ЕУРАЗИЯ ҰЛТТЫҚ УНИВЕРСИТЕТІ

ҚАЗАҚСТАН РЕСПУБЛИКАСЫ
ТҰҢҒЫШ ПРЕЗИДЕНТІ - ЕЛБАСЫНЫҢ ҚОРЫ

«ҒЫЛЫМ ЖӘНЕ БІЛІМ – 2017»

студенттер мен жас ғалымдардың
XII Халықаралық ғылыми конференциясының
БАЯНДАМАЛАР ЖИНАҒЫ

СБОРНИК МАТЕРИАЛОВ
XII Международной научной конференции
студентов и молодых ученых
«НАУКА И ОБРАЗОВАНИЕ – 2017»

PROCEEDINGS
of the XII International Scientific Conference
for students and young scholars
«SCIENCE AND EDUCATION - 2017»

14th April 2017, Astana

ҚАЗАҚСТАН РЕСПУБЛИКАСЫ БІЛІМ ЖӘНЕ ҒЫЛЫМ МИНИСТРЛІГІ
Л.Н. ГУМИЛЕВ АТЫНДАҒЫ ЕУРАЗИЯ ҰЛТТЫҚ УНИВЕРСИТЕТІ

«Ғылым және білім - 2017»
студенттер мен жас ғалымдардың
XII Халықаралық ғылыми конференциясының
БАЯНДАМАЛАР ЖИНАҒЫ

СБОРНИК МАТЕРИАЛОВ
XII Международной научной конференции
студентов и молодых ученых
«Наука и образование - 2017»

PROCEEDINGS
of the XII International Scientific Conference
for students and young scholars
«Science and education - 2017»

2017 жыл 14 сәуір

Астана

УДК 378

ББК 74.58
Ғ 96

Ғ 96
«Ғылым және білім – 2017» студенттер мен жас ғалымдардың XII Халықаралық ғылыми конференциясы = The XII International Scientific Conference for students and young scholars «Science and education - 2017» = XII Международная научная конференция студентов и молодых ученых «Наука и образование - 2017». – Астана: http://www.enu.kz/ru/nauka/nauka-i-obrazovanie/, 2017. – 7466 стр. (қазақша, орысша, ағылшынша).

ISBN 978-9965-31-827-6

Жинаққа студенттердің, магистранттардың, докоранттардың және жас ғалымдардың жаратылыстану-техникалық және гуманитарлық ғылымдардың өзекті мәселелері бойынша баяндамалары енгізілген.

The proceedings are the papers of students, undergraduates, doctoral students and young researchers on topical issues of natural and technical sciences and humanities.

В сборник вошли доклады студентов, магистрантов, докторантов и молодых ученых по актуальным вопросам естественно-технических и гуманитарных наук.

УДК 378

ББК 74.58

ISBN 978-9965-31-827-6

©Л.Н. Гумилев атындағы Еуразия ұлттық университеті, 2017

УДК 341

ПРАВОВОЙ АСПЕКТ ОБЕСПЕЧЕНИЯ КИБЕРБЕЗОПАСНОСТИ В ЕВРОПЕЙСКОМ СОЮЗЕ

Абдуллина Жанар Бауржанкызы
she_wolf777@mail.ru
Студентка 3 курса специальности «Международное право» Юридического факультета ЕНУ им. Л.Н. Гумилёва, Астана, Казахстан.
Научный руководитель – М.Ж.Куликпаева

На сегодняшний день становится всё более актуальным вопрос правового регулирования киберпространства. Причины этого кроется в том, что всё большее количество сфер жизни человека находит своё отражение в электронных носителях информации, Интернете и иных средствах. Недостаточно полное регулирование данной области с точки зрения закона потенциально опасно, начиная с банального нарушения авторских прав и заканчивая раскрытием защищаемых персональных данных и государственных тайн, разглашение которых может повлечь за собой преступления уже в реальной жизни.

Для того, чтобы обеспечить защиту киберпространства, нужно первоначально определить, чем оно является. Согласно стандарту ИСО/МЭК 27032:2012 «Руководящие указания по кибербезопасности» киберпространство – это «сложная среда, не существующая ни в какой физической форме, возникающая в результате взаимодействия людей, ПО, интернет сервисов посредством технологических устройств и сетевых связей» [1]. Таким образом, можно выделить три основных объекта для защиты. Это:

1. Информация в ее цифровом представлении: статическом (файлы, записанные на носители данных) и динамическом (пакеты, потоки, команды, запросы, и т.д. передаваемые по различным сетям, обрабатываемые в автоматизированных системах и представляемые на средствах отображения в графическом или текстовом виде).
2. Техническая инфраструктура, информационно-коммуникационные технологии, программное обеспечение, с помощью которых осуществляется реализация основных действий с информацией: сбор, обработка, хранение и передача. К таковым средствам можно отнести инфраструктуру Интернет и сетевые взаимосвязи, компьютеры, всевозможные гаджеты и т.д.
3. Информационное взаимодействие субъектов с использованием информации получаемой (передаваемой) и обрабатываемой посредством технической инфраструктуры. Здесь подразумеваются все виды деятельности пользователей или участников киберпространства, которые они осуществляют с использованием информационных ресурсов, потоки и хранилища которых располагаются на технической инфраструктуре [2].

И для того, чтобы иметь возможность защищать все вышеприведённые объекты на уровне Союза, им было создано Европейское агентство по сетевой информационной безопасности (ENISA) в 2004 году. Целью появления данного агентства Европейского Союза было увеличение уровня эффективности функционирования и работоспособности внутреннего рынка. ЭНИСА выступает в организации как консультант и центр передовых технологии в сфере сетевой и информационной безопасности для стран-членов и институтов Европейского Союза. Помимо этого агентство оказывает содействие развитию отношений между государствами-участниками Европейского союза, его отдельными институтами, хозяйствующими субъектами и сектором частного бизнеса, то сеть теми, на кого сфера кибербезопасности оказывает наибольшее влияние. Одним из важнейших аспектов в структуре ЭНИСА является то, что при нём также существует экспертная комиссия (Permanent Stakeholder Group, PSG), в числе которых есть представители частных компаний, например,

таких как Google, SAP, Verizon и ряд ученых. То есть это свидетельствует о том, что в работе ЭНИСА принимают участие специалисты, обладающие достаточным уровнем знаний в необходимой сфере, и что Европейский Союз сам стремится к обеспечению данного типа безопасности на своей территории.

Первоначально должным образом данным вопросом озаботились на уровне государств-членов. Так, в 2005 году Германия приняла Государственный план защиты информационной инфраструктуры (National Plan for Information Infrastructure Protection – NPSI). И уже в следующем, 2006 году Швеция вслед за ней разработала свою Стратегию усиления безопасности Интернета в Швеции (Strategy toim prove Internet security in Sweden). Ожидаемым последствием обширной кибератаки в 2007 году для Эстонии стало опубликование в 2008 году широкой государственной стратегии кибербезопасности. С того момента в данной области на уровне стран была проведена обширная работа, и её результатом последних лет стало то, что десять государств-участников Европейского Союза опубликовали собственные государственные стратегии кибербезопасности. Некоторые страны, также входящие в Европейский Союз, на сегодняшний день создают свои стратегии, работа над которыми близится к завершению [3].

Если говорить, что происходило на уровне институтов Евросоюза, то следует сказать, что на собраниях Европейской комиссии затрагивался вопрос важности сетевой и информационной безопасности и необходимости создания единого Европейского Информационного Пространства. В существующих и продвигаемых правках нормативно-правовой базы, а также на собраниях Европейской комиссии, посвященных защите ключевой информационной инфраструктуры (CIIP), предлагаются практические меры и регулятивные нормы по усилению безопасности и надёжности сетей общего пользования. Таким образом, нельзя сказать, что данный вопрос не освещается на заседаниях важнейших институтов Европейского Союза.

Также в 2013 году был одобрен Европейским Парламентом проект Директивы о масштабных кибератаках, согласно которой неавторизованный доступ к информационным системам, нарушение их работы и перехват контроля будут квалифицироваться как уголовно наказуемые правонарушения. Данная директива определила и криминализировала абсолютно новые для европейского пространства в целом составы преступлений. В их число вошли: создание и использование пригодного для атак инструментария, такого как ботнеты или средства автоматизированного подбора паролей, а также «незаконный перехват» информационных систем. Круг лиц, способных нести правовую ответственность, также был подвержен изменению и расширению: теперь подвергаться уголовной ответственности будет не только непосредственный исполнитель киберпреступления, но и его подстрекатель, пособник (например, человек, создающий потенциально опасные программы и распространяющий их без специальных разрешений – то есть человек, своими действиями способствовавший совершению преступления), покушающийся на совершение преступления. Был определён Директивой и максимальный срок за совершение правонарушения — 2 года и более, за совершенное в составе организованной преступной группировки — до 5 лет и более. Получили должное определение и отягчающие обстоятельства в данной разновидности преступлений, которые могут влечь за собой увеличение ответственности сверх уже установленного максимума: использование специализированного инструментария (в первую очередь ботнетов) против значительного количества информационных систем — не менее 3 лет; причинение серьезного ущерба — не менее 5 лет; атака на критическую, то есть особенно важную для ЕС, инфраструктуру — не менее 5 лет. Кроме того новая Директива также рассматривает и усиление трансграничного взаимодействия судебных органов и полиции. Государствам-участникам ЕС согласно ей будет необходимо привести в действие использование общеевропейской сети защитников правопорядка, функционирующей в круглосуточном режиме. Длительность ожидания ответа на срочный запрос, который будет подан по этой сети, составляет не более 8 часов. Сбор базовой статистики по киберпреступлениям является обязательным для всех членов Европейского Союза, которые

помимо всего прочего будут должны обеспечить наличие и функционирование каналов для передачи соответствующих отчётов в органы, обладающие надлежащей компетенцией [4].

То есть, кибербезопасность все чаще уходит от того уровня регулирования, когда это осуществлялось только государством, и сейчас рассматривается, как стратегическая проблема не только государственной важности, но и достигшей уровня Союза и затрагивающей все слои общества. Для осуществления поддержки стран-членов Европейского Союза в разработке и поддерживании государственной политики кибербезопасности, ENISA разрабатывает специальное руководство (Good Practice Guide). В данном руководстве приводятся рекомендации, а также передовая практика по разработке, внедрению и поддержке в актуальном состоянии стратегии кибербезопасности. Это руководство содержит в себе краткий анализ состояния стратегий кибернетической безопасности государств-участников Евросоюза на момент издания, а также других стран; получают определение аналогичные характеристики и различия в стратегиях; и в самом конце содержатся выводы и рекомендации. Также с 2010 года ENISA осуществляет сотрудничество с группами экспертов по кибербезопасности и правоохранительными органами стран-членов ЕС. В число их совместных действий входит проведение семинаров, объединяющих членов обеих структур для обсуждения таких тем, как аспекты киберпреступности, смягчения массовых кибератак, объединяющих силы для борьбы с ботнетами и т.д. Также эксперты в сотрудничестве с правоохранительными органами в борьбе с киберпреступностью издают сборник передовой практики. Между обеими структурами проходят исследования по обмену информацией и общей таксономии. Особняком стоит вопрос о выявлении возможных правовых и оперативных проблем, которые могут мешать и мешают сотрудничеству, и вытекающих из этого рекомендациях.

Также ENISA осуществляет свою деятельность в сфере стандартизации. Так, Группа по координации кибербезопасности Агентства,имеющая мандат на координацию стандартов кибербезопасности, опубликовала «Белую книгу» с рекомендациями по цифровой безопасности.

В 2015 году ENISA участвовала в двух исследованиях: в разработке Рамочного решения для европейской стандартизации и Определения кибербезопасности.

Вдобавок к этой работе ENISA подготовила в 2015 году исследование, чтобы подготовить рекомендации о том, как повысить понимание кибербезопасности и стандартов конфиденциальности в сфере малого и среднего бизнеса. Анализ, основанный на интервью с экспертами по тематике и обзоре имеющихся исследований, показывает, что, несмотря на растущую обеспокоенность по причине рисков информационной безопасности, уровень обеспечения информационной безопасности и конфиденциальности частной жизни предприятий малого и среднего бизнеса относительно низок [5].

Возвращаясь к вопросу о том, как регулируется на уровне отдельных государств-членов ЕС, следует упомянуть, что именно содержится в соответствующих стратегиях этих государств.

Так, Эстонская Стратегия ставит во главу угла необходимость защиты кибернетического пространства в общем и акцентирует внимание на безопасности информационных систем. Меры, которые она рекомендует, носят гражданский характер и зиждутся на правовом регулировании, обучении и сотрудничестве.

Отличительной чертой Стратегии Финляндии является то, что она понимает кибербезопасность как проблему экономического характера, и недостаток в обеспечении данного типа безопасности рассматривает как способный оказать негативное влияние на развитие финского информационного общества.

Словакия в свою очередь рассматривает обеспечение информационной безопасности как необходимое условие для нормального функционирования и развития общества. Именно по этой причине цель стратегии определяется как служение прочным фундаментом для защиты информации. Стратегия направлена в равной степени как на предотвращение

непосредственных угроз, так и на обеспечение готовности и устойчивости средств их предотвращения.

Стратегии кибербезопасности Чехии определяет для себя ключевыми целями защиту информационно-коммуникационных систем от тех уязвимостей, которым эти системы подвергнуты, и минимизацию потенциального ущерба от атак на системы. Основной упор стратегии приходится на проблемы свободного доступа к информационным сервисам, целостности и конфиденциальности данных в киберпространстве Чехии. Таким образом, отличительной чертой Стратегии данного государства является то, что она затрагивает немаловажный вопрос недостаточного уровня регулирования доступа обычных граждан – а значит и потенциальных преступников – к средствам осуществления деятельности в электронных сетях. Помимо прочего Стратегия согласуется в достаточной мере с иными нормативно-правовыми документами Чехии, которые в той или иной степени также регулируют данную сферу.

Направленность Франция характеризуется фокусировкой на том, чтобы информационные системы обладали способностью противостоять событиям в кибернетическом пространстве, которые могут негативно повлиять на доступность, целостность и конфиденциальность информации. Технические средства защиты информации, борьба с киберпреступностью и установление киберзащиты – то, чем отличается стратегия Франции, и здесь моно заметить, что именно это государство одним из первых обратило внимание на выделение киберпреступности из ряда иных нарушений деятельности в киберпространстве.

Немецкая Стратегия освещает важность обеспечения безопасности критически важных информационных систем. Таковыми следует считать те, функционирование которых серьёзно сказывается на жизни общества и государства. Германия фокусируется на предотвращении и, так же, как и Франция, на уголовном преследовании кибератак, а также на предупреждении выхода из строя IT-оборудования, которые может быть вызвано случайно. Последнее особенно касается значительно важных информационных систем. В стратегии проводится анализ того, нужно ли предпринимать дополнительные действия (в случае, если нужно, то где именно) по защите IT-систем посредством предоставления основных функций безопасности, сертифицированных государством, а также поддержкой малого и среднего бизнеса путём создания новой рабочей группы.

Характерной чертой деятельности Литвы в этой сфере является то, что её стратегия уделяет внимание развитию оборота электронной информации, обеспечения сохранения её конфиденциальности, доступности и целостности в кибернетическом пространстве. Помимо этого Литва поднимает тему защиты персональных данных пользователей, телекоммуникационных сетей, информационных систем и инфраструктур, являющихся особенно важными для жизни общества, от нарушения безопасности и применения в отношении них кибератак. В стратегии Литвы также указываются мероприятия, целью которых является гарантирование полной безопасности деятельности в электронном пространстве.

Люксембургская Стратегия упирает на важность безопасности социума и экономики. В ней также выделяется значимость информационно-коммуникационных технологий для осуществления повышения уровня экономики и экономического роста отдельных граждан и общества в целом. У Стратегии существуют пять направлений: защита ключевой информационной инфраструктуры и своевременная реакция на инциденты безопасности; модернизация нормативно-правовой базы, государственное и международное сотрудничество; обучение и информирование; продвижение стандартов.

Интересна позиция Голландии – у неё присутствует стремление к безопасным и надёжным информационно-коммуникационным системам, так как она располагает опасениями серьёзных нарушений в них, и в то же время она признает важность наличия свободы и открытости Интернет-пространства. В стратегии даётся также определение кибербезопасности. “Кибербезопасность – это защищенность от сбоев и неправильной

эксплуатации информационно-телекоммуникационных систем. Сбои и неправильная эксплуатация может отрицательно повлиять на доступность и надежность информационно-телекоммуникационных систем, поставить под угрозу конфиденциальность и целостность информации, хранящейся в системах" [3].

Поводя итог, можно сделать следующие выводы.

1) На уровне отдельных стран-участниц ЕС развитие системы кибербезопасности идёт неравномерно, так как их стратегии делают упор на разные аспекты.

2) Тем не менее, общий уровень борьбы с киберпреступностью и обеспечения кибербезопасности растёт с каждым годом всё заметнее. Улучшается работа органов, созданных с этой целью (развитие обеспечения кибербезопасности в Европейском Союзе начало развиваться на должном уровне относительно недавно, с момента активной работы ENISA), система регулирования, создаются правовые источники, более чётко определяющие, что именно является угрозой кибербезопасности и как бороться с её нарушениями.

Список использованных источников

1. ИСО/МЭК 27032:2012 Руководящие указания по кибербезопасности (ISO/IEC 27032:2012 Informationtechnology – Securitytechniques – Guidelinesforcybersecurity)/ URL: Официальный сайт ИСО/МЭК https://www.iso.org/news/2012/10/Ref1667.html (дата обращения: 10.03.2017).

2. Безкоровайный М.М., Татузов А.Л. Кибербезопасность – подходык определению понятия/ URL: http://cyberleninka.ru/article/n/kiberbezopasnost-podhody-k-opredeleniyu-ponyatiya (дата обращения: 10.03.2017).

3. Государственные стратегии кибербезопасности/ URL: http://www.securitylab.ru/analytics/429498.php (дата обращения: 10.03.2017).

4. Вопросы и ответы: Директива об атаках на информационные системы/ URL: Официальный сайт Европейской Комиссии http://europa.eu/rapid/press-release_MEMO-13-661_en.htm (дата обращения: 10.03.2017).

Официальный сайт Европейского агентства по сетевой информационной безопасности/ URL: https://www.enisa.europa.eu/topics/standards/standards

УДК 341.1

МЕРЫ ПО БОРЬБЕ С МОНОПОЛИЕЙ В ЕВРОПЕЙСКОМ СОЮЗЕ

Айтжанов Султан Талгатович

AytzhanovSultanTalgatovich@gmail.com

Студент 3 курса специальности «Международное право» Юридического факультета ЕНУ им. Л.Н. Гумилёва, Астана, Казахстан.

Научный руководитель – М.Ж.Куликпаева

Данная статья описывает конкурентное право и стратегический режим в Европейском союзе (EU).Право о конкуренции ЕС, в общем и целом, последовательно применяется в государствах-членах и является эффективным механизмом осуществления относительно методов, которые затрагивают внутренний рынок, и способствует развитию единого рынка ЕС. На фоне многих других государств, конкурентное законодательство ЕС можно назвать одним из самых прогрессирующих, так как существуют государства, не имеющие в своем распоряжении всеобъемлющий закон о конкуренции, не говоря о его систематическом применении.

1.Закон о конкуренции и политика в ЕС

Закон о конкуренции, который прописан в Договоре о Функционировании Европейского Союза (TFEU) направлен на ускорение интеграции рынка через нормативную базу с централизованными органами власти. Договор о Функционировании Европейского