Федеральное государственное автономное
образовательное учреждение
высшего образования
«СИБИРСКИЙ ФЕДЕРАЛЬНЫЙ УНИВЕРСИТЕТ»

Юридический институт

кафедра международного права

УТВЕРЖДАЮ
Заведующий кафедрой
_____ Т.Ю. Сидорова
подпись инициалы, фамилия
«____» _____ 2020 г.

БАКАЛАВРСКАЯ РАБОТА

41.03.05. Международные отношения
профиль подготовки 41.03.05.01 Международные отношения и внешняя политика

Европейские инициативы в области информационной безопасности

Руководитель	_____	доцент, к.филос.н	М.С. Бухтояров
	подпись, дата	должность, ученая степень	инициалы, фамилия
Выпускник	_____		Е.Е. Широбокова
	подпись, дата		инициалы, фамилия

Красноярск 2020

СОДЕРЖАНИЕ

ВВЕДЕНИЕ

В современном мире одним из ключевых ресурсов стала информация. Человечество столкнулось с внедрением в жизнь информационных технологий и массовой компьютеризацией. Ключевое место занимает и Интернет – всемирная система объединённых компьютерных сетей для хранения и передачи информации. Однако подключение любого устройства к глобальной сети снижает гарантию защиты информации.

Актуальность исследуемой темы состоит в том, что сегодня, в эпоху информационных технологий для государств очень остро стоит проблема информационной безопасности. Поскольку информационное пространство выходит за рамки одного государства, необходимо понимать, какие совместные меры принимают государства Европы, где особенно высока степень интеграции, для защиты своих интересов и интересов граждан. Страны Европы представляют особый интерес, поскольку неоднократно подвергались атакам в информационной среде, в связи с этим увеличивается роль европейских государств в законотворчестве в сфере информационных технологий. В Европе очень высоко ценят идеалы прав человека поэтому для этих государств очень важно найти нужный баланс между защитой интересов личности и обеспечением собственного национального интереса, при этом действуя в духе единой политики.

Объектом исследования данной работы является информационная безопасность.

Предметом исследования данной работы является сотрудничество государств в сфере защиты информации.

Целью работы является изучение действий европейских государств в области защиты информации, а также определить основные принципы политики европейских стран в этой области

Задачи: 1) Изучить понятие информационной безопасности и кибербезопасности.

2) Изучить угрозы информационной безопасности на разных исторических этапах.

3) Выявить основные черты защиты информации в европейских государствах на национальном уровне.

4) Проанализировать совместные действия европейских стран по обеспечению информационной безопасности и оценить их эффективность.

5) Выявить подход европейской политики к проблеме информационной безопасности.

Глава I.ПОНЯТИЕ И ИСТОРИЯ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ

1.1 Понятие информационной безопасности. Ее отличительные черты и особенности.

В современном мире ключевую роль играет понятие безопасности. Большинство государств считает своей главной задачей обеспечение безопасности практически во всех жизненных процессах. Само понятие безопасности очень обширно и охватывает такие компоненты, как наличие и взаимодействие внешних факторов, минимально необходимых для благополучного существования и прогрессивного развития объекта безопасности; совокупность отдельных свойств самого объекта, отражающих его способность активно функционировать в указанных выше условиях, а также сохранять собственную целостность и восстанавливать жизнедеятельность при реализации опасностей и угроз[1].

Приоритетной задачей является обеспечение безопасности во всех сферах жизни: экономической, политической, социальной и др. Наряду с ними остро стоит вопрос обеспечения безопасности в информационной сфере, поскольку в современном мире технологии развиваются настолько быстро, что контролировать этот процесс становится все труднее. Поэтому основной задачей становится оперативное реагирование на вызовы современности и эффективность принимаемых мер.

Говоря о безопасности в информационной сфере, часто люди употребляют два понятия: «кибербезопасность» и «информационная безопасность». Хоть эти два понятия и относятся к одной сфере, назвать их полностью синонимичными нельзя, но в то же время они тесно связаны между собой.

[1] Мартиросян Т. А. К вопросу о содержании понятия “безопасность” [Электронный ресурс]. -Режим доступа: https://cyberleninka.ru/article/n/k-voprosu-o-soderzhanii-ponyatiya-bezopasnost (дата обращения 25.03.2020)

Согласно проекту Концепции кибербезопасности Российской Федерации, кибербезопасность – это совокупность условий, при которых составляющие киберпространства защищены от максимального числа угроз и нежелательных воздействий[2].

Если давать более точное определение кибербезопасности, то необходимо указать следующие пункты: кибербезопасность – раздел безопасности, изучающий процессы формирования, функционирования и эволюции киберобъектов, с целью выявления источников киберопасности, которые могут нанести им ущерб, и формирования законов и других нормативных актов, регламентирующих термины, требования, правила, рекомендации и методики, выполнение которых должно гарантировать защищенность киберобъектов от всех известных и изученных источников киберопасности. Таким образом, к понятию кибербезопасность относится исключительно цифровая среда, отсутствие угроз незаконного доступа к киберобъектам и нарушения их работы[3].

В статье А. С. Алпеева “Терминология безопасности: кибербезопасность, информационная безопасность” также даны определения понятиям киберобъект и киперпространство. К киберобъектам можно отнести любой объект, который работает при участии программируемых средств. В основе определения безопасности лежит также понятие киберпространства. Киберпространство – это сфера, образованная каналами связи между киберобъектами. Технологическая инфраструктура, обеспечивающая функционирование киберобъектов. Подводя небольшой итог, можно сказать, что к кибербезопасности относится отсутствие угроз функционированию электронных, связанных между собой устройств, а также создание правовой базы, регулирующей защиту этих процессов.

[2] Концепция стратегии кибербезопасности Российской Федерации [электронный ресурс]. - Режим доступа: http://www.council.gov.ru/media/files/41d4b3dfbdb25cea8a73.pdf (дата обращения 24.03.2020)
[3] Алпеев А. С. Терминология безопасности: кибербезопасность, информационная [электронный ресурс]. - Режим доступа:https://cyberleninka.ru/article/n/terminologiya-bezopasnosti-kiberbezopasnost-informatsionnaya-bezopasnost (дата обращения 24.03.202)

В Концепции информационной безопасности Российской Федерации дано следующее определение. Информационная безопасность - состояние защищенности личности, общества и государства от внутренних и внешних информационных угроз, при котором обеспечиваются реализация конституционных прав и свобод человека и гражданина, достойные качество и уровень жизни граждан, суверенитет, территориальная целостность и устойчивое социально-экономическое развитие Российской Федерации, оборона и безопасность государства[4].

В отличие от кибербезопасности, ИБ (информационная безопасность) имеет 3 уровня: безопасность личности, общества и государства. Информационная безопасность личности сводится к реализации прав человека на доступ к информации, к использованию информации для реализации, не запрещенной законом деятельности, защите информации, обеспечивающей личную безопасность. Безопасность общества представляет собой защиту общества от деструктивного воздействия информационных потоков. Информационная безопасность государства – обеспечение национального интереса государства, а также защита информационных ресурсов от несанкционированного доступа. То есть, информационная безопасность охватывает защиту самого контента от деструктивного воздействия извне и его искажение, а также свободный доступ индивидов к необходимой информации и защиту общества от негативного воздействия вредоносного контента[5].

Для более точного понимания информационной безопасности необходимо выяснить задачи средств информационной безопасности. Они указаны в Критериях, разработанных странами Европы (Information

[4] Указ Президента РФ от 5 декабря 2016 г. №646 “Об утверждении доктрины информационной безопасности Российской Федерации” [электронный ресурс]. - ГАРАНТ - Режим доступа: https://www.garant.ru/products/ipo/prime/doc/71456224/ (дата обращения 24.03.2020)

[5] Ильичев И. Е. Проблемы обеспечения информационной безопасности личности, общества и государства в современной России [электронный ресурс]. - Режим доступа: https://cyberleninka.ru/article/n/problemy-obespecheniya-informatsionnoy-bezopasnosti-lichnosti-obschestva-i-gosudarstva-v-sovremennoy-rossii (дата обращения 25.03.2020)

Technology Security Evaluation Criteria (ITSEC)). В основе всего лежат три критерия:

- обеспечение конфиденциальности (защита от несанкционированного доступа),
- обеспечение целостности (несанкционированные изменения, модификации, уничтожение),
- обеспечение доступности (поддержание работоспособности информационных систем)

Помимо этого в Европейских критериях выделены три уровня безопасности:

- базовая (случаи отдельных случайных атак, когда злоумышленник – физическое лицо),
- средняя (корпоративный злоумышленник),
- высокая (средства защиты способны преодолеть только злоумышленники с высоким уровнем квалификации, например государственная спецслужба).

Выделены также некоторые виды угроз в информационном пространстве. К ним относятся:

- перехват сообщений,
- несанкционированный доступ в компьютерную сеть,
- нарушение работы сети,
- использование вредоносного программного обеспечения,
- использование компьютерных сетей для дезинформации, запугивания и шантажа[6].

Стоит отметить, что все угрозы нацелены на нарушение следующих составляющих информации: целостность, доступность, конфиденциальность. Таким образом, все угрозы направлены на искажение или неправильное распространение самого контента, содержания, а значит именно владелец

[6] Information Technology Security Evaluation Criteria (ITSEC) [электронный ресурс]. - Режим доступа: https://www.sogis.eu/documents/itsec/ITSEC-JIL-V2-0-nov-98.pdf(дата обращения 27.03.202)

контента может определять, какие внешние условия несут опасность его информации, а какие нет.

Необходимо также упомянуть, что исходя из определений, кибербезопасность относится только к онлайн среде, в то время как информационная относится ко всем видам носителей и источников информации, а следовательно возникла информационная безопасность гораздо раньше. Несмотря на то, что понятие информационной безопасности гораздо шире кибербезопасности большинство нормативных актов, касаемые цифровой среды, имеют в названии слово кибербезопасность. Связать этот факт можно с тем, что сейчас с распространением IT-технологий, компьютеров и Интернета практически любая информация хранится на электронном носителе, поэтому кибербезопасность и сочетают с информационной, хотя, конечно, эти понятия немного различны.

На современном этапе для государств информация представляет собой не только главнейший ресурс, но и средство международного влияния. Информационная революция, благодаря своей трансграничности, сделала шире возможности отдельных индивидов в глобальном масштабе, тем самым бросив вызов суверенитету государств. Проблема информационной безопасности стала актуальной на наднациональном уровне, так как глобальное информационное пространство дало возможность свободно взаимодействовать различным акторам международных отношений.

Однако в каждом государстве свой подход к проблеме обеспечения безопасности, что затрудняет международное сотрудничество. В статье П. Шарикова и Н. Степановой рассмотрены подходы к пониманию информационной безопасности в США, Европе и России. Лидерами информационного прогресса стали США в конце XX века, когда администрация Б. Клинтона пыталась извлечь как можно больше выгоды из информационной сферы, усиливая над ней контроль. Усиление контроля требовала и администрация Дж. Буша младшего с целью борьбы с терроризмом. Политика Б. Обамы отличалась от предшественников, был

провозглашен принцип нейтральности сети, обеспечивавший равный доступ всех пользователей к информации, а государственный контроль ослабевает, безопасность информации обеспечивается безопасностью инфраструктуры. В 2018 году Дональд Трамп утверждает принцип соперничества в киберпространстве против стратегических противников, государств-изгоев и криминальных сетей в Стратегии кибербезопасности США и отменяет принцип нейтральности сети. По заявлению Д. Трампа во время предвыборной гонки проблемы, препятствующие развитию Америки, это постправда и фальшивые новости[7].

Подобные заявления и действия Трампа говорят об обеспокоенности Президента США состоянием как кибербезопасности, так и качеством и правдивостью контента, а следовательно и информационной безопасностью. Предпринимаются попытки поставить под контроль свободу распространения информации.

В странах Европы сложилась нормативно-правовая база, способная регулировать рыночные аспекты таким образом, чтобы принцип "сетевого нейтралитета" соблюдался практически повсеместно. В своих национальных доктринах страны ЕС уделяют больше внимания защите персональных интересов, чем государственных. Все стратегии затрагивают и безопасность инфраструктур и защиту от пропаганды и деструктивных новостей из-за рубежа. Определяются пределы государственного контроля и устанавливается ответственность провайдеров за сохранность персональных данных пользователя[8]. Можно сказать о том, что вектор политики информационной безопасности зависит от приоритетов и национального интереса государства. То есть, например, приоритетом для США в свое время являлась борьба с терроризмом, поэтому контроль над

[7] Шариков П., Степанова Н. Подходы США, ЕС и России к проблеме информационной политики [электронный ресурс]. - Режим доступа:https://cyberleninka.ru/article/n/podhody-ssha-es-i-rossii-k-probleme-informatsionnoy-politiki (дата обращения 27.03.2020)

[8] Шариков П., Степанова Н. Подходы США, ЕС и России к проблеме информационной политики [электронный ресурс]. - Режим доступа:https://cyberleninka.ru/article/n/podhody-ssha-es-i-rossii-k-probleme-informatsionnoy-politiki (дата обращения 27.03.2020)

информационным пространством был ужесточен. Вскоре он был ослаблен, но после снова усилен для борьбы с постправдой и фальшивыми новостями, по словам Дональда Трампа. То есть государство пытается оградить население от деструктивного воздействия информационных потоков на них. В Европе всегда идеалом считались права человека. А следовательно и политика европейских стран направлена больше на защиты интересов отдельной личности, конфиденциальность информации.

Подводя итог, можно сделать вывод, что понятия информационной безопасности и кибербезопасности не тождественны, но при этом тесно связаны. Главное их отличие заключается в среде их существования. Кибербезопасность относится лишь только к киберпространству, онлайн доступу и информации на электронных носителях, в то время как информационная безопасность относится и к офлайн среде. Угрозы кибербезопасности более направлены на нарушение работы устройств, получение доступа к информации, информационные угрозы более направлены на контент, его целостность и конфиденциальность. Однако в современном мире с развитием IT-технологий все больше информации переходит в онлайн среду, поэтому угрозы целостности и конфиденциальности информации становятся тесно связаны с киберугрозами. Именно поэтому нормативные акты, касаемые информации, имеют в названии понятие кибербезопасность, включая также информационную безопасность.

1.2 История информационной безопасности в Европе, методы защиты, методы воздействия

XXI век принято считать веком информации и информационных технологий, следовательно вопросы защиты информации обсуждаются сейчас очень широко. Однако для обладателя информацией всегда остро стоит вопрос о ее сохранности, целостности, поэтому проблемы информационной безопасности зародились гораздо раньше, чем принято считать.

Информационное противоборство возникло еще в Древнем мире, оно ограничивалось в основном вербальными каналами. Даже использование воинами в бою устрашающих масок, боевых кличей для сопровождения военных действий можно отнести к информационному воздействию на противника посредством вербальных каналов. Основной целью древних правителей было поднятие боевого духа своих воинов и деморализация соперника. Начало информационному противоборству положило осознание правителями древних государств эффективности ненасильственного управления массами людей.

Если говорить об информационных угрозах в более привычном понимании, то ими являлись дезинформация противника, получение секретной информации, а также распространение ложных слухов, опасных взглядов и порочащих сведений, выступление ораторов и проповедников с целью психологического воздействия. Классическим примером дезинформации может послужить троянский конь, благодаря которому грекам удалось захватить Трою во время Троянской войны. Распространением ложной информации также успешно пользовался Ганнибал. Во время подготовки к битве с римлянами при реке Треббин он активно распускал слухи о мощи нового оружия карфагенян, тем самым способствовал деморализации римской армии. Другой пример,

распространение слухов о появлении страшной болезни в рядах его войск, таким образом, усыпляя бдительность римлян.

Также в Древнем мире правителей и философов волновали не только способы воздействия на врагов, но и также возможность противостоять таким же действиям со стороны оппонента. Главной задачей была устойчивость населения своего государства к влиянию иностранных нравов. Например, Платон и Аристотель полагали, что сохранению государственного строя способствует воспитание в духе соответствующего строя. Населению внушались устойчивость и божественность существующих законов, а также суровые наказания свыше за неподчинение.

Таким образом, первые угрозы информационной безопасности зародились уже в Древнем мире. Они представляли собой устрашение и дезинформацию противника. Но, наряду с угрозами, возникают и методы противостояния им. В древности люди осознали силу воздействия информации на человеческое сознание, поэтому прибегали к инструментам внушения и пропаганды ценностей своего государства. Это помогало в большей степени овладеть разумом человека, дать ему приемлемую систему ценностей, заставить в нее верить и защищать. Но, поскольку научного обоснования всему этому не было, делалось это с помощью религии.

Новым этапом развития информационных угроз можно считать Средние века. В XV веке увеличение охвата аудитории обеспечивает изобретение книгопечатания. Поскольку мировоззрение в то время было религиозным, основным оружием воздействия была религиозная пропаганда. Философ Фома Аквинский полагал, что для укрепления своей власти и влияния Римской католической церкви необходим контроль за публицистикой. Именно для этого в Ватикане был учрежден специальный орган для борьбы с инакомыслием, Sacra Congregatio de Propaganda Fide, отсюда и происходит термин «пропаганда». Агрессивные военные походы, совершавшиеся с целью распространения христианства, обозначались

священными, а действия противника дискредитировались распространением слухов о совершаемых ими зверствах.

Инструмент дезинформации активно использовали в Средние века монгольские захватчики. Например, в 1241 во время монгольского вторжения в Венгрию. Заполучив случайно королевскую печать в качестве трофея, монгольским ханом Батыем было приказано написать письмо на венгерском языке от имени короля о прекращении сопротивления.

Нельзя сказать, что угрозы информации в Средние века кардинально отличались от угроз древности. Все так же использовалась дезинформация противника, идеалы государства также навязывались с помощью религии. Однако с появлением книгопечатания охват аудитории увеличился, информация стала гораздо доступнее. Поэтому чтобы не допустить ее деструктивного воздействия применялись более жесткие меры такие как: создание специального органа по борьбе с инакомыслием в Ватикане и расцвет инквизиции в Европе.

Значительным переменам информационная сфера подверглась в конце XIX – начале XX вв. В конце XIX в. Появляется телеграфная связь, которая выходит за рамки одной страны. 17 мая 1865 года в Париже был основан Международный телеграфный союз. Его задачами было разрешение технических, организационных и правовых вопросов, относящихся электросвязи. Это первая попытка государств установить общие правила и разработать нормы в информационном пространстве. Поскольку Международный телеграфный союз существует до сих пор (теперь это Международный союз электросвязи, специализированное учреждение в составе ООН), то можно сказать, что эта попытка была достаточно успешной.

Теперь основным источником информационных угроз становится пресса. В структурах средств массовой информации создаются отделы контрразведки и пропаганды, выстраивалось сотрудничество между газетами разных стран. Во время Первой мировой войны активно применялись инструменты психологического воздействия. Так, например, над немецкими

позициями и в тылу французы распространили до 29 млн. экземпляров листовок, т.е. примерно по 750 тыс. в месяц. Англичане распространяли до 1 млн. экз. листовок в месяц[9].

В 20-е и 30-е годы XX века активно развивается кинематограф. Информация постепенно приобретает визуализацию, что по сравнению с печатной прессой, оказывает еще большее психологическое давление.

В эти годы информационное противостояние в большей степени опирается на идеологию. Наиболее ярко это прослеживается в СССР и фашистской Германии. Впервые в мире создается министерство народного просвещения и пропаганды во главе с Йозефом Геббельсом. Под контролем министерства находились все виды СМИ и другие средства передачи информации: пресса, радиовещание, литература, музыка, кинематограф, театр, изобразительное искусство, коммерческая деятельность, туризм. Геббельсу удалось создать образ опасного, но очень уязвимого врага и сильного и уверенного Гитлера, заставить таким образом все слои населения почитать своего лидера. В основном, под угрозу попадали молодые люди с неокрепшей психикой и небольшим багажом знаний, которые легко поддавались внушению.

В Советском Союзе население воспитывалось в духе патриотизма. Также был создан Управление пропаганды и агитации при ЦК ВКП(б), занимавшийся ведением информационно-психологического воздействия. Одним из способов пропаганды в СССР были плакаты, возвышающие советский народ. Но в СССР также пытались противостоять нацистской пропаганде. Был введен запрет на распространение информации в виде газет и журналов, но помимо этого, блокировались также и немецкие радиостанции.

Таким образом, начиная с древнейших времен, люди осознали важность информации и ее воздействия на человеческое сознание. Основными борьбы инструментами были дезинформация и пропаганда.

[9] Панарин И., СМИ, пропаганда и информационные войны; Издательский дом - Поколение, Москва; 2012, с 59

Вторая мировая война доказала эффективность метода пропаганды. Она применялась как к гражданам государства-оппонента (распространение листовок, радиоволн), так и гражданам своего государства, пример тому деятельность Геббельса. Средства защиты также выходят на новый технический уровень (блокировка радиоволн).

В послевоенное время и во время Холодной войны бурно развивается телевидение и радиовещание, охват аудитории становится все больше и больше, а следовательно повышается воздействие СМИ на общество. В это время государства впервые принимают законодательные акты для борьбы с негативной информацией и снижения ее влияния на граждан. Так, например, в 1953 году в ФРГ принят закон о распространении произведений и медиа-контента, вредных для молодежи и в 1955 в Великобритании Закон о детях и молодежи.

В период Холодной войны, как известно, наблюдалось идеологическое противостояние между СССР и США. В США ключевую роль в осуществлении такой пропаганды играло учрежденное в 1953 г. Информационное агентство США, ЮСИА (United States Information Agency, USIA) в целях «изучения, информирования и оказания влияния на иностранную аудиторию в целях продвижения интересов США, а также расширения диалога американских граждан и институтов с их зарубежными контрагентами». Основными формами работы ЮСИА выступали: организация распространения информационной продукции и зарубежного вещания американских СМИ, включая радиостанцию «Голос Америки» (Voice of America), образовательные и культурные обмены, проведение выставок и конференций. Ключевым моментом явилось сотрудничество этого агентства с ЦРУ, что подтверждает использование правительством инструмента пропаганды для информационно-психологического воздействия на противника.

В 80-е годы XX популярность набирают ЭВМ и персональные компьютеры, что положило начало удаленному доступу к информации и

компьютерным сетям. Как следствие зарождаются новый вид преступности – компьютерная преступность и новые информационные угрозы, связанные с хищением или уничтожением данных. Уже появляются предпосылки киберугроз[10].

В современном мире информационная сфера приобретает системообразующий характер. Более 3 миллиардов человек имеет доступ в Интернет к информации различного характера, а следовательно теперь информация стала гораздо доступнее. Теперь возрастают не только масштабы угроз, но и уровень их опасности. Благодаря Интернету информационные угрозы приобретают трансграничный характер, что делает борьбу с ними на национальном уровне менее эффективной. Именно сейчас информационная безопасность начинает выделяться в отдельный вид безопасности со своей нормативной базой как на национальном так и наднациональном уровнях.

На современном этапе проблемы больше касаются угроз в цифровой сфере. Среди них:

- утечка информации,
- повреждение информации,
- повреждение системы хранения информации,
- нелегальное использование информационного носителя,
- хакерские атаки,
- вирусные программы,
- пираты,
- фальсификация информации,
- распространение фейковых новостей[11].

Таким образом, проблемы информационной безопасности существовали на протяжении всей истории человечества. От более

[10] Сулейманова Ш.С., Назарова Е.А., Информационные войны: история и современность: Учебное пособие. – М.: Международный издательский центр «Этносоциум», 2017 124 с.

[11] Тершуков Д. А., Анализ современных угроз информационной безопасности [электронный ресурс]. - Режим доступа: https://cyberleninka.ru/article/n/analiz-sovremennyh-ugroz-informatsionnoy-bezopasnosti (дата обращения 28.03.2020)

вербальных способов (устрашение, боевые кличи) угрозы трансформировались в дезинформацию и ее искажение, далее активную роль начали приобретать СМИ, их деятельность, пропаганда и распространение ложной информации. На сегодняшний момент информация в большинстве случаев существует в цифровой среде, поэтому ко всем видам угроз добавляется и угрозы цифровым сетям, хранящим информацию. С течением времени менялась сама информация, ее носители и способы распространения, вместе с ней трансформировались и сами угрозы. От противоборства в СМИ до проникновения в компьютерные сети. Исходя из этого, у государств появилась новая необходимость регулирования информационного пространства. Проблема безопасности информации все больше приобретает трансграничный характер и выходит за рамки одного государства, тем не менее, универсального подхода обеспечения безопасности нет. Каждое государство отдает приоритет определенным элемента безопасности в зависимости от приоритета своей внутренней политики и национальной безопасности

Глава II. ИНФОРМАЦИОННАЯ БЕЗОПАСНОСТЬ ЕВРОПЫ

2.1 Меры обеспечения информационной безопасности стран Европы на национальном уровне.

Как известно, страны Европы обладают достаточно высоким уровнем интеграции. Поскольку угрозы информационной безопасности уже давно приобрели трансграничный характер, то объединение стран, устранение этих угроз совместными усилиями, принятие общих законодательных актов, иными словами совместные инициативы, выглядят вполне логично. Однако все же каждое государство суверенно, а следовательно каждое преследует свой национальный интерес, у каждого государства свое видение и понимание проблем безопасности, а также свои ресурсы ее обеспечения.

На данный момент единственной страной, заявившей о своем выходе из Евросоюза является Великобритания. Однако ее информационной политике все же стоит уделить внимание, так как географически Великобритания все же относится к европейскому региону. Во-вторых после переходного периода, который длится до 31 декабря 2020 года Великобритания перестанет быть членом Европейского Совета по защите данных. Тем не менее Великобритания является членом других европейских организаций, например Совет Европы, Европол, и подписантом других общеевропейских документов, например, Конвенции 108 Совета Европы, которая сильно перекликается с принятым ЕС GDPR. Поэтому общий дух европейской политики в Великобритании сохранится.

По словам члена британского парламента, канцлера казначейства, Филиппа Хаммонда, Соединенное Королевство одна из ведущих цифровых держав, поэтому процветание страны зависит от способности государства защищаться от новых угроз[12].

[12] National Cyber Security Strategy 2016-2021 [электронный ресурс]. - Режим доступа: https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/567242/national_cyber_security_strategy_2016.pdf (дата обращения 11.04.2020)

Одним из документов, в котором упоминается защита информации является Security Policy Framework, описывающее стандарты и практики защиты людей, информации и инфраструктуры. В документе подчеркивается важность защиты информации, упомянуты защита конфиденциальности, целостности и доступность информации. То есть, упомянуты критерии, разработанные странами Европы в 1991 году (Information Technology Security Evaluation Criteria (ITSEC)). В приоритетах информационной политики указаны защита конфиденциальности персональных данных граждан и коммерческой информации, эффективное предоставление государственных услуг, надлежащая защита информации, связанной с национальной безопасностью, выполнение обязательств перед международными партнерами.

В 2019 была в Великобритании была принята Белая книга о вреде онлайн. В документе подчеркивается, что онлайн среда стала платформой распространения информации не только подрывающей значимость национальных ценностей, но и угрожающей безопасности обычных пользователей, в частности детей. Благодаря сети, растет пропаганда терроризма и криминальных ценностей. Согласно Белой книге целью Великобритании является сохранение свободного интернета, свободу выражения онлайн, безопасная среда, где компании смогут предпринимать активные шаги по обеспечению безопасности пользователей, выработка норм по регулированию активности, повышение уровня цифровой грамотности населения и международное сотрудничество. В документе установлено требование Duty of care, позволяющее компаниям устанавливать ответственность социальных медиа за информационный контент[13].

Комитет Палаты общин по цифровым технологиям, культуре, СМИ и спорту рекомендовал правительству отойти от определения «фейкньюс», а оперировать понятием «дезинформация». Данный шаг демонстрирует

[13] Closed consultation Online Harms White Paper Updated 12 February 2020, Department for Digital, Cultural, Media & Sport. [электронный ресурс]. - Режим доступа: https://www.gov.uk/government/consultations/online-harms-white-paper/online-harms-white-paper (дата обращения 13.04.2020)

обеспокоенность правительства состоянием информационной безопасности, поскольку фейкньюс – единичный случай недостоверной информации, который не обязательно связан с вмешательством иностранных государств, а дезинформация – политический термин, предполагающий иностранное вмешательство. Такое предложение было связано с обострением информационного противоборства Великобритании и Российской Федерации по делу Скрипалей[14].

Большое внимание в Великобритании уделяется кибербезопасности, поскольку большая часть информации в XXI веке находится в электронном виде, а следовательно защищая свое киберпространство, государство принимает меры по обеспечению и информационной безопасности.

В 2016 году была принята Национальная стратегия кибербезопасности до 2021 года. В стратегии отмечены приоритеты Великобритании в киберсфере: защита (эффективное реагирование на развитие киберугроз), сдерживание (пресечение враждебных действий), развитие (поддержка научных исследований в киберсфере). Отмечено также, что Великобритания готова к международному сотрудничеству в этой сфере и может выступить страной-спонсором для продвижения международных партнерских проектов стран НАТО и ЕС. Основными принципами концепции являются защита граждан и процветание государства, кибератаки сопоставимы с вооруженными атаками, Великобритания будет действовать согласно международному праву и от других акторов международных отношений ожидает того же. Также приоритетом для Великобритании является защита приватности граждан и распространения ее ценностей, таких как демократия, права человека, верховенство закона, открытость и подотчетность правительства.

В рамках стратегии был создан Национальный центр кибербезопасности. Но это не единственный орган, занимающийся

[14] Годованюк, Кира Анатольевна. Кибербезопасность и борьба с дезинформацией: опыт Великобритании [электронный ресурс]. - Режим доступа: https://cyberleninka.ru/article/n/kiberbezopasnost-i-borba-s-dezinformatsiey-opyt-velikobritanii (дата обращения 13.04.2020)

вопросами кибер- и информационной безопасности. Помимо этого, вопросами кибер- и информационной безопасности занимаются органы разведки Соединенного Королевства MI5 и MI6. Также в Великобритании функционирует Управление уполномоченного по делам информации (Information Commissioner's Office), независимый орган Великобритании, созданный для защиты прав на информацию в общественных интересах, содействия открытости государственных органов и конфиденциальности данных для частных лиц. В компетенцию органа входит рассмотрение жалоб о нарушении прав на информацию граждан или организаций, выработка пути решения проблемы и содействие в ее устранении, поощрение исследований в цифровой сфере, а также международное сотрудничество с европейскими партнерами, а также с такими органами как Европейская Комиссия и Европол.

Таким образом, Великобритания уделяет внимание проблемы содержания информации и ее вредное воздействие на население, а также техническую сторону вопроса, говоря о кибербезопасности. Неоднократно подчеркнуто стремление Великобритании к международному сотрудничеству в рамках международного права, что говорит об осознании государством трансграничного характера проблемы.

Не меньшую обеспокоенность безопасностью своих информационных систем выражает и Франция. В 2015 году была принята Национальная стратегия по безопасности в цифровой сфере. В стратегии отмечено, что безопасность информационного пространства в целом зависит от 3 сообществ: компании (предложение новых средств по предотвращению угроз), государственные органы (претворение в жизнь курса государства в информационных технологиях), сами пользователи (повышение уровня цифровой грамотности). Таким образом, можно сделать вывод, что национальная кибербезопасность зависит от каждого гражданина Франции.

Главной целью Франции является создание платформы для роста компаний, процветание экономики и сохранение приватности пользователей[15].

Как и в Великобритании во Франции функционируют специальные органы, обеспечивающие безопасность в цифровом пространстве: Генеральная дирекция внешней безопасности (DGSE), Управление военной разведки (DRM), Управление военной контрразведки (DPSD) – аналоги британских MI5 и MI6. Данные структуры подотчетны Министерству обороны Франции, но также функционирует и открытая ассоциация физических и юридических лиц CLUSIF (Club de la securite informatique francaise), занимающаяся разработкой стратегических направлений политики по обеспечению национальной безопасности.

Согласно стратегии Франция поставила перед собой задачи развития международного сотрудничества (двусторонние и многосторонние связи), повышение уровня доверия государств в киберпространстве, становление Франции в роли главного проводника цифровой автономии Европы. По оценке Ф. Дельрю (Институт стратегических исследований при парижской Военной школе, *IRSEM*) и О. Жери (Кафедра по киберстратегии им. Кастекса при Институте высших исследований национальной обороны, *IHEDN*) Франция рассчитывает выступать одним из главных гарантов мира и безопасности в киберсреде, способна предложить собственный целостный взгляд. При этом для страны важно сохранение цифрового суверенитета и защита национальных сетей[16].

Конечно же, помимо технической области, не осталась без внимания проблема содержания. Связано это в большей степени с распространением контента экстремистского характера, оказывающего пагубное воздействие на население, а также с проблемой информационных войн. В 2018 был принят закон о Фейкньюс. Поводом для принятия закона стал конфликт Bloomberg и

[15] French National Digital Security Strategy [электронный ресурс]. - Режим доступа: https://www.enisa.europa.eu/topics/national-cyber-security-strategies/ncss-map/France_Cyber_Security_Strategy.pdf\ (дата обращения 11.04.2020)

[16] Чихачев, Алексей. Франция: киберреспублика на марше [электронный ресурс]. - Режим доступа: https://russiancouncil.ru/analytics-and-comments/analytics/frantsiya-kiberrespublika-na-marshe/ (дата обращения 14.04.2020)

компании Vinci. В результате публикации недостоверной информации, акции компании Vinci упали. Но также этот закон позволяет кандидатам во время выборных кампаний подавать жалобы о распространении заведомо ложной информации о себе, а государству — блокировать занимающиеся этим СМИ. В данной ситуации очень важно найти баланс между свободным доступом к достоверной информации и ужесточением цензуры. На рассмотрении также находился законопроект о разжигании ненависти в Интернете.

Подводя небольшой итог, можно сказать, что Франция, как и Великобритания, заботится и о безопасности пользователей, и национальном интересе, о технической и содержательной стороне вопроса. Франция также выражает свою приверженность международному праву и стремление к международному сотрудничеству. При этом Франция, как и Великобритания, готова взять лидерство в сотрудничестве на себя.

Немного по-другому обстоят дела в Германии. Впервые в мире в 1970 году закон о защите персональных данных был принят в Германии в земле Гессен. Все административные единицы Германии (все 16 земель) имеют свои собственные законы о защите данных.

Документом, который регулирует информационную сферу и распространяется на все земли, является Национальная стратегия кибербезопасности. В стратегии обозначены основные принципы: доступность, целостность, конфиденциальность и аутентичность информации. Конечно, были созданы и специальные органы по обеспечению кибербезопасности: Национальный центр киберреагирования (National Cyber Response Center), Совет национальной кибербезопасности (National Cyber Security Council), Федеральный офис информационной безопасности Министерства внутренних дел (Bundesamt für Sicherheit in der Informationstechnik, BSI). Последний стал ответственным органом всей

страны. Также подчеркивается стремление к международному сотрудничеству на полях ООН, НАТО, ЕС, ОБСЕ[17].

Главным минусом этого документа является его устарелость. Данная стратегия была принята в 2011 году. За 10 лет технологии усовершенствовались, появились новые вызовы, угрозы модифицировались, однако документ, определяющий основную политику государства не изменился. Поэтому по оценке немецких экспертов, Германия не может соразмерно ответить всем вызовам современности. Во время предвыборной кампании 2015 года Август Ханнинг, бывший глава Федеральной разведывательной службы заявил, что нет достаточной защиты серверов Бундестага, где хранится конфиденциальная информация[18].

Помимо кибербезопасности обострена также и ситуация с содержанием, а именно с фейковыми новостями. По словам канцлера ФРГ Ангелы Меркель, фейкньюс – это одна из угроз безопасности государства. Меркель также подчеркнула особую роль Федеральной разведывательной службы, потому что дезинформация – это целенаправленная государственная пропаганда.[19] Однако по мнению Марселя Йона, капитана-резервиста ВМФ Германии и президента немецкого Совета по кибербезопасности Ханс-Вильгельма Дюнна, Германия не готова к отражению кибератак и попыток манипулирования общественным сознанием[20]. Эксперты подчеркивают, что психологический аспект манипулирования сознанием гораздо важнее технической стороны вопроса, но из-за неповоротливости государственного механизма и неспособности оперативно реагировать на происходящее, Германии тяжело бороться с вызовами в киберпространстве.

---

[17] Cyber Security Strategy for Germany [электронный ресурс]. - Режим доступа:https://www.enisa.europa.eu/media/news-items/german-cyber-security-strategy-2011-1 (дата обращения 11.04.2020)

[18] Анализ-Кибератаки, утечки, фейковые новости: страхи Германии перед парламентскими выборами [электронный ресурс]. - Режим доступа: https://forbes.kz/news/2017/05/12/newsid_144030 (дата обращения 13.04.2020)

[19] Меркель назвала фейковые новости угрозой безопасности Германии [электронный ресурс]. - Режим доступа: https://iz.ru/843586/2019-02-08/merkel-nazvala-feikovye-novosti-ugrozoi-bezopasnosti-germanii (дата обращения 29.03.2020)

[20] Германия абсолютно не готова к отражению кибератак - немецкие эксперты [электронный ресурс]. - Режим доступа: https://eadaily.com/ru/news/2019/05/09/germaniya-absolyutno-ne-gotova-k-otrazheniyu-kiberatak-nemeckie-eksperty (дата обоащения 29.03.2020)

Таким образом, несмотря на высокий уровень интеграции в Европе и высокий уровень развития стран, ситуация по защите информационной безопасности на национальном уровне разная. Такой вывод можно сделать, рассмотрев ситуацию в трех ведущих европейских государствах: Великобритании, Франции и Германии. Можно сказать, что все страны действительно обеспокоены технической и содержательной стороной вопроса, во внимание берется как защита государства в целом, так и интересы отдельной личности. Это первая общая черта политики информационной безопасности в Европе. Второй чертой информационной политики в европейских странах является законодательная база, отвечающая принципам прав человека, а также вовлечение органов иностранных дел, обороны и разведки в вопросы информационной безопасности. Третье, важным вопросом является также недопущение манипулирования общественным сознанием своих граждан, распространения фейковых новостей, дезинформации. Одной из целью политики безопасности также является сотрудничество на международном уровне. При этом не во всех странах законодательная база отвечает вызовам современности, из-за чего заметна неспособность оперативного реагирования на проблемы. Этим всем характеризуется общий дух политики стран Европы в области информационной безопасности. При этом такие страны, как Великобритания и Франция готовы не только к сотрудничеству, но и к тому, чтобы взять на себя лидерство в данном вопросе.

2.2 Меры обеспечения информационной безопасности стран Европы на наднациональном уровне.

Защита информационной безопасности в Европе не ограничивается только национальным уровнем защиты. Государства всегда выражали готовность и стремление к сотрудничеству.

Еще в начале XXI века одной из платформ по сближению государств по данной проблеме стал Совет Европы. В 2001 году была подписана Будапештская конвенция о киберпреступности. Главной идеей документа является сближение национальных уголовно-правовых и уголовно-процессуальных норм в области защиты информации, а также авторского и гражданского права. Помимо этого упоминается международное сотрудничество, направленное на собирание улик. Текст Конвенции базируется на основных принципах международного права: защита прав человека, сотрудничество и добросовестное исполнение обязательств.

В Конвенции впервые представлена классификация преступлений в IT-среде. К ним относятся несанкционированный доступ в IT-среду, нелегальный перехват IT -ресурсов, вмешательство в компьютерную систему и информацию, содержащуюся на носителях данных. Регулируются также правила расследования преступлений в киберпространстве.

Однако у документа есть и недостатки. Была предпринята попытка обязать Интернет-провайдеров записывать данные трафика в режиме реального времени, а также хранить данные клиентов. Фактически, это нарушение принципа конфиденциальности, что противоречит принципам в основе конвенции[21].

Несмотря на это к Конвенции присоединились 38 стран-членов Совета Европы, а также США, Канада, Япония и ЮАР. Россия, член Совета Европы, отказалась подписывать данный документ. По словам директора департамента МИД РФ по вопросам новых вызовов и угроз Ильи Рогачева

[21] Волеводз, А.Г. Конвенция о киберпреступности: новации правового регулирования / А.Г. Волеводз // Правовые вопросы связи. – 2007 – № 2 – С. 17-25.

Конвенция имеет ряд недостатков. Один из них п. 2 ст. 32 о трансграничном доступе к компьютерным системам других государств без уведомления их правительств, что противоречит принципам целостности суверенитета государства. Россия была и не готова до сих пор дать разрешение на доступ к своим сетям путем подписания этой Конвенции. Не смотря на это, данную инициативу в целом можно считать удачной, поскольку это первый документ подобного рода, которому удалось выйти за рамки Совета Европы и распространиться на несколько других развитых государств[22].

Подписанием Конвенций история защиты информации в Европе не ограничивается. В 2004 году было основано Европейское агентство по сетевой и информационной безопасности (ENISA), независимое агентство ЕС по кибербезопасности. Главной целью агентства является развитие сетевой и информационной культуры во благо граждан, пользователей, бизнеса и организациям государственного сектора, способствуя развитию внутреннего рынка.

С течением времени атаки на системы развивались, а сами информационные сети, экономика и общество становились более уязвимыми. Именно поэтому появилась необходимость в совершенствовании законодательств и технических оснащений. Это главная задача агентства – помощь в создании условий быстрого реагирования, эффективных и скоординированных ответов на вызовы современности и компетентное управление кризисом на уровне ЕС, а также обеспечение взаимопомощи государств и регулярная оценка уровня состояния государственной кибербезопасности. Каждый год организация публикует доклады о состоянии кибербезопасности, руководства к новым способам отражения атак и рекомендации к применению новых средств усиления безопасности.

В марте 2019 года на заседании Европарламента было принято решение об укреплении позиций Агентства путем предоставления агентству постоянного мандата, укрепления его финансовых и человеческих ресурсов и

[22] Российский дипломат назвал Будапештскую конвенцию по киберпреступлениям устаревшей [электронный ресурс]. - Режим доступа: https://tass.ru/politika/4782506 (дата обращения 30.03.2020)

в целом повышения его роли в поддержке ЕС в достижении общей и высокого уровня кибербезопасности. Этот факт подтверждает важность работы ENISA для ЕС.

В данный момент агентство готовится к проведению масштабного мероприятия по тестированию систем безопасности в июне 2020 года. Эксперты центра предрекают развитие киберкризиса после пандемии COVID-19. Цель теста – проверка компьютерных систем в условиях пандемии, а также их способность ответить угрозам, с которыми они столкнутся после мирового кризиса из-за коронавируса. Задачи исследования: построение доверия, повышение осведомленности, проверка реакции на возникающие проблемы. Поскольку кризис связан со здравоохранением, то помимо властей и самого агентства, отвечающих за кибербезопасность, будут протестированы министерства здравоохранения, медицинские организации, медицинское оборудование и электронные услуги, оказываемые медицинскими центрами. В качестве угроз будут рассмотрены распространение вредоносных программ, хищение информации, утечка медицинских данных, инсайдерские атаки, мошенничество через Wi-Fi. Это еще раз доказывает эффективную работу организации, способную отвечать вызовам современности.

Еще одной европейской организацией, занимающейся преступлениями в цифровом пространстве является Европол, Европейская организация уголовной полиции. Европол реализует все принятые ранее правовые и технические достижения на практике, координирует деятельность национальных полиций. В мае 2019 года под контролем Европола, при участии Федеральной криминальной полиции Германии, различных правительственных учреждений США (Управление по борьбе с наркотиками, Федеральное бюро расследований…), финской таможни (Тулли) и французской Национальной полицией закрыла рынок на Уолл-стрит, крупную платформу продажи наркотиков в даркнете. Европол поддержал скоординированный подход правоохранительных органов по всей Европе, и

США были ключом к успеху этих двух расследований. Исполнительный директор Европола Кэтрин де Болле прокомментировала: «это расследование показывает важность сотрудничества правоохранительных органов на международном уровне и демонстрирует, что незаконная деятельность в темной паутине не так анонимна, как могут думать преступники»[23]. Европолу отводится более практическая сторона вопроса, а именно координация уголовных органов, разработка инструментов, тактики и методов проведения расследований. Причем в данном контексте речь идет не только о кибербезопасности (блокировка сайтов даркнета), но и именно информационной безопасности (распространение вредоносной информации о наркотиках).

В 2018 страны Европейского Союза перешли к новому Общему регламенту по защите данных (General Data Protection Regulation – GDPR). Согласно статье 5 GDPR основаны на 6 принципах:

- Принцип законности, честности и обзорности данных. Пользователи имеют право быть в курсе, кто и зачем собирают о них данных, и как планируют с ними распоряжаться.
- Данные пользователей собираются для конкретных и ясных целей. Если первоначальная цель сбора данных изменилась, это считается нарушением прав пользователей.
- Минимальный набор данных.
- Принцип точности. Данные должны быть точными и обновленными.
- Ограничение по хранению. Хранить данные не следует дольше, чем это необходимо.
- Защита данных от несанкционированного доступа.

[23] Double Blow to Dark Web Marketplaces // Europol Press Release, 3.05.2019 [электронный ресурс]. - Режим доступа: https://www.europol.europa.eu/newsroom/news/double-blow-to-dark-web-marketplaces (дата обращения 30.03.2020)

В дополнение к этому документ обязывает компании своевременно уведомлять пользователей, если произошла кража их данных. Особое внимание уделяется защите данных детей и родительский контроль.

Но основным достижением GDPR можно назвать его экстерриториальный принцип. Документ защищает права всех граждан ЕС и применяется ко всем компаниям, которые занимаются обработкой данных пользователей независимо от их места нахождения[24].

GDPR можно назвать прорывом европейских стран в защите персональных данных своих граждан. Здесь отражается и общий дух прав человека. Это доказывает обязанность компаний защищать данные, не хранить их дольше, чем нужно, предоставлять информацию только владельцу по его запросу и передавать данные пользователей только с согласия пользователей. А также экстерриториальный принцип позволяет защищать данные пользователей не только внутри ЕС, но и также за его пределами.

Ранее было упомянуто, что Великобритания и Франция готовы не только к расширению и укреплению международного сотрудничества, но и к лидерству в данном вопросе. В 2018 году на форуме ЮНЕСКО Франция продемонстрировала свое стремление. В ноябре был опубликован текст Парижского призыва к доверию в киберпространстве. В очередной раз подчеркнуто, что киберпространство является не только пространством возможностей, но и угроз, как для частного сектора, так и для объектов инфраструктур. Упомянута важность международного права, Устава ООН, международного гуманитарного права и применение их норм при использовании технологий. Закреплена защита прав личности в онлайн-пространстве. Основными положениями призыва являются:

1. предотвращать злонамеренную кибердеятельность, которая угрожает отдельным лицам или критическим инфраструктурам

[24] General Data Protection Regulation // Regulation (EU) 2016/679 Of The European Parliament And Of The Council 27 April 2016, [электронный ресурс]. - Режим доступа: https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32016R0679 (дата обращения 31.03.2020)

или наносит им значительный неизбирательный или системный вред, и устранять её;

2. предотвращать преднамеренные действия, которые значительным образом подрывают доступность и целостность центрального Интернета;
3. развивать наши возможности по предотвращению вмешательства со стороны иностранных субъектов, направленного на дестабилизацию избирательных процессов посредством злонамеренной кибердеятельности;
4. предотвращать хищение интеллектуальной собственности с помощью ИКТ, в частности, промышленных секретов и другой конфиденциальной коммерческой информации, с целью получить конкурентные преимущества для предприятий или для какого-либо коммерческого сектора;
5. разрабатывать средства для предотвращения распространения вредоносных инструментов и компьютерных методов;
6. усилить безопасность цифровых процессов, продуктов и услуг в течение всего срока эксплуатации и на протяжении всей цепочки снабжения;
7. поддерживать действия, направленные на развитие продвинутой компьютерной гигиены для всех участников;
8. принимать меры, чтобы помешать негосударственным субъектам, в том числе из частного сектора, предпринимать агрессивные кибердействия в ответ на нападение на них, будь то для себя лично или для других негосударственных субъектов;
9. содействовать широкому принятию и внедрению международных норм ответственного поведения, а также мер по усилению доверия в киберпространстве[25].

[25] Парижский призыв к доверию и безопасности в киберпространстве [электронный ресурс]. - Режим доступа: /https://www.diplomatie.gouv.fr/IMG/pdf/appel_de_paris_en_russe_cle8a41ae.pdf (дата обращения 31.03.2020)

К документу присоединились 51 государство, 50 международных и региональных организаций, более 170 частных компаний и корпораций. По сообщению Департамента информации и печати МИД России основной посыл данного документа – необходимость обеспечить мир и безопасность в глобальной информационной среде – соответствует духу российских подходов к обеспечению МИБ, закрепленных в наших ключевых инициативах по данной проблематике, которые недавно были одобрены Первым и Третьим комитетами 73-й сессии ГА ООН. Однако в документе есть и свои минусы, а именно предложение взять за основу Будапештскую Конвенцию 2001 года. По оценке РФ данная конвенция в значительной степени устарела и не отвечает вызовам современного времени. По словам директора департамента МИД РФ по вопросам новых вызовов и угроз Ильи Рогачева в 1997-2001 годах (когда разрабатывалась конвенция) преступления в информационной сфере были довольно примитивными, в то время не существовало таких проблем, как современные бот-сети или повсеместная спамерская деятельность[26].

Тем не менее, Парижский призыв все-таки в большей степени нацелен на техническую сторону вопроса, в отличие от Новозеландского Крайстчерчского призыва к действию по искоренению террористического и насильственного экстремистского контента в Интернете. В 2019 году в Новой Зеландии произошел теракт, во время которого террористу удавалось вести онлайн-трансляцию массового убийства через приложение Facebook Live. Видео распространилось на такие платформы как YouTube, Instagram, Twitter, где было доступно несколько часов. Поэтому 15 мая на форуме в Париже по инициативе Новой Зеландии и Франции был представлен Крайстчерчский призыв, к которому присоединились Великобритания, Япония, Австралия, Канада, Франция, Германия, Индонезия, Индия, Ирландия, Италия, Иордания, Нидерланды, Новая Зеландия, Норвегия, Сенегал, Испания, Швеция), Еврокомиссия и восемь

[26] Российский дипломат назвал Будапештскую конвенцию по киберпреступлениям устаревшей [электронный ресурс]. - Режим доступа:https://tass.ru/politika/4782506 (дата обращения 31.03.2020)

технологических компаний (Amazon, Daily Motion, Facebook, Google, Microsoft, Qwant, Twitter, YouTube. Теперь членами призыва являются 48 государств, Совет Европы, Еврокомиссия и частные компании. Призыв представляет собой план по предотвращению превращения Интернета в инструмент терроризма. Ведь известно, что террористы используют Интернет для распространения своих ценностей, привлекать людей, трансляция в Новой Зеландии стала поводом к принятию новых мер.

Призыв представляет собой договор государственного сектора и частных компаний о разделении полномочий и ответственности по блокировке экстремистского контента. Например, государство берет на себя ответственность за повышение медийной грамотности, разработка правовых норм и стандартов освещения террористических действий в СМИ. В компетенцию компаний входит блокировка неприемлемого экстремистского контента, немедленное удаление, предоставление отчетов. А также от интернет-провайдеров требуется разработка технических решений, сотрудничество с правоохранительными органами во время расследований интернет-преступлений, создать условия, позволяющие органам, правительствам и поставщикам услуг оперативно реагировать на распространение террористического контента.

Несмотря на общий дух документа к нему не присоединились США, Россия и Китай. Официально Россия не прокомментировала свой отказ от присоединения, а Вашингтон сослался на принципы свободы слова, но в целом поддержал идею документа, заявив также, что в Соединенных штатах борьба с распространением террористического контента тоже идет, но другими методами[27].

В 2018 году Генеральная ассамблея ООН приняла российский проект резолюции о противодействии использования ИКТ в преступных целях. Как

[27] Толстухина, Анастасия Борьба глобальных технологических компаний с террористическим контентом в Интернете [электронный ресурс]. - Режим доступа: https://russiancouncil.ru/analytics-and-comments/analytics/borba-globalnykh-tekhnologicheskikh-kompaniy-s-terroristicheskim-kontentom-v-internete/ (дата обращения 1.04.2020)

известно, существует 2 видения проблемы: американский (предоставление полной свободы в Интернете и приверженность принципам свободы слова, а также заявления о важности Будапештской конвенции 2001 года) и российский (закрепляющий цифровой суверенитет государства в киберпространстве). Российский вариант резолюции может заменить Будапештскую Конвенцию 2001 года, причем положение о трансграничном доступе спецслужб к хранящимся данным без уведомления другой стороны исключено. В то время как представители американского варианта считали, что новые меры, закрепляющие права государства не нужны, ведь есть Будапештская конвенция. Европейские государства в этом вопросе выступили на стороне американского варианта, но тем не менее ГА ООН приняла российский вариант.

Говоря об эффективности европейских инициатив можно говорить о том, что несмотря на некоторые недостатки меры достаточно эффективны. Это подтверждает присоединение к Конвенции Совета Европы, Парижскому и Крайстчерчскому призывам стран за пределами региона. Принятие GDPR, которые защищают граждан ЕС не только внутри Союза, но и за его пределами. А также деятельность Европола, которая демонстрирует раскрытие преступлений в информационной сфере на деле.

Проанализировав состояние информационной безопасности в Европе, можно сделать вывод, что региональным лидером в этой сфере является Франция, поскольку государство принимает все необходимые меры на национальном уровне и выдвигает собственные международные инициативы. По словам Макрона, он не является сторонником ни российского, ни американского варианта и это отражено в его Парижском призыве, а количество подписантов говорит о согласии с французской инициативой. Поэтому можно сказать, что призыв Макрона выражает общую европейскую идею. По своей сути Парижский и Крайстчерчский призывы полностью не следуют принципам ни американского, ни российского варианта, но все же некоторые положения о роли и ответственности государств в

информационном пространстве говорят о том, что государства Европы не готовы полностью провозгласить свободу в Интернете и возложить ответственность полностью на частный сектор, однако и усиливать контроль государства Европа тоже не хочет. В Крайтчерчском призыве, можно сказать, оформилась европейская идея безопасности информации – совместная ответственность государства и частных компаний за техническую и содержательную сторону вопроса, или иными словами государственно-частное партнерство.

ЗАКЛЮЧЕНИЕ

Угрозы информации существовали всегда, с древнейших времен до настоящего времени. Однако с течением времени они, конечно же, изменялись с развитием информационных технологий. В свое время информационное противостояние случалось в печатных изданиях, радиоволнах, телевидении и компьютерных сетях. Угрозы прошли путь от устрашающих боевых кличей времен Александра Македонского до распространения печатных пропагандистских листовок, от блокировок радиоволн до незаконного проникновения в компьютерные сети.

В связи с этим различается две стороны вопроса: техническая (сохранность систем, их способность противостоять незаконному доступу) и содержательная (сохранность информации, защита от искажения, хищения, дезинформация и пропаганда ценностей, способных пагубно влиять на сознание граждан). По этому признаку различаются понятия кибербезопасности и информационной безопасности. Однако в XXI веке с развитием и доступностью Интернета, увеличением числа пользователей ПК практически любая информация хранится на электронном носителе, а следовательно кибербезопасность и информационная безопасность тесно переплелись. Из-за этого многие документы, в названии которых упоминается кибербезопасность посвящены также и содержательной стороне вопроса.

Государства в первую очередь принимают меры защиты на национальном уровне, при этом в каждом национальном документе подчеркивается важность международного сотрудничества, следования принципам международного права, добросовестное исполнение взятых на себя обязательств. Связано это со всемирной паутиной, благодаря которой, угрозы информации приобрели трансграничный характер.

Государства Европы обладают самым высоким уровнем интеграции в мире. Они уже давно проводят единые финансовую, экономическую, торговую, миграционную политики и многие другие. В стороне не осталась и проблема информационной безопасности. Если говорить о национальном уровне, то информационная политика государств все-таки находится на разных уровнях. Например в ФРГ, одном из развитых государств ЕС, до сих пор действует стратегия 2011 года, в то время как Великобритания и Франция разработали пятилетние планы до 2021 и выражают готовность взять лидерство в международном сотрудничестве на себя. В каждом государстве существуют специально созданные органы по борьбе с кибер- и информационными угрозами, и все они подотчетны министерствам обороны, министерствам иностранных дел и органам разведки.

Европейские инициативы берут свое начало в 2001 с принятием Будапештской Конвенции и в 2004 с созданием ENISA. Несмотря на некоторые несовершенства Конвенции, она вышла за рамки Совета Европы, до сих пор в призывах государств она упоминается, как основной документ в цифровой сфере. Европейское агентство анализирует действия государств, публикует отчеты, рекомендации к действиям, анализ новых угроз, которые совершенствуются с каждым годом. А также еще одна европейская организация Европол координирует действия по раскрытию преступлений в информационной сфере. Таким образом Европа тщательно занимается вопросом сближения государств, унификации законодательных мер, координации их действий и взаимопомощи.

Тем не менее границами Европы их инициативы не ограничиваются. Это подтверждают два призыва Франции: Парижский и Крайстчерчский. Один посвящен предотвращению киберугроз, другой распространению экстремистского контента. К документам присоединились страны за пределами европейского континента. Эти призывы демонстрируют общий европейский взгляд на проблему: в основе всего – соблюдение международного права, приверженность принципам прав человека, но в то

же время Европа не готова полностью передать контроль над информационным пространством частному сектору, провайдерам. Государства и IT-компании в равной степени ответственны за устранение информационных угроз. Это демонстрирует небольшую схожесть европейского и российского видения проблемы.

Таким образом, Европейские государства, благодаря высокому уровню развития и интеграции, предлагают миру свое видение IT-проблем. Отличительной чертой Европы является баланс между государственными интересами и интересами частных лиц. Следование всем принципам права, способность защитить данные граждан, не допустить влияния на сознание своих граждан, но при этом не отказываться от государственного контроля.

Список использованных источников

1. Camino Mortera-Martinez, Game Over? Europe's Cyber Problem [Электронный ресурс] / Camino Mortera-Martinez // Centre for European Reforms, 08 July 2018. – Режим доступа https://www.cer.eu/publications/archive/policy-brief/2018/game-over-europes-cyber-problem
2. Camino Mortera-Martinez, Big Data, Big Brother? How to Secure Europeans' Safety and Privacy [Электронный ресурс] / Camino Mortera-Martinez // Centre for European Reforms, 04 December 2015. – Режим доступа https://www.cer.eu/publications/archive/policy-brief/2015/big-data-big-brother-how-secure-europeans-safety-and-privacy
3. Camino Mortera-Martinez, Europe's Cyber Problem [Электронный ресурс] / Camino Mortera-Martinez // Centre for European Reforms, 22 March 2020. – Режим доступа https://www.cer.eu/publications/archive/bulletin-article/2018/europes-cyber-problem
4. Closed consultation Online Harms White Paper Updated 12 February 2020 [Электронный ресурс]: Department for Digital, Cultural, Media & Sport. – Режим доступа https://www.gov.uk/government/consultations/online-harms-white-paper/online-harms-white-paper
5. Cyber Security Strategy for Germany Электронный ресурс]: European Union Agency for Cyber Security (ENISA) . – Режим доступа https://www.enisa.europa.eu/media/news-items/german-cyber-security-strategy-2011-1
6. Directive (EU) 2016/1148 of the European Parliament and of the Council [Электронный ресурс] 6 July 2016. – Режим доступа https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32016L1148&from=EN

7. Double Blow to Dark Web Marketplaces [Электронный ресурс] // Europol Press Release, 3.05.2019. – Режим доступа https://www.europol.europa.eu/newsroom/news/double-blow-to-dark-web-marketplaces
8. French National Digital Security Strategy [Электронный ресурс]: European Union Agency for Cyber Security (ENISA) . – Режим доступа https://www.enisa.europa.eu/topics/national-cyber-security-strategies/ncss-map/France_Cyber_Security_Strategy.pdf\
9. General Data Protection Regulation [Электронный ресурс]: Regulation (EU) 2016/679 Of The European Parliament And Of The Council 27 April 2016. – Режим доступа: https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32016R0679
10. Information Technology Security Evaluation Criteria (ITSEC) [Электронный ресурс]: ITSEC Joint International Library (ITSEC JIL), Version 2.0, November 1998 – Режим доступа https://www.sogis.eu/documents/itsec/ITSEC-JIL-V2-0-nov-98.pdf
11. Jake Olcott Cybersecurity Vs. Information Security: Is There A Difference [Электронный ресурс] / Jake Olcott // BitSight The Standard Ratings, 15 September 2019. – Режим доступа https://www.bitsight.com/blog/cybersecurity-vs-information-security
12. Jesse Lichtenstein, Digital Diplomacy [Электронный ресурс] / Jesse Lichtenstein // The New York Times Magazine, 16 July 2010. – Режим доступа https://www.nytimes.com/2010/07/18/magazine/18web2-0-t.html
13. National Cyber Security Strategy 2016-2021 [Электронный ресурс]: HM Government. – Режим доступа https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/567242/national_cyber_security_strategy_2016.pdf
14. Алпеев, А. С. Терминология безопасности: кибербезопасность, информационная безопасность [Электронный ресурс] /А. С. Алпеев // Вопросы кибербезопасности - №5(8) - 2014. – Режим доступа

https://cyberleninka.ru/article/n/terminologiya-bezopasnosti-kiberbezopasnost-informatsionnaya-bezopasnost

15. Анализ-Кибератаки, утечки, фейковые новости: страхи Германии перед парламентскими выборами [Электронный ресурс] // Forbes, 12.05.2017. – Режим доступа https://forbes.kz/news/2017/05/12/newsid_144030
16. Волеводз, А.Г. Конвенция о киберпреступности: новации правового регулирования / А.Г. Волеводз // Правовые вопросы связи. – 2007 – № 2 – С. 17-25.
17. Годованюк, Кира Анатольевна. Кибербезопасность и борьба с дезинформацией: опыт Великобритании [Электронный ресурс] / Годованюк, К. А. // Научно-аналитический Вестник Института Европы РАН, 2019. – Режим доступа https://cyberleninka.ru/article/n/kiberbezopasnost-i-borba-s-dezinformatsiey-opyt-velikobritanii
18. Ильичев, И. Е. Проблемы обеспечения информационной безопасности личности, общества и государства в современной России [Электронный ресурс] / Ильичев, И. Е //Проблемы правоохранительной деятельности - № 2, 2015. – Режим доступа https://cyberleninka.ru/article/n/problemy-obespecheniya-informatsionnoy-bezopasnosti-lichnosti-obschestva-i-gosudarstva-v-sovremennoy-rossii
19. Казарин Олег Викторович, Тарасов Александр Алексеевич, Современные концепции кибербезопасности ведущих зарубежных государств [Электронный ресурс] / Казарин, О. В. Тарасов, А. А. // История и архивы, 2013. – Режим доступа https://cyberleninka.ru/article/n/sovremennye-kontseptsii-kiberbezopasnosti-veduschih-zarubezhnyh-gosudarstv-1
20. Концепция стратегии кибербезопасности Российской Федерации [Электронный ресурс]: Официальный сайт Совета Федерации РФ. – Режим доступа http://www.council.gov.ru/media/files/41d4b3dfbdb25cea8a73.pdf

21. Мартиросян, Т. А. К вопросу о содержании понятия “безопасность” [Электронный ресурс] / Мартиросян, Т. А. // Стратегия гражданской защиты: проблемы и исследования. 2013. – Режим доступа https://cyberleninka.ru/article/n/k-voprosu-o-soderzhanii-ponyatiya-bezopasnost
22. Мелисса Хатауэй, Киберготовность Германии 2.0 Национальная стратегия [Электронный ресурс]: Digital.Report, 15.05.2017.- Режим доступа https://digital.report/kibergotovnost-germanii-2-0-natsionalnaya-strategiya/
23. Мелисса Хатауэй, Киберготовность Франции 2.0 Национальная стратегия [Электронный ресурс]: Digital.Report, 15.05.2017.- Режим доступа https://digital.report/kibergotovnost-frantsii-2-0-natsionalnaya-strategiya/
24. Меркель назвала фейковые новости угрозой безопасности Германии [Электронный ресурс] // Известия, 8.02.2019. – Режим доступа https://iz.ru/843586/2019-02-08/merkel-nazvala-feikovye-novosti-ugrozoi-bezopasnosti-germanii
25. Об итогах голосования в Генассамблее ООН по российскому проекту резолюции по противодействию киберпреступности [Электронный ресурс] // Министерство иностранных дел Российской Федерации, 30.12.2019. – Режим доступа https://www.mid.ru/main_en/-/asset_publisher/G51iJnfMMNKX/content/id/3988579
26. Парижский призыв к доверию и безопасности в киберпространстве [Электронный ресурс] // Дипломатия Франции, Министерство Европы и иностранных дел, 12.11.2018. – Режим доступа https://www.diplomatie.gouv.fr/IMG/pdf/appel_de_paris_en_russe_cle8a41ae.pdf
27. Почему Россия не присоединилась к плану Макрона по регулированию в Сети [Электронный ресурс] // РБК, 12.11.2018. – Режим доступа

https://www.rbc.ru/technology_and_media/12/11/2018/5be9a3029a794731248739ab

28. Российский дипломат назвал Будапештскую конвенцию по киберпреступлениям устаревшей [Электронный ресурс] // ТАСС, 4.12.2017. – Режим доступа https://tass.ru/politika/4782506
29. Сулейманова Ш.С., Назарова Е.А., Информационные войны: история и современность /Сулейманова Ш.С., Назарова Е.А.// Учебное пособие. – М.: Международный издательский центр «Этносоциум», 2017 124 с.
30. Стадник, Илона. Россия и США: два разных взгляда на кибербезопасность [Электронный ресурс] / Стадник, И.// Российский совет по международным делам, 13.11.2018. – Режим доступа https://russiancouncil.ru/analytics-and-comments/analytics/rossiya-i-ssha-dva-raznykh-vzglyada-na-kiberbezopasnost/
31. Толстухина, Анастасия Борьба глобальных технологических компаний с террористическим контентом в Интернете [Электронный ресурс] / Толстухина, А. // Российский совет по международным делам, 24.03.202. – Режим доступа https://russiancouncil.ru/analytics-and-comments/analytics/borba-globalnykh-tekhnologicheskikh-kompaniy-s-terroristicheskim-kontentom-v-internete/
32. Туликов, А.В. Обеспечение информационной безопасности как гарантия прав человека / Туликов, А.В // Право. Журнал Высшей школы экономики № 2 С. 50–60, 2015.
33. Указ Президента РФ от 5 декабря 2016 г. №646 “Об утверждении доктрины информационной безопасности Российской Федерации” [Электронный ресурс]: Правовая система «Гарант». – Режим доступа https://www.garant.ru/products/ipo/prime/doc/71456224/
34. Фалеев, Михаил Иванович, Сардановский Сергей Юрьевич. Вопросы кибербезопасности в современной государственной политике в области национальной безопасности [Электронный ресурс] / Фалеев, М. И.

Сардановский С. Ю. // Технологии гражданской безопасности, 2016. – Режим доступа https://cyberleninka.ru/article/n/voprosy-kiberbezopasnosti-v-sovremennoy-gosudarstvennoy-politike-v-oblasti-natsionalnoy-bezopasnosti

35. Шариков, П., Степанова, Н. Подходы США, ЕС и России к проблеме информационной политики [Электронный ресурс] / Шариков, П., Степанова, Н. // Современная Европа, 201, №, с. -8, 2019. – Режим доступа https://cyberleninka.ru/article/n/podhody-ssha-es-i-rossii-k-probleme-informatsionnoy-politiki

36. Чихачев, Алексей. Франция: киберреспублика на марше [Электронный ресурс] / Чихачев, А.// Российский совет по международным делам, 11.12.2019. – Режим доступа https://russiancouncil.ru/analytics-and-comments/analytics/frantsiya-kiberrespublika-na-marshe/

Федеральное государственное автономное
образовательное учреждение
высшего образования
«СИБИРСКИЙ ФЕДЕРАЛЬНЫЙ УНИВЕРСИТЕТ»

Юридический институт

кафедра международного права

УТВЕРЖДАЮ
Заведующий кафедрой
_____ Т.Ю. Сидорова
подпись инициалы, фамилия
«01» 06 2020 г.

БАКАЛАВРСКАЯ РАБОТА

41.03.05. Международные отношения
профиль подготовки 41.03.05.01 Международные отношения и внешняя политика

Европейские инициативы в области информационной безопасности

Руководитель _____ 1.06.2020 доцент, к.филос.н М.С. Бухтояров
подпись, дата должность, ученая степень инициалы, фамилия

Выпускник _____ 29.05.20 Е.Е. Широбокова
подпись, дата инициалы, фамилия

Красноярск 2020