СЕТЕВАЯ ФОРМА КОММУНИКАЦИИ КАК АСПЕКТ РАЗВИТИЯ ИНФОРМАЦИОННЫХ УГРОЗ

РЫЖИКОВ Михаил Сергеевич
преподаватель
ГБПОУ «Миасский геологоразведочный колледж»
г. Миасс, Россия

Одним из наиболее опасных источников угроз для людей является использование его же персональных данных против него.

Ключевые слова: угрозы, коммуникация, сетевая форма коммуникации, персональные данные, источник угроз, перегрузка личности, IT технологии.

Наиболее опасными источниками угроз можно считать манипулирование сознанием человека посредством формирования вокруг него среды с измененным «более правильным» мнением, что приводит его к неизбежному следованию за новыми идеалами. Так же к отрицательным остаткам можно отнести информационную перегрузку личности. Если вкратце это происходит из-за возникновения у человека интернет-зависимости, вследствие чего человек начинает ощущать дефицит новой информации, межличностного общения и прочих видов потребностей, которые он никак не может утолить. В свою очередь это приводит к обесцениванию устоявшихся норм и правил привычной жизни.

Одним из наиболее опасных источников угроз для людей является использование его же персональных данных против него. Инструментарий социальных сетей позволяет с легкостью надавить на нужные рычаги и выставить любое лицо в необходимом свете.

Сетевые коммуникации и сейчас обладают огромным инструментарием и предоставляют большие возможности для СМИ. В современном обществе большинство СМИ начало работать «на два фронта». Они комбинируют традиционные и современные медиа с целью привлечения большей аудитории. Посему в интернет-среде появляется такое огромное количество «Веб порталов» и Интернет-магазинов. Современное сетевое информационное пространство характеризуется медиа глобализацией. Их называют «новыми электронными медиа», для того чтобы отрезать их от привычных всем традиционным медиа: печати, радио, телевидения [7].

Новые электронные медиа обладают почти безграничными возможностями передачи любой информации любым ее отправителем в различных направлениях, но медийные информационные потоки формируются в интересах владельцев транснациональных информационных агентств. Процесс монополизации на медиарынке приводит к угрозам манипулирования общественным мнением по отношению к тем или другим значимым событиям и, что еще более серьезно, к деформации моральных устоев общества, его национальной культуры путем навязывания ему чужих ценностей. Разумеется, сетевые коммуникации сами по себе являются просто эффективной технологией для успешного развития бизнеса владельцев транснациональных информационных агентств.

Одной из самых распространенных групп угроз в современном обществе, можно без зазрения совести назвать киберпреступления. Они нацелены в основе своей на мошеннические махинации с использованием современных сетевых систем. Так же они служат для отмывания денег, полученных преступным путем, неправомерного использования финансовой, банковской информации и т. п.

Нет никаких сомнений, что социальные сети – это единственное место, хозяева которого если не напрямую нарушают установленные законом предписания, то занимают нейтральную позицию в правовом секторе. Это наглядно можно увидеть если обратить свое внимание на проблему авторских прав. На сегодняшний день в социальных сетях находится огромное количество пиратского и не нелицензионного контента, из-за которого обладатели прав интеллектуальной соб-

ственности находятся в не уделе. Однако только на этом противоречия между правом и сетевыми коммуникациями никак не останавливаются.

По данным аналитиков, число опасных Интернет-ресурсов за последнее время увеличилось в три раза. Эксперты по Интернет-безопасности утверждают, что сегодня атаки на ресурсы Всемирной паутины происходят каждые четыре с половиной минуты. Во многих странах отмечается увеличение объемов утечки данных, при этом только около 20% происходит из-за хакерских атак. По данным МВД, в 1 квартале 2021 г. Количество IT-преступлений выросло на 83,9%, а удельный вес таких деяний достиг 19,9% от общего числа. В основном из-за этого фактора уровень преступности в стране в целом вырос на 4% [1].

А в нынышнее время в России за период с января по октябрь 2022 г. сократилось количество преступлений, которые были совершены с использованием IT-технологий, на 5,6 процента.

По данным ведомства, за девять месяцев 2022 г. было зарегистрировано 429,2 тысячи преступлений, совершенных в сфере компьютерной информации [7].

Во Всемирной паутине сегодня существуют различного рода закрытые сети. Сетевые структуры эффективно используются организациями в условиях конспирации. Их главным козырем становится молниеносность распространения информации и новые возможности дистанционного управления террористическими актами. Террористические группы и мафиозные структуры используют нелегальные, полулегальные и криминальные методы политической борьбы, игнорируя правовые нормы и традиции, нарушая законы, расшатывая политический строй обществ.

Бесспорно опасный источник угроз в условиях сетевой коммуникации – это непрерывно разрастающееся влияние информационных войн и распространение информации, напрямую влияющее на сознание и мировоззрение людей. Информационные войны идут на всех уровнях и механизмы их работы практически всегда идентичны. У тех людей кто её ведут, остаются одни и те же рычаги давления на общественное мнение. Кто-то недосказывает часть информации и намеренно вызывает её дефицит, чем и подогревает внимание общественности. Кто-то в свою очередь наоборот давит на неудовлетворённость людей конкретной ситуацией или продуктом и заставляет активно противостоять и оппонировать ей. Существуют также методы ведения информационной войны на территории информационной среды противника с целью полной дезинформации и создания хаоса и паники посредством методов и технологий дающих воздействовать на информационную среду. Илья Леонидович Морозов различает три вида информационно-психологического оружия относительно стратегии нападения:

1. Системы дистанционного искажения или уничтожения информации: компьютерные вирусы общего и специализированного назначения (программы, проникающие извне и разрушающие систему); логические бомбы, тайно внедряемые в компьютер на этапе заводской сборки, которые при активизации парализуют работу компьютера.

2. Системы хищения информации: электронные шпионы (программы, проникающие извне и производящие незаметный для пользователя сбор служебной и непосредственно личной информации).

3. Системы комплексного воздействия на психику пользователя: мультимедийные сайты в виде информационно развлекательных или аналитических страниц с «горячей», «сенсационной» информацией.

Существует мнение, что повышение уровня «прозрачности» и доступности информации для всех участников политического процесса (например, в случае проведения президентских и парламентских выборов) облегчает общественный контроль за ним со стороны общественности. Однако И.Л. Морозов выделяет два блока угроз, ведущих к подрыву политических режимов: системные и периферийные угрозы [3].

Первый тип угроз направлен на дестабилизацию конкретных политических систем или их сегментов со стороны враждующего государства и затрагивает в основе своей атаки на информационное поле оппонента с использованием информационно-психологических атак

властных и околовластных структур

Не менее серьезную опасность представляют угрозы второго типа, которые связаны с деятельностью широкого спектра внесистемных сил – от международных террористических организаций до всевозможных хакерских групп. Неструктурируемость и непрогнозируемое возникновение периферийных информационных угроз крайне затрудняют выработку действенной защиты от них.

Ирина Алексеевна Василенко, анализируя состав политических факторов, различает их на носителей власти и внесистемную оппозицию. Сетевые пользователи, составляющие внесистемную оппозицию, делятся им на две группы – легальное «самобытное сопротивление», которое находит себе опору в традиционных и нетрадиционных ценностях сообщества, и на нелегальные криминально-мафиозные сети. Основной силой легального и нелегального сопротивления является исключительно сетевая, децентрализованная форма организации и политических действий [1]. Характерным примером такого сопротивления становится стремительно нарастающее движение антиглобалистов, которое строится на основе национальных и международных сетей, активно используется Интернет, и при этом сети не только обеспечивают организацию их деятельности, но и совместное использование информации [6].

Децентрализованный, неуловимый характер сетевых структур сопротивления антиглобалистов и других самобытных движений (экологисты, «зеленые», женские движения, различные молодежные субкультуры, представленные, в частности, в блогосфере) во многом затрудняет их восприятие и идентификацию со стороны государственного управления. «Новые гибкие сетевые структуры внесистемной оппозиции становятся сегодня главным козырем в борьбе с неповоротливыми институтами политической власти, которая в большинстве случаев имеет старую иерархическую организацию и только отдельные силовые подразделения в ней перестроены по сетевому принципу» [4].

В конечном итоге мы выделили основные категории информационных угроз, оказывающих свое влияние на общество, государство, личность посредством сетевых коммуникаций:

1. Угрозы безопасности личности, связанные с манипуляцией над сознанием и информационной перегрузкой человека, с непосредственным увеличением в информационную зависимость. Сюда же можно отнести и использования личных данных во вред личности, как пример сбор личных данных с целью внедрения таргетированной рекламы конкретному человеку.

2. Угрозы, связанные с управлением и манипуляцией над общественным мнением, появлением особых механизмов управления массы людей с целью организации процессов направленных на разрушение привычных ценностей общества.

3. Угрозы безопасности всех структур, на которые пытаются повлиять посредством международной преступности и терроризма.

4. Угрозы стабильности существующих режимов власти, обусловленные неконтролируемыми всплесками высказывания и активизации опасной оппозиции в социальной и сетевой коммуникации.

ЛИТЕРАТУРА

1. *Василенко И.А.* Политическая философия: Учебное пособие. – М.: Гардарики, 2019. – 239 с.
2. *Кулагина Я.М., Тарасова И.Ю.* Влияние интернета на современную молодежь // Актуальные вопросы общественных наук: социология, политология, философия, история: сб. ст. по матер. XXXV междунар. науч.-практ. конф. № 3(35) /. – Новосибирск: СибАК, 2018. – С. 37-43.
3. *Морозов И.Л.* Информационная безопасность политической системы // Политические исследования. – 2018. – № 5. – С. 134-144.
4. *Пелипенко А.А.* Интернет как феномен эволюции культуры // Власть. – 2019. – Том. 23. – № 1. – С. 164-169.
5. *Раянов М.Р.* Формирование интернет-культуры будущего учителя. – Самара, 2018. – 204 с.
6. *Южанинова Э.Р.* Интернет как новое пространство самореализации молодёжи / // Вестник ОГУ. – 2019. – С. 82-89.
7. URL: https://russian.rt.com/russia/news/1078022-prestuplenie-rossiya-internet.

THE NETWORKED FORM OF COMMUNICATION AS AN ASPECT OF THE DEVELOPMENT OF INFORMATION THREATS

RYZHIKOV Michael Sergeyevich
teacher
Miass Geological Exploration College
Miass, Russia

One of the most dangerous sources of threats to people is the use of his personal data against him.
Key words: threats, communication, network form of communication, personal data, source of threats, personality overload, IT technology.