постановлением Правительства Республики Казахстан от 30 июня 2017 года была принята Концепция кибербезопасности «Киберщит Казахстана», определяющая основные направления реализации государственной политики в сфере защиты электронных информационных ресурсов, информационных систем и сетей телекоммуникаций, обеспечения безопасного использования информационно-коммуникационных технологий. Концепция направлена на обеспечение информационной безопасности государственных органов, физических и юридических лиц, а также выработку механизмов предупреждения и оперативного реагирования на инциденты информационной безопасности [2].

Необходимо отметить, что принимая правовые меры только на национальном уровне, в настоящее время ни одно государство не может в полной мере защитить себя от преступных посягательств в информационном пространстве. Тем самым, представляется возможным организация и осуществление противодействия преступности в указанной сфере на международном уровне, включающего:

– сближение национальных уголовных законодательств о преступлениях, совершаемых посредствам сетей телекоммуникаций и информационных систем;

– разработку на международном уровне и имплементацию в национальное законодательство процессуальных стандартов, позволяющих эффективно расследовать преступления в глобальных информационных сетях;

– международное сотрудничество правоохранительных органов при расследовании преступлений, совершаемых посредствам сетей телекоммуникаций на оперативном уровне [3];

Положения о международном сотрудничестве содержатся в ряде международных и региональных документов в области противодействия «киберпреступности», «преступлениям, связанным с компьютерной информацией» или «преступлениям в сфере информации и информационных технологий». К указанным документам относятся: Конвенция Совета Европы о компьютерных преступлениях, Конвенция Лиги арабских государств, Соглашение о сотрудничестве государств – участников Содружества Независимых государств (СНГ) в борьбе с преступлениями в сфере информационных технологий, Соглашение между правительствами государств – членов Шанхайской организации сотрудничества (ШОС) об обеспечении международной информационной безопасности. Данные международные документы, как правило, содержат общие обязательства государств-членов по сотрудничеству и конкретные механизмы взаимодействия, в том числе выдачу правонарушителей и взаимную правовую помощь.

Республика Казахстан является государством-участником Соглашения СНГ о сотрудничестве в борьбе с преступлениями в сфере информационных технологий, а также участником Соглашения между правительствами государств-членов ШОС о сотрудничестве в области обеспечения международной информационной безопасности.

Кроме того с 2010 года в Казахстане функционирует государственная техническая служба реагирования на компьютерные инциденты KZ-CERT, созданная в целях осуществления координации мероприятий по обеспечению информационной безопасности объектов информатизации «электронного правительства» и критически важных объектов информационно-коммуникационной инфраструктуры, а также реагирование на инциденты информационной безопасности.

Служба является участником ряда международных организаций, в том числе FIRST (Форум Групп реагирования на инциденты и обеспечения безопасности), TI (Надежный представитель для Групп безопасности и реагирования на инциденты), OIC-CERT (Организация исламского взаимодействия Служб реагирования на компьютерные инциденты). Службой реагирования на компьютерные инциденты заключено 20 меморандумов о взаимопомощи и сотрудничестве с профильными структурами зарубежных стран, зафиксировано и обработано более 100 тысяч инцидентов информационной безопасности [4].

Таким образом, международное сотрудничество для Республики Казахстан является ключевым моментом в ликвидации правового вакуума, существующего между развитием информационных технологий и реагированием на них законодательства.

Организационные меры противодействия преступлениям, совершаемым посредствам информационно-телекоммуникационных сетей включают в себя разработку, внедрение в практику, непосредственное осуществление и совершенствование организационных и профилактических мероприятий.

В свою очередь к организационным мероприятиям можно отнести создание органов и организаций, координирующих и осуществляющих противодействие преступлениям, совершаемым посредствам информационных систем и сетей телекоммуникаций.

В большинстве стран мира указанные органы и организации входят в структуру правоохранительных органов. В некоторых государствах ведующую роль в координации противодействия преступности в информационной сфере играют генеральная прокуратура и министерство юстиции, в единичных случаях – министерство связи и технологий (агенство кибербезопасности).

Согласно исследованию, проводимому группой экспертов Управления организации объединенных наций по наркотикам и преступности, наиболее эффективным видом межведоственного сотрудничества по вопросам противодействия преступности в информационной сфере является взаимодействие правоохранительных органов и министерства связи. Кроме того в исследовании подчеркивается важность взаимодействия правоохранительных органов, предпринимательской среды, общественных организаций, исследовательских структур и граждан. Сотрудничество между указанными субъектами имеет большое значение для предупреждения преступности в сфере информационных систем и сетей телекоммуникаций [5].

В Республике Казахстан специализированным подразделением по борьбе с уголовными правонарушениями в сфере информационных технологий является Управление «К», входящее в структуру Департамента криминальной полиции Министерства внутренних дел. Кроме того в составе управлений криминальной полиции Департаментов полиции областей Республики функционируют отделы «К». При раскрытии и расследовании преступлений, совершенных посредствам сетей телекоммуникаций, сотрудники отдела «К» входят в состав следственно-оперативной группы, которая формируется из числа следователей, специализирующихся в расследовании общеуголовных преступлений.

Таким образом существенным недостатком в практической деятельности является то, что выявление и расследование указанной категории преступлений осуществляют сотрудники, имеющие высшее юридическое образование (в соответствии с квалификационными требованиями). Отсутствие у следственных работников органов внутренних дел спецпознаний в расследовании уголовных дел о преступлениях в информационной сфере, недостаточный уровень навыков у сотрудников оперативных подразделений не позволяет своевременно раскрывать преступления, устанавливать доказательства и привлекать к ответственности виновных лиц.

При этом согласно уголовно-процессуальному кодексу РК (ст.ст. 79, 80) лица, обладающие специальными знаниями в IT-сфере и не являющиеся сотрудниками правоохранительным органов (соответственно, не заинтересованные в исходе дела), могут привлекаться лишь в качестве экспертов или специалистов для дачи заключения или технического сопровождения отдельных процессуальных действий [6].

Кроме того, следует отметить, что в Республике Казахстан межведомственное сотрудничество правоохранительных органов с заинтересованными государственными органами (например, с Министерством информатизации и общественного развития РК и с Министерством цифрового развития, инноваций и аэрокосмической промышленности РК) в сфере противодействия правонарушениям, совершаемым посредствам сетей телекоммуникаций находится на недостаточном уровне. Этому свидетельствует отсутствие соглашений и меморандумов о сотрудничестве.

Не смотря на то, что государство и частные компании принимают различные меры по предупреждению преступлений в сфере информационных систем и сетей телекоммуникаций, одной из главных проблем является низкая цифровая грамотность обычных пользователей. Таким образом, важным аспектом предупреждения преступности является виктимологическая профилактика, включающая в себя:

– информирование собственников частных информационных систем, владельцев промышленных предприятий, финансовых организаций и других категорий объектов экономики, а также населения о способах совершения преступлений в сфере компьютерной информации и преступлений, совершаемых с использованием информационно-телекоммуникационных технологий, посредством электронных средств платежа и т.п.,

– информирование ответственности за совершение указанных уголовных правонарушений, а также о способах защиты от таких посягательств;

– формирование в обществе культуры информационной безопасности (правила хранения данных, периодичность и случаи смены паролей, программы родительского контроля за виртуальной деятельностью несовершеннолетних и т.п. [7].

В этой связи в Стратегическом плане развития Республики Казахстан до 2025 года выдвинута инициатива 2.11, которая предусматривает повышение осведомленности граждан по вопросам информационной безопасности, а также внедрение обучения основам безопасного использования информационно-коммуникационных технологий в школах и высших учебных заведениях [8].

Технические меры противодействия преступлениям, совершаемым посредствам сетей телекоммуникаций предполагают предотвращение правонарушений, совершаемых посредствам сетей телекоммуникаций за счет осуществления мероприятий технического характера, обеспечивающих безопасность в информационной сфере, а также формирование материально-технической базы подразделений, осуществляющих борьбу с преступлениями в сфере информационных систем и сетей телекоммуникаций.

Следует отметить, что качественное обеспечение технических мер зависит от оснащенности государственных органов и частных компаний (в том числе занятых в сфере оказания информационно-коммуникационных услуг) системами информационной безопасности, а также от профессиональной компетенции специалистов, обеспечивающих информационную безопасность сетей телекоммуникаций.

Таким образом, в Республике Казахстан предусмотрены правовые, международные, организационные, и технические меры противодействия уголовным правонарушениям в сфере информационных систем и сетей телекоммуникаций. Так, благодаря принимаемым мерам по итогам 2021 года Республика Казахстан поднялась на 9 позиций и занимает 31 место в Глобальном индексе кибербезопасности [9].

Однако с учетом приведенных в статье проблем в сфере противодействия преступлениям, совершаемым посредствам сетей телекоммуникаций, а также в целях более эффективного противодействия указанной категории правонарушений в Республике Казахстан, предлагается следующее:

1. В системе органов внутренних дел (на центральном и областном уровнях) организовать специализированные подразделения по борьбе с преступлениями, совершаемыми посредствам сетей телекоммуникаций, которые будут включать следственно-оперативные группы, функционирующие круглосуточно - 24/7.

2. Пересмотреть вопрос кадровой политики в подразделениях по борьбе с преступлениями, совершаемыми посредствам сетей телекоммуникаций, а именно назначать на должности оперативных работников и специалистов лиц, имеющих техническое образование, с прохождением курсов юридической подготовки.

3. Установить сотрудничество подразделений МВД РК по борьбе с преступностью в информационной сфере с подразделениями Управления мобилизационных работ и информационной безопасности Министерства информатизации и общественного развития РК, а также с Комитетом по информационной безопасности Министерства цифрового развития, инноваций и аэрокосмической промышленности РК путем подписания соглашений и меморандумов о сотрудничестве; а также выстроить эффективную систему взаимодействия государственных органов, коммерческих организаций и населения Республики Казахстан.

Предложенные меры в целом, на наш взгляд, будут способствовать дальнейшему совершенствованию системы предупреждения преступности в сфере информационных систем и сетей телекоммуникаций.

Список литературы:

1. Вечерский Д.А., Шалькевич И.И. Расследование компьютерных преступлений – Минск, 2001.– С.128-145

2. Об утверждении Концепции кибербезопасности «Киберщит Казахстана» // https://adilet.zan.kz
3. Журавленко Н. И., Шведова Л. Е. Проблемы борьбы с киберпреступностьюи перспективные направления международного сотрудничества в этой сфере – Вестник КазГЮ ИУ №1(37)-2018
4. Сайт государственной технической службы реагирования на компьютерные инциденты KZ-CERT // https://sts.kz/nkcib/
5. Доклад Управления организации объединенных наций по наркотикам и преступности «Всестороннее исследование проблемы киберпреступности», Вена, 2013 //https://www.unodc.org/documents/organizedcrime/cybercrime/Cybercrime_Study_Russian.pdf
6. Уголовно-процессуальный кодекс Республики Казахстан от 4 июля 2014 года // https://adilet.zan.kz
7. Чепрасова Ю.В., Шмарион П.В., Основные направления противодействия киберпреступности – Вестник Воронежского института МВД России № 3-2020
8. Стратегический план развития Республики Казахстан до 2025 // https://www.akorda.kz/ru/official_documents/strategies_and_programs
9. Мировой индекс кибербезопасности // https://www.itu.int/hub/pubs/

КӘМЕЛЕТКЕ ТОЛМАҒАН КИБЕРБУЛЛЕРЛЕРДІҢ ЖЕКЕ БАСЫН СИПАТТАУ

Жалмаханов Ж.Ш., Қазақстан Республикасы ІІМ Б.Бейсенов атындағы Қарағанды академиясының ЖООКББФ докторанты

Жасөспірімдердің XXI ғасыр кеселі – кибербуллингке ұшырауының әлеуметтік себептері мен заңнамалық негіздерін сипаттау үшін олардың генетикалық (физиологиялық) және онтогенетикалық (психологиялық) жас ерекшеліктерін, агрессияның пайда болу себеп-салдарларын, кибербуллингке ұшраудың тұрмыстық-тәрбиелік, психологиялық-психикалық себептерін зерттеушілер ізденістерінің негізінде бағамдау қажет.

Кибербуллинг құбылысының мән-мағынасын толық түсіну және түсіндіру үшін осы құбылысқа тікелей қатысы бар агрессия, жас ерекшеліктері, жасөспірімдердің заң алдындағы жауапкершілігі, іс-әрекет мотивациясы, негізгі белгілері деген ұғымдарды ғалымдардың зерттеулеріне сүйене отырып сипаттаймыз.

Зерттеудің өзектілігінеқазіргі уақыттағы жасөспірімдер арасындағы кибербуллинг құбылысының танымалдылығының өсуінегіз болып отыр. Кибербуллинг интернет желісі шеңберінде жүзеге асырылатын кибербуллердің агрессиялық іс-әрекетімен жүзеге асырылады. «Агрессия» түсінігіне (агрессия (aggredi) латын тілінде «шабуыл жасау») дүниежүзілік тәжірибеде көптеген анықтамаларберіліп, іс-әрекеттің кең тарауы жағдайды шиеленістіре түсті [1,139]. Ресейлік психолог С.Н.Еникалоповтың айтуынша, агрессия – бұл адамдардың қоғамда өмір сүру нормалары мен ережелерін бұзатын, шабуыл нысандарына, адамдарға физикалық зиян келтіретін немесе психологиялық тұрғыдан белгілі бір қолайсыздықты тудыратын мақсаттағы деструктивті және қорлайтын мінез-құлық [2,60].

Н.П.Романова агрессивті мінез-құлықтың дамуына анасынан айыру, толық емес отбасылар, билік және авторитарлық отбасылар; жанжалды отбасылық қатынастармен ерекшеленетін отбасылар, зорлық-зомбылыққа генетикалық бейімділігі бар отбасылар [3, 38 б.] деген факторлар әсер етуі мүмкін деген дәлелді тұжырым ұсынады.

Агрессордың жеке басын қалыптастырудың мүмкін алғышарттары көптеген зерттеулердің тақырыбы болды. Мысалы, С.А.Решенин виртуалды тұлғаны психологиялық және әлеуметтік компоненттері бар тұлға ретінде қарастырады, ол өте көп қырлы және негізінен өзін-өзі қалыптастырады және сонымен бірге оның өзін-өзі