ВОПРОСЫ ОБЕСПЕЧЕНИЯ БЕЗОПАСНОСТИ СМИ

https://doi.org/10.5281/zenodo.10557607

Эргашева Ф

Факультет «экономики, политики и туризма восточных стран»
Кафедра политики стран востока и международных отношений

Аннотация:*Вопросы обеспечения информационной безопасности государства неразрывно связаны с политическими, экономическими и правовыми гарантиями реализации свободы слова и самовыражения в международном информационном пространстве. В современных политико-правовых условиях одинаково опасны и неприемлемы проявления цензуры и злоупотребления свободой СМИ, самоизоляция и экстремизм, предвзятость и безразличие к событиям, происходящим в международной системе.*

Abstarct. *Issues of ensuring the information security of the state are inextricably linked with political, economic and legal guarantees for the implementation of freedom of speech and self-expression in the international information space. In modern political and legal conditions, manifestations of censorship and abuse of freedom of the media, self-isolation and extremism, bias and indifference regarding the events that occur in the international system are equally dangerous and unacceptable.*

Ключевые слова: *Информация, инфраструктура, медиабезопасность, медиакоммуникация, медиаресурсы, мультимедийная культура.*

Key words: *Information, infrastructure, media security, media communication, media resources, multimedia culture.*

ВВЕДЕНИЕ

Увеличение количества тех национальных интересов, для которых безопасность информационной сферы жизни имеет особое значение, в целом соответствует парадигме постиндустриальной общественной формации. Национальная информационная безопасность становится комплексным институтом государственной политики, что существенно усложняет административные процедуры защиты конкретных интересов при производстве и распространении информационных сообщений.

Субъекты информационной безопасности в зависимости от собственных навыков определяют тот или иной аспект национальной системы информационной безопасности, особая значимость которого для них непосредственно определяется теми сегментами, которые представляют информационную деятельность, безопасность, за которую несут ответственность отдельные стороны.

При этом информационная безопасность обеспечивается в сфере компьютерных технологий, в средствах массовой информации и сетях общественной связи, в архивном и библиотечном деле, закрытых информационных системах [1].

Информационный суверенитет государства предполагает не только верховенство и независимость государственной власти в формировании и реализации информационной политики, но и предполагает активное участие органов власти и институтов гражданского общества в глобальной конкуренции на международном рынке средств массовой информации.

В результате активной проникновения компьютерных технологий в социально-культурные процессы современное общество фактически в рамках системы обеспечения информационной безопасности сформировало три относительно самостоятельных института: медиабезопасность, информационные технологии безопасности, защиту информации от несанкционированного доступа и утечки. Эти основные элементы института информационной безопасности нормативно объединяются в стратегические объединения национальных интересов в информационной сфере.

Информационная безопасность — это во многом техническая проблема, решаемая техническими методами; безопасность информационных технологий определяется наличием информационных систем и технологий в современном мире и зависит от уровня экономического развития и качества образования населения, в свою очередь медиабезопасность, как и информационная безопасность в сфере средств массовой информации, является важнейшим компонентом эффективной государственной политики в медиасфере *(рис.1.).*

Чем выше уровень информатизации социальных процессов, тем выше риски и шире спектр угроз информационной безопасности с точки зрения утечки информации и несанкционированного доступа к ней. качество и производительность труда [2].

Субъекты, участвующие в предоставлении услуг информационной сети (абоненты, поставщики услуг, поставщики контента, сетевые поставщики, поставщики технологий, электронные или мобильные платежные системы) влияют на эффективность системы информационной безопасности. Каждый из этих участников имеет доступ к сетевому терминалу и, следовательно, представляет собой потенциальную угрозу безопасности.

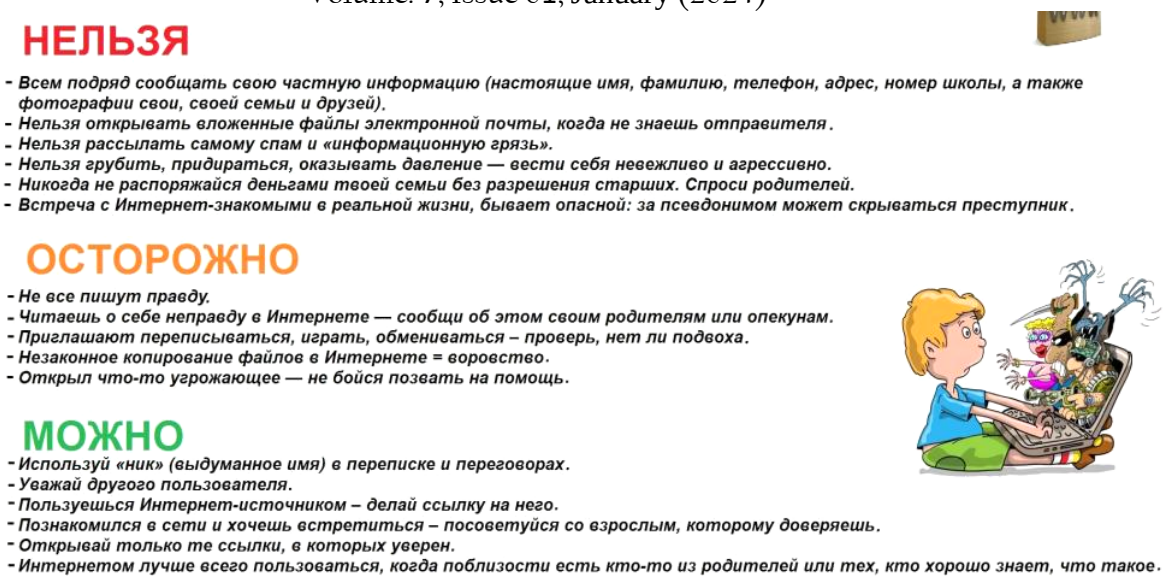

Рис.1. Интернет. Территория безопасности.

Все исследование безопасности требует сбора данных из всех источников угроз. Кроме того, различные принципы доступа к сети (проводная, беспроводная, с поддержкой 3G) создают множество точек доступа, которые могут быть использованы для несанкционированного доступа и неправильного использования. Внешняя угроза безопасности требует обмена данными между всеми субъектами сетевого оборудования. Учитывая политику безопасности транснациональных корпораций, которая учитывается в предоставляемых услугах социальных сетей, могут существовать специфические различия, которые затрудняют взаимодействие между ними [3].

Допустимая степень активности по защите своих интересов в сфере компьютерной безопасности в последние годы стала одной из наиболее спорных тем, поднимаемых в рамках научной дискуссии по вопросу способов обеспечения информационной безопасности в современных социальных сетях. Отсутствие понимания принципиальных различий между вредоносным и средствами активной защиты и блокировки вредоносного контента создает трудности в разработке универсального подхода к информационной безопасности.

За последние 30 лет международный Интернет превратился из академической информационной системы в глобальное средство массовой коммуникации, имеющее жизненно важное значение для глобальной торговли и политики, основанное на принципах открытости и обмена данными, которые имеют первостепенное значение для существования глобальной сети как оно существует сегодня.

Стратегическая идея медиабезопасности, как информационной безопасности в сфере массовых коммуникаций, формируется на основе алгоритмов решения тех практических задач, с которыми государственные учреждения сталкиваются в современных информационных коммуникационных сетях общего пользования. Угрозой безопасности страны в информационной сфере стало отставание политико-

правовых институтов государства от темпов развития глобальных коммуникационных систем, что обусловливает расширение спектра угроз информационной безопасности интересам отдельных лиц в различных сферах. сферах народного хозяйства страны.

Традиционные административные алгоритмы и регламенты, направленные на обеспечения национальной безопасности работа в информационной сфере недостаточно эффективна. Интенсивность развития информационных систем и технологий требует гибкой и адаптивной системы медиакоммуникаций, ключевым свойством которой является способность к саморегуляции и самовосстановлению.

Прозрачность государственных границ в системе международной связи, технологическая простота и удобство выполнения действий внутри элементов глобальной сети связи, расположенных в районах, географически удаленных от абонента сети, не всегда позволяют соблюдать традиционные законы и формальности. в современной системе массовых коммуникаций.

Краеугольным и не до конца решенным вопросом обеспечения информационной безопасности является правовая подсудность общественных отношений в системах социотехнических коммуникаций. Отсутствие универсального понимания подсудности в киберпространстве существенно усложняет понимание места и времени актов медиакоммуникаций всеми участниками международного общения и субъектами процесса в частности.

Изначально многие сетевые администраторы использовали принцип территориальной привязки интернет-коммуникаций к местоположению терминала. Посредством которых распространяется информация так физически подход используется для защиты государственных границ и способствует реализации соответствующие технологии управления коммуникациями. Однако такой подход, проникая с уровня национальной безопасности в корпоративную культуру, становится все более деструктивной тенденцией по отношению к единству глобальной сети и негативно влияет на популярность корпоративных ресурсов.

Скорость обработки информации в условиях возрастающей конкуренции становится одним из ключевых показателей безопасности информационной системы.

В процессе развития глобальной сети электронные устройства становятся все более распространенными и важными для нашей социальной и экономической жизни.

Торговля, новостные медиа-ресурсы и мультимедийная культура. Обеспечение целостности киберпространства зависит от комплекса технических, экономических, правовые меры, отражающие политику расширения возможностей человека посредством внедрения информационных технологий.

Основными участниками создания норм поведения в глобальной компьютерной сети являются частные корпорации, контролирующие предоставление телекоммуникационных услуг. В то же время широкое использование компьютерных технологий влияет на поведение пользователей технических систем. Методы и

средства информационной безопасности призваны обеспечить безопасность личных данных и конфиденциальность, но узнать чужие тайны зачастую оказываются сильнее любых мер безопасности.

Медиакорпорации, благодаря своему участию в процессах разработки программного обеспечения, получают практически неограниченный доступ ко всему контенту глобальной сети, создают административные угрозы, связанные с рисками злоупотребления правами, полученными вследствие технологического превосходства.

Системы технологической защиты информации получили весьма ограниченное распространение не только из-за своей ненадежности и высокой затрат на постоянную модернизацию, но и из-за их неудобства для пользователей, связанные с постоянными рисками дополнительных расходов из-за утраты оперативный доступ к системам хранения и обработки информации.

С одной стороны, меры защиты информации должны использовать самые передовые технологические разработки, имеющие существенное значение.

Стоимость и негативно влияют на конкурентоспособность продукции предприятия; с другой стороны, технологическая сложность систем информационной безопасности негативно влияет на скорость доступа к актуальной информации.

Канадский профессор Университета Онтарио Стефан Марш отмечает, что в большинстве сфер национальной экономики обеспечить информационную безопасность при сохранении ее социально-экономической целесообразности возможно только в той мере, в какой это соответствует уровню образования и культуры пользователей социальных сетей. Информационная безопасность в таких условиях приобретает значение некой благоприятной парадигмы, к которой следует стремиться, но обеспечить ее в полном объеме крайне сложно из-за комплекса технических и социальных ограничений [4].

Проблемы неизбежны в сложном техническом оснащении; выявлен ряд угроз и со стороны человеческого фактора: пользователи могут иметь недостаток веры, понимания, терпения по отношению к мерам безопасности, которые существуют в компьютерах.

Многие зарубежные эксперты в области информатики считают, что системы безопасность сетей социальных коммуникаций и других информационных ресурсов не ориентированы на потребности и возможности пользователей и подчинены логике некий образный дух безопасности, продиктованный техническими алгоритмами.

В процессе реализации политики, направленной на усложнение систем безопасности в ходе своеобразной гонки в сфере кибербезопасности, возникают риски потери доверия к технологическому прогрессу как фактору благотворно влияя на качество жизни и доступность социальных благ для каждого человека без какой-либо дискриминации.

ЗАКЛЮЧЕНИЕ

Сложный этап эволюции информационных систем связан с угрозой снижения интереса к материалам информационных сетей на фоне расширяющегося спектра потенциальные угрозы интересам абонентов. На наш взгляд, современные вызовы информационная безопасность связаны не только с увеличением количества кибератак, но они также связаны с новыми технологиями социальной инженерии, накладываемыми поверх обычных вредоносных программ.

Система социальных угроз в информационной сфере развивается гораздо быстрее, чем формирование политико-правовых институтов противодействия возникающим опасностям. Расширенные механизмы безопасности, более совершенные пароли, более сложные процедуры входа в систему и ряд других технических решений безопасности не отвечают интересам обычных пользователей компьютеров.

ИСПОЛЬЗОВАННЫЕ ЛИТЕРАТУРЫ:

1. Кириленко В. П., Алексеев Г. В. Международное право и информационная безопасность государств: монография. СПб. : СПб ГИКиТ, 2016

2. Kiountouzis E. A., Kokolakis S. A. Information systems security: facing the information society of the 21st century. London : Chapman & Hall, Ltd., 2008.

3. Marsh S., Basu A., Dwyer N. Security enhancement with foreground trust, comfort, and ten commandments for real people / Theories and Intricacies of Information Security Problems.
Potsdam : Universitätsverlag, 2013. P. 1–7.

4. Pipkin D. Information security: Protecting the global enterprise. New York : Hewlett-Packard Company, 2000.