ДЕЯТЕЛЬНОСТЬ ЕВРОПЕЙСКОГО СОЮЗА В БОРЬБЕ С КИБЕРПРЕСТУПНОСТЬЮ

Мусабаев Мади Маратулы

студент КазНУ им. аль-Фараби, Республика Казахстан, г. Алматы

Самалдыков Максут Кошекович

научный руководитель, канд. юрид. наук, доц., КазНУ им.аль-Фараби, Республика Казахстан, г. Алматы

Актуальность данной статьи заключается в том, что мы живем в век информационных технологий и в будущем они будут вовлечены в потребности практически во всех сферах человеческой деятельности. Целью правового регулирования всегда были социальные отношения, которые важны для государства, общества и людей, и в наше время информационные отношения стали такими. Это подтверждается тем фактом, что информационные технологии используются в совершенно разных областях, от торговли до государственных услуг. Они также используются для различных целей (торговля, коммуникация, транспорт и т. д.). Все это говорит о том, что информационные технологии уже доказали свою ценность для человечества. Поэтому информационные отношения должны быть справедливо урегулированы законом и обеспечены правовой защитой. Киберпреступность - одна из самых актуальных проблем в мире. Универсальность использования, широкое распространение и доступность дают этой области все больше искушений для представителей криминального мира.Тема статьи является актуальной не только в Российской Федерации и Республики Казахстан , но и в других государствах, в рамках данной работы был взят опыт Европейского союза по борьбе с киберпреступностью.

Поскольку европейское общество трансформируется под влиянием информационных и коммуникационных технологий, вопросы безопасности информационных и коммуникационных технологий (далее именуемые ИКТ) становятся приоритетными для многих государств ЕС, что отражается в реализации стратегий кибербезопасности многими правительствами, причем первостепенное внимание уделяется сосредоточиться на защите критически важной информационной инфраструктуры. В то же время правительства также несут позитивные обязательства по защите граждан от киберпреступности и их прав, а также по привлечению виновных к ответственности.

В марте 2000 года в Лиссабоне состоялся специальный саммит Европейского Союза: Европа на пути инноваций и знаний. (Чрезвычайный Европейский совет Лиссабона (март 2000 г.): к Европе инноваций и знаний). Целью этого саммита было принятие долгосрочных мер со стороны Европейского Союза, в том числе радикальная реформа европейской системы в связи с возрастающей важностью информационных и коммуникационных технологий. В качестве организатора этого саммита Европейская комиссия представила Совету Европы, Европейскому парламенту и Экономическому и социальному комитету регионов сообщение о необходимости создания безопасного информационного общества путем повышения безопасности информационных инфраструктур и борьбе с киберпреступностью (COM (2000) 890).

«Европейская комиссия отметила, что растущее значение информационной и коммуникационной инфраструктуры открывает новые возможности для преступной деятельности. В этом контексте Европейский союз принял ряд мер по борьбе с вредным и незаконным контентом в Интернете, интеллектуальной собственностью и персональными данными. защищать, развивать электронную коммерцию и повышать безопасность

транзакций, в том числе:

• Программа действий против организованной преступности, утвержденная Советом ЕС в мае 1997 года и утвержденная Амстердамским Европейским Советом, по которой Комиссия предложила изучить проблему киберпреступности. Результаты этого исследования («исследование COMCRIME») были представлены в апреле 1998 года;

• пункт «Выводы» саммита Совета Европы в Тампере, в котором подчеркивалась необходимость учитывать преступления в сфере высоких технологий, чтобы согласовать общее определение некоторых преступлений и санкций для их комитета;

• Первоначальные меры в контексте стратегии ЕС по борьбе с преступлениями в сфере высоких технологий ». [1].

«Еврокомиссия предложила подкрепить законодательные меры по гармонизации нормативно-правовых актов государств-членов ЕС по киберпреступности мерами не правового характера, включая:

- Создание специализированных национальных структур;
- Проведение постоянных специальных тренингов для сотрудников полиций и судов;
- Разработку единообразных правил полицейского и судебного делопроизводства и соответствующих методов статистического анализа компьютерной преступности;
- Учреждение Европейского форума в целях поощрения сотрудничества различных участников;
- Поощрение акций соответствующей отрасли промышленности для борьбы с компьютерными преступлениями;
- Проведение исследования под эгидой Евросоюза и проектов по развитию технологий»[1].

Кроме того, «Еврокомиссия намеревалась представить проекты нормативных актов по следующим вопросам:

- Гармонизация национального законодательства государств
- Членов по преступлениям, связанных с детской порнографией;
- Гармонизация уголовного права государств-членов в отношении преступлений в сфере высоких технологий;
- Применение принципа взаимного признания к досудебным решениям, связанных с расследованием киберпреступлений с участием двух и более государств-членов.

Запланированные меры не правового характера включали:

- Создание Европейского форума по сотрудничеству правоохранительных органов, провайдеров услуг, операторов сети, групп потребителей и структур по защите данных на уровне Евросоюза;
- Проведение новых акций по усилению безопасности и доверия в контексте инициативы «Электронная Европа», «Плана действий по Интернету», программы «Технологии информационного общества» и предстоящей рамочной программы по развитию технологий;
- Инициирование новых проектов в рамках существующих программ для поддержки обучения сотрудников;
- Финансирование акций, направленных на улучшение содержания и использования баз данных по национальному законодательству государств-членов»[1].

В 2008 году Совет Европейского Союза разработал стратегию и практические меры по борьбе с киберпреступностью. «В целом, действия Совета ЕС, направленных на борьбу с детской порнографией и других форм сексуального насилия в отношении террористических угроз и крупномасштабных атак в электронных сетях и других традиционных преступлений в Интернете, таких как мошенничество, кражи личных данных, финансовых преступлений, торговли в Интернете, в частности наркотики и оружие, поэтому пятилетняя программа (2010–2014 годы) была утверждена для Генерального директората юстиции и внутренних дел

в области свободы, безопасности и правосудия.»[2].

«Среди трех неотложных мер для борьбы с киберпреступностью Совет ЕС увидел свою роль:

1) призвать все государства-члены Союза ратифицировать Конвенцию Совета Европы о киберпреступности 2001 года как можно скорее, чтобы дать полную поддержку национальным органам, отвечающим за борьбу с киберпреступностью, а также подчеркнуть необходимость сотрудничества со странами вне пределов Европейского Союза;

2) пригласить Европейскую Комиссию принять меры для улучшения публично-частного партнерства;

3) призвать Европол активизировать стратегический анализ киберпреступности»[3].

«Совет также предложил государствам-членам и Европейской комиссии принять технические меры по борьбе с киберпреступностью; Он призвал к принятию долгосрочных и среднесрочных мер в Плане действий, сопровождающем Стокгольмскую программу (2010–2014 годы) и будущую стратегию внутренней безопасности. Среднесрочные меры включают в себя повышение образовательных стандартов для специализации сотрудников полиции, судей, прокуроров и судебных приставов по проведению расследований киберпреступлений и поощрению обмена информацией между правоохранительными органами со стороны государств-членов и других.

Также важно оценить ситуацию в борьбе с киберпреступностью в ЕС и с представителями государств-членов ЕС, чтобы лучше понять тенденции и события и выработать единый подход к борьбе с киберпреступностью на международном уровне. Установление отношений между отдельными европейскими институтами (Евроюст, Европол, ENISA и др.), А также с международными организациями »[3].

Среди организаций, которые в настоящее время борются с киберпреступностью на уровне ЕС, мы можем выделить следующие:

- Европол (обучение национальных полицейских структур, судей и прокуроров борьбе с киберпреступностью);
- Евроюст;
- Европейское агентство сетевой и информационной безопасности (ENISA).

Европейское полицейское управление «было создано на основе Маастрихтского договора 1992 года, далее по тексту статьи 88 Лиссабонского договора 2007 года. Интегрировано в качестве агентства. Основой для условно эффективного функционирования Европола является его информационная система (EIS). Он позволяет вам использовать децентрализованное хранилище и находить информацию об организованных предпочтениях. 11 мая 2016 года Совет Европы и Европейский парламент приняли Регламент (ЕС) 2016/794 о европейском институте сотрудничества правоохранительных органов (Европол), который вступил в силу в 2017 году. Он определил ряд конкретных задач в соответствии со стратегией Европола на 2016–2020 годы, которая будет сосредоточена на существующих проблемах.»[4].

С 2013 года существует новый «Европейский центр по борьбе с киберпреступностью» под эгидой Европола, который координирует деятельность правоохранительных органов и других учреждений, посвященную борьбе с киберпреступностью. Интернет-эксперт Ян Филип Альбрехт, член Партии зеленых и Представитель Европейского парламента считает создание Центра важным шагом в борьбе с киберпреступностью и, в частности, с деятельностью по обучению персонала. «Прежде всего, нам необходимо пройти обучение в полицейских участках в государствах-членах Европейского Союза и обучение персонала. , И не только персонал, который сконцентрирован в Гааге, где расположен Центр, но повсюду в Европейском Союзе », - сказал Альбрехт.»[4].

Что касается Агентства Европейского Союза, в судебных вопросах или Евроюст: «его деятельность по обеспечению безопасности в Европе становится все более ясной: он рассмотрел 1424 дела в 2010 году, 2214 дел в 2015 году. Евроюст выполняет, включая

координацию действий правоохранительных органов различных государств в расследованиях киберпреступлений оказывает содействие в проведении расследований по запросу соответствующих государственных органов стран Европейского союза и предоставляет правоохранительным органам этих стран информацию о проводимых расследованиях киберпреступников. уголовное расследование или внесение предложений о его введении в правоохранительные органы стран-членов ЕС и последующей координации текущих расследований.»[5].

Серьезная озабоченность, как всегда, «ставит вопрос о том, как бороться с киберпреступностью одновременно, не нарушая при этом основных прав и свобод граждан Европейского Союза, особенно после вступления в силу Лиссабонского договора. Обеспечение контроля за деятельностью по борьбе с киберпреступностью является Директивой Европейского парламента и Совета 2009/136 / ЕС от 25 ноября 2009 года »[6].

7 февраля 2013 года Европейская комиссия и Верховный представитель Союза по иностранным делам и политике безопасности объявили о панъевропейской стратегии кибербезопасности и внесли предложения по директиве о мерах по обеспечению высокого общего уровня кибербезопасности в странах Европейского союза. Исполнительный директор ENISA Удо Хельбрехт отметил, что Комиссия достигла огромных успехов, потому что благодаря этой стратегии у Европейского Союза теперь есть направление для действий, которые также будут проводиться в государствах-членах для создания безопасного киберпространства в их странах »[7].

Само агентство поддержало разработку «общеевропейской стратегии», и в 2015 году Европейский совет опубликовал документ об обновлении стратегии кибербезопасности, в котором говорится, что ENISA также будет участвовать в разработке рабочих групп новая стратегия. Кроме того, агентство активно участвовало в разработке национальных стратегий кибербезопасности (НСК), анализируя существующие национальные стратегии, предлагая планы разработки и внедрения неавтоматизированных процедур и предоставляя информацию об успешных проектах по реализации стратегии, с тем чтобы Страны-члены ЕС заявляют о своей стратегии. Например, в декабре 2012 года ENISA выпустила практическое руководство по разработке и реализации национальной стратегии кибербезопасности, ряд действий, которые приведут к реализации успешной национальной стратегии кибербезопасности »[8].

Общеевропейская стратегия »предлагает 5 основных целей для решения проблем кибербезопасности:

1. Обеспечить устойчивость киберпространства Европейского Союза;

2. Сокращение количества киберпреступлений;

3.Разработка политики киберзащиты на основе общей политики безопасности и обороны Европейского Союза;

4. Разработка производственных и технологических средств обеспечения кибербезопасности;

5. Разработать международную политику кибербезопасности, координируемую всеми государствами-членами ЕС с иностранными партнерами для улучшения сотрудничества с третьими странами в этой области "[9].

Для первой цели отмечается необходимость «совместных усилий частного сектора с общественностью, для которой в прошлом была разработана Политика сетевой и информационной безопасности (NIS) и организована ENISA. Кроме того, предлагаются такие шаги, как создание национальных стратегий кибербезопасности». и орган, отвечающий за политику в этой области в каждом государстве-члене; создание механизма обмена информацией между этими органами "[10].

Для второй цели необходимо «принять определенный закон о кибербезопасности, который помог бы сотрудничать с силами стран - членов Европейского союза в борьбе с киберпреступниками. Один из первых шагов что должно стать стратегическим документом -

это подписание всеми государствами ЕС Будапештского договора о киберпреступности (принятого в 2001 году), в котором содержится список преступлений в киберпространстве, которые должны быть зафиксированы в уголовном законодательстве стран, подписавших договор подписать, и соответственно принять реальный тюремный срок в случае нарушения.

Третья цель, в соответствии со стратегией, заключается в содействии развитию киберзащиты Европейского союза с помощью различных средств и технологий: например, доктрин, органов, подготовки специализированного персонала, обеспечения обучения, развития технологий и инфраструктуры. Кроме того, существует необходимость в тестовом сотрудничестве в этой области на международной арене, особенно с НАТО »[10].

Что касается двух последних целей: «Согласно этой стратегии, Европейский Союз должен создать свой собственный рынок для информационных и коммуникационных технологий для безопасных технологий. Чтобы предотвратить зависимость от поставок, и развивать международное сотрудничество в области кибербезопасности, в частности, Соединенные Штаты в рамках Рабочей группы по кибербезопасности и киберпреступности [10].

Исходя из вышеизложенного, общеевропейская стратегия кибербезопасности не является конкретным практическим руководством, а содержит только рекомендованное общее направление, согласно которому государства-члены ЕС разрабатывают свою собственную стратегию кибербезопасности. К недостаткам этой стратегии относится отсутствие концептуального устройства.

На данный момент, каждая национальная стратегия имеет свое определение. Например, финская стратегия определяет слово «кибер» как «совокупность электронной обработки данных, информационных технологий, электронных коммуникаций, информационных и компьютерных систем» [11].

У испанской стратегии уже есть немного другое определение киберпространства: «глобальное поле, которое охватывает информационные технологии, информационные и телекоммуникационные системы (включая сети Интернет), которое не знает границ, вовлекая пользователей в глобализацию» [12].

Однако национальные стратегии – «это конкретные рекомендации, которые необходимо обновить в связи с появлением новой информации, появлением новых угроз и способов борьбы с ними. В этом государства-члены ЕС активно помогают ENISA. С момента публикации первых европейских национальных стратегий (2011 г., Великобритании, Румынии, Германии, Чехии, Литвы) прошло почти 8 лет - с этого момента ENISA активно работала над анализом существующей ситуации в кибер-сфере, давала множество практических рекомендаций, проводила различные общеевропейские мероприятия по кибербезопасности. В настоящее время 23 государства-члена Европейского Союза имеют национальные стратегии кибербезопасности, большинство из которых были созданы после выпуска руководящих принципов ENISA для внедрения НСК в 2012 году - «Национальные стратегии кибербезопасности: руководство по внедрению», в которых собраны практические шаги по реализации целостная национальная стратегия кибербезопасности а также описал показатели эффективности, которые будут нацелены. В 2012 году ENISA также опубликовала статью «Национальные стратегии кибербезопасности» с анализом существующих европейских и международных стратегий кибербезопасности, а также с набором рекомендаций по внедрению и совершенствованию НСК на краткосрочную и долгосрочную перспективу »[13].

Гармонизация законодательства в области «борьбы с киберпреступностью» среди 27 государств-членов ЕС была понята путем принятия следующих законов:

- Европейская конвенция о киберпреступности (преступления в киберпространстве), Будапешт, 23 ноября 2001 года.
- Дополнительный протокол к Конвенции о киберпреступности в отношении криминализации расистских и ксенофобских актов, осуществляемых с использованием компьютерных систем Страсбург, 28 января 2003 г.
- Директива 2000/31 / ЕС о некоторых правовых аспектах услуг информационного

общества, в частности электронной коммерции, на внутреннем рынке;
- Рамочное решение Совета Европейского Союза 2000/413 / JHA «Борьба с мошенничеством и контрафактными безналичными платежными средствами»;
- Рамочное решение Совета Европейского Союза 2004/68 / ПВД «О борьбе с сексуальной эксплуатацией детей и детской порнографии;
- Рамочное решение Совета Европейского Союза 2005/222 / JHA о нападениях на информационные системы »;
- Директива 2006/24 / ЕС о сохранении данных, созданных или обработанных в связи с предоставлением общедоступных услуг электронной связи или сетей связи общего пользования, и изменение Директивы 2002/58 / ЕС
- Рамочное решение Совета Европейского Союза 2008/919 / JHA "О внесении изменений в Рамочное решение 2002/475 / JHA" Против терроризма "".

Перед вступлением в силу Лиссабонского договора „опорный” подход и ограниченные полномочия Европейского Союза принимать законодательство в области уголовного права представляли собой главное препятствие на пути к гармонизации борьбы с киберпреступностью в рамках ЕС. Возможность гармонизации национальных уголовных актов была четко ограничена»[14].

В мае 2007 года, Еврокомиссия представила «Сообщение Европейскому Парламенту Совету и Комитету Регионов от 22 мая 2007 - К общей политике в сфере борьбы с киберпреступностью (COM(2007) 267 final). В этом документе Еврокомиссия презентовала инициативу по содействию общей политике Евросоюза в борьбе со всеми формами киберпреступности. Учитывая ограниченные полномочия Комиссии в области уголовного права, политика Сообщества разрабатывалась исключительно в качестве дополнения деятельности государств-членов.

Комиссия поддержала меры, уже принятые в борьбе с киберпреступностью, в том числе:

• Установление оперативного сотрудничества между правоохранительными органами государств-членов, инициированное совещанием экспертов в 2007 году, результатом которого стало создание Центрального контактного пункта Европейского союза для борьбы с киберпреступностью;

• Усилить финансовую поддержку инициатив по обучению сотрудников правоохранительных органов, занимающихся расследованиями киберпреступлений;

• Помочь правительству более эффективно бороться с киберпреступностью и обеспечить их необходимыми ресурсами;

• Проводить научные и прикладные исследования в борьбе с киберпреступностью;

• Провести Конференцию представителей правоохранительных органов и частного сектора в 2007 году для укрепления их сотрудничества;

• Действовать государственному и частному сектору по предупреждению ущерба и опасностей киберпреступности; - содействие международному сотрудничеству в борьбе с киберпреступностью;

• Помощь государствам-членам ЕС и третьим странам в ратификации Конвенции Совета Европы о киберпреступности;

• Совместные действия Сообщества и государств-членов по предотвращению и борьбе со скоординированными и крупномасштабными атаками на национальные информационные инфраструктуры »[15].

Европейская комиссия подчеркнула, что «борьба с традиционной преступностью в электронных сетях включает в себя следующие действия:

• Проведение обширных исследований для разработки проектов правил ЕС по борьбе с

присвоением «личности» («кража личности»);

• Совершенствование методов борьбы с мошенничеством и незаконной торговлей в интернете;

• Более широкое использование мер по борьбе с мошенничеством в конкретных секторах в отношении использования безналичных платежных средств в электронных сетях.

Инициатива Европейской комиссии, изложенная в этом сообщении, преследует следующие цели:

• Усиление борьбы с незаконным контентом в Интернете, который ведет к терроризму и сексуальному насилию над детьми;

• Рекомендовать государствам-членам увеличить свою финансовую поддержку для правоохранительных органов, с тем чтобы они могли более эффективно выполнять свои обязанности, в частности, путем выявления жертв сексуального насилия с помощью электронных изображений;

• Продвижение мер по борьбе с незаконным содержанием материалов в сети, способных спровоцировать агрессивное поведение несовершеннолетних;

• Укрепление диалога между государствами-членами ЕС и третьими странами по техническим методам борьбы с нелегальным контентом и процедурам ликвидации нелегальных веб-сайтов;

• Установить соглашения на уровне ЕС между государственными органами и частным сектором, в частности с Интернет-провайдером, о процедурах блокирования и закрытия нелегальных веб-сайтов »[15].

Одной из наиболее важных мер ЕС по борьбе с киберпреступностью стала также рекомендация Совета от 25 июня 2001 года о круглосуточных контактных пунктах для борьбы с преступлениями в сфере высоких технологий. 19 марта 1998 года в контексте «восьмерки» Совет Европейского Союза призвал государства-члены присоединиться к круглосуточной информационной сети по преступлениям в сфере высоких технологий. Эта сеть должна была предоставить странам-членам аналитическую оценку преступлений в компьютерных сетях, принимая во внимание тот факт, что такие преступления часто совершаются одновременно в разных местах и в разных странах. На своей встрече в Вашингтоне 9 и 10 декабря 1997 года министры юстиции и внутренних дел стран G8 приняли основные принципы информационной сети, а также План действий, предусматривающий условия доступа для стран, не входящих в "восьмерку". Эта сеть была создана в период 1998-2000 годов "[16].

Те государства-члены ЕС, которые не были включены в информационную сеть под эгидой «большой восьмерки», присоединились к центральной справочной системе Интерпола. Но она не всегда обеспечивает работу 24 часа в сутки. Необходимо было работать совместно двумя информационными сетями. Кроме того, страны, участвующие в Европейском союзе, которые не участвуют в сети G8, должны были иметь возможность 24 часа в сутки звонить своим специализированным подразделениям, которые были частью сети Интерпола »[16].

Исходя из вышесказанного, Совет рекомендовал государствам членам, не присоединившихся к информационной сети контактных пунктов «Большой Восьмерки», вступить в нее, а национальным подразделениям, действующим в качестве контактных центров, специализироваться по преступлениям в сфере высоких технологий. Рекомендовалось также обеспечить этим подразделениям возможность принимать оперативные меры.

Кроме того, в «сообщении Комиссии от 22 января 2004 года о нежелательных коммерческих сообщениях или «спаме» Европейский союз принимает меры по борьбе с киберпреступностью в форме так называемого «спама». Электронная почта, предназначенная для неопределенного круга лиц, доставленная абоненту и / или пользователю без их предварительного согласия, в результате чего отправитель сообщения не может быть

идентифицирован, в том числе из-за упоминания несуществующего или поддельного адреса отправителя». 17]. В сообщении подчеркивается, что всего за несколько лет проблема спама чрезвычайно возросла. Более 50% мирового почтового трафика в 2004 году было спамом, хотя доля в World Wide Web в 2001 году составляла всего 7%.

По мнению комисии, спам является проблемой общества по следующим причинам:

- Вторжение в личную жизнь;
- Предоставление часто мошеннической и вводящей в заблуждение информации;
- Шокирующий порнографический спам;
- Потеря времени (пустые почтовые ящики) и финансовых затрат пользователя (покупка программного фильтра);
- Значительные затраты на структуру компании: ИТ-отделы тратят все больше энергии и денег на решение этой проблемы.

Время, затрачиваемое на пустые почтовые ящики, также снижает эффективность и производительность деятельности. Существуют косвенные расходы: некоторые легальные коммерческие и деловые сообщения не доставляются из-за доступных технологий антиспамовой фильтрации. По имеющимся оценкам, спам обошелся европейским компаниям в производстве в 2,5 миллиарда евро в 2002 году, отметили в Европейской комиссии. «[18]

Нашей задачей в данной статье было проанализировать деятельность Европейского союза в борьбе с киберпреступностью. Исходя из вышесказанного, мы пришли к выводу, что ЕС осознает важность предупреждения и пресечения киберпреступлений. Проведение саммитов и различного рода собраний и конференций, направленных на определение эффективных способов и мер пресечения и предупреждения компьютерных преступлений, играют важную роль в борьбе с киберпреступностью. Создание большого количества структур, (Европол, Евроюст, ENISA и т.д.) ведущие борьбу с киберпреступностью, и наделение их широкой компетенцией говорит о том, что для Евросоюза борьба с киберпреступлениям действительно является приоритетной целью. Принятие международных актов, которые регулируют борьбу с киберпреступностью, привело к гармонизации европейского законодательства в исследуемой сфере. Многолетние программы, имеющие рекомендательный характер, также регулирующие борьбу с киберпреступностью, были приняты в целях совершенствования законодательства государств участников ЕС. Тем самым, Европейский союз внес огромный вклад в борьбу с киберпреступностью.

Хотим отметить, что в Республике Казахстан была принята «концепция кибербезопасности «Киберщит Казахстан» от 30 июня 2017 года №407, в ходе разработки, которой был изучен международный опыт таких стран как Малайзия, Сингапур, Великобритания, Франция, Германия и д.р.

Период реализации Концепции состоит из двух этапов: первый этап 2017-2018 гг., Второй этап 2019-2022 гг., В период первого этапа будет:

- создана широкая правоприменительная практика для удовлетворения требований, уже установленных в области информационной безопасности;

- проведен аудит образовательных программ и профессиональных стандартов, увеличено количество и качество подготовленных специалистов по информационной безопасности и повышена квалификация существующих сотрудников в этой области;

- создана эффективная схема взаимодействия и сотрудничества промышленности и науки в создании отечественных разработок.

Что позволит на втором этапе обеспечить:

- значительное участие IT-компаний в Казахстане в обеспечении национальной информационной и коммуникационной инфраструктуры системами информационной безопасности.

«Загрузка отечественным компаниям в электронной промышленности заказов на закупки со стороны государственных органов и квазигосударственного сектора телекоммуникационного оборудования» [19]. В Российской Федерации «на основе международного опыта была принята Доктрина информационной безопасности от 5 декабря 2016 года, которая представляет собой сборник официальных взглядов на цели, принципы и основные направления обеспечения информационной безопасности Российской Федерации для:

- Формирование государственной политики в области информационной безопасности Российской Федерации;
- Подготовка предложений по совершенствованию правового, методического, научно-технического и организационного обеспечения информационной безопасности Российской Федерации;
- Разработка целевых программ обеспечения информационной безопасности Российской Федерации »[20].

На наш взгляд, необходимо перенять европейский опыт в законодательство РК и РФ, путем создания безопасной среды с помощью «горячих линий», принятия кодекса поведения интернет провайдеров, развития систем фильтрации информации в сети, повышение осведомленности населения, в первую очередь, детей так как они наиболее уязвимы а также стимулирование и поощрение саморегулирования в вопросах оценки качества сайтов, содержания информации, рейтинга системы фильтрации и т.д.

Список литературы:

1. В. Г. Киютин А. П. Новиков правовое регулирование борьбы с киберпреступностью, кибертерроризмом и трафиком людей: опыт европейского союза 2010 М. с .9-15.

2. Ralf Bosen, Cybercrime is Europe’s ‘big challenge’, Sci-Tech, Dw.De, 31.05.2012. Интернет-ресурс: https://www.dw.com/en/cyber-crime-is-europes-big-challenge/a-15988087

3. Прокофьев, В.К. Международно-правовые проблемы обеспечения международной информационной безопасности в сети Интернет. Москва, 2009 г. с. 57-60

4. Якимова Е.М. Нарутто С.В. Международное сотрудничество в борьбе с киберпреступностью 2016. М. с.376

5. Директива Европейского Парламента и Совета Европейского Союза 2002/22/ЕС от 7 марта 2002 г. об универсальных услугах и правах пользователей в отношении сетей электронных коммуникаций и услуг. Интернет-ресурс: https://pd.rkn.gov.ru/docs/Direktiva_Evropejskogo_Parlamenta_i_Soveta_Evropejskogo_Sojuza_200222ES_ot_7_marta_2002.pdf

6. National Cyber Security Strategies. Practical Guide on Development and Execution [Electronic resource] / European Network and Information Security Agency. 2012. URL: https://www.enisa.europa.eu/media/news-items/new-eu-cybersecurity-strategy-directive-announced

7. Draft Council Conclusions on the Renewed European Union Internal Security Strategy 2015-2020 [Electronic resource] / Council of the European Union. 2015. URL: http://statewatch.org/news/2015/jun/eu-council-iss-draft-conclusions-9416-15.pdf

8. Cybersecurity Strategy of the European Union: An Open, Safe and Secure Cyberspace [Electronic resource] / Brussels. 2013. URL: http://eeas.europa.eu/policies/eu-cyber-security/cybsec_comm_en.pdf

9. Вагнер Е.В. Оценка эффективности и перспективы развития Европейского агентства по сетевой и информационной безопасности (ENISA). 2016- Санкт-Петербург/ с.43-47

10. Finland´s Cyber security Strategy [Electronic resource] / Finland. : Forssa print, 2013. URL: https://www.enisa.europa.eu/activities/Resilience-and-CIIP/national-cyber-security-strategies-

ncsss/FinlandsCyberSecurityStrategy.pdf

11. NATIONAL CYBER SECURITY STRATEGY [Electronic resource] / Spain. 2013. URL: https://www.enisa.europa.eu/activities/Resilience-and-CIIP/national-cyber-security-strategies-ncsss/NCSS_ESen.pdf

12. An evaluation Framework for National Cyber Security Strategies [Electronic resource] / European Union Agency for Network and Information Security. 2014. URL: https://www.enisa.europa.eu/activities/Resilience-and-CIIP/national-cyber-security-strategies-ncsss/an-evaluation-framework-for-cyber-security-strategies-1

13. П.Н. Бирюков Международное право том-2, г. Воронеж,2018 – с. 290

14. Communication from the Commission to the European Parliament, the Council and the Committee of the Regions of 22 May 2007 – Towards a general policy on the fight against cybercrime [COM(2007) 267 final https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=LEGISSUM%3Al14560

15. Council Recommendation of 25 June 2001 on contact points maintaining a 24-hour service for combating high-tech crime. Интернет-ресурс: https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX:32000F0503

16. Ляпидов К.В. Спам: понятие, виды, последствия и методы противодействия. М. 2015 Интернет-ресурс: http://xn----7sbbaj7auwnffhk.xn--p1ai/article/7647

17. Communication from the Commission of 22 January 2004 on unsolicited commercial communications or 'spam' Интернет-ресурс: https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=LEGISSUM%3Al24190a

18. Decision 276/1999/EC of the European Parliament and of the Council of 25 January 1999 adopting multiannual Community action plan on promoting safer use of the Internet by combating illegal and harmful content on global networks. Интернет-ресурс: https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A31999D0276

19. Постановление Правительства Республики Казахстан от 30 июня 2017 года № 407 «Об утверждении Концепции кибербезопасности («Киберщит Казахстана»). Интернет-ресурс: https://tengrinews.kz/zakon/pravitelstvo_respubliki_kazahstan_premer_ministr_rk/hozyaystvennaya_deyatelnost/id-P1700000407/

20. Указ Президента Российской Федерации от 05.12.2016 г. № 646 «Об утверждении Доктрины информационной безопасности Российской Федерации». Интернет-ресурс: https://rg.ru/2016/12/06/doktrina-infobezobasnost-site-dok.html