Fledu.uz
foreign language education

Scientific-methodological electronic journal
"Foreign Languages in Uzbekistan", 2020, No 1(30), 146–157
https://journal.fledu.uz
ISSN: 2181-8215 (online)

ВИДЫ ИНФОРМАЦИОННО-ПСИХОЛОГИЧЕСКИХ УГРОЗ В СОЦИАЛЬНЫХ СЕТЯХ (НА ПРИМЕРЕ УЗБЕКИСТАНА)

Наргис Суннат кизи КОСИМОВА
Кандидат филологических наук, доцент
Узбекский государственный университет мировых языков, Ташкент, Узбекистан

ИЖТИМОИЙ ТАРМОҚЛАРДА АХБОРОТ-ПСИХОЛОГИК ТАҲДИДЛАРНИНГ ТУРЛАРИ (ЎЗБЕКИСТОН МИСОЛИДА)

Наргис Суннат қизи КОСИМОВА
Филология фанлари номзоди, доцент
Ўзбекистон давлат жаҳон тиллари университети, Тошкент, Ўзбекистон

TYPES OF INFORMATIONAL AND PSYCHOLOGICAL THREATS IN SOCIAL NETWORKS (ON THE EXAMPLE OF UZBEKISTAN)

Nargis Sunnat kizi KOSIMOVA
Candidate of philological sciences, associate professor
Uzbekistan State World Languages University, Tashkent, Uzbekistan n.qosimova2012@yandex.com

UDC (УЎК, УДК): 004.056.53

For citation (иқтибос келтириш учун, для цитирования):
Косимова Н.С. Виды информационно-психологических угроз в социальных сетях (на примере Узбекистана) // Ўзбекистонда хорижий тиллар. — 2020. — № 1 (30). — С.146–157.

https://doi.org/ 10.36078/1585242480

Received: December 21, 2019
Accepted: February 15, 2020
Published: February 20, 2020

Аннотация. В статье изучены виды информационно-психологических угроз в социальных сетях и их негативное воздействие на личность и общество на примере Узбекистана. В настоящее время вопросы информационно –психологической безопасности в нашей стране рассматриваются применительно к обществу или государству. В стороне остается личная безопасность гражданина Узбекистана. Учитывая тот факт, что обеспечение информационной безопасности носит глобальный характер, все более увеличиваются и виды информационно-психологических угроз. Актуальность проблемы безопасности государства и общества в информационной сфере в настоящее время определяется. с одной стороны, влиянием возникающих в современном обществе различных изменений, порождающих потребность в информации какой бы она не была, а также увеличением потребности, в широком понимании смысла этого явления, в системе общественно-государственной защиты, формирования механизмов информационной защиты.

Сегодня безопасность личности в социальных сетях как совокупности сбалансированных интересов личности, общества и государства, нахождение их координированного баланса в информационной сфере актуализировали проблемы информационно-психологической безопасности. Обеспечением безопасностей пользователя социальных сетей должны выступать соответствующие государственные органы. Иначе в действие вступают механизмы, создающие предпосылки для активизации процессов, способных вызвать переполох и разрушение общества. Следствие данного процесса может носить неконтролируемый характер, поэтому своевременная разработка

необходимых мер по противодействию различным виртуальным угрозам имеет огромное значение.

Сегодня информационно-психологические угрозы в социальных сетях узбекскими учеными практически не изучены. Автором предпринята попытка классификации и систематизации имеющихся научных взглядов по проблемам противодействия информационно-психологическому воздействию на пользователя в социальных сетях, которые сегодня практически не наказуемы. Именно этот факт способствует появлению новых угроз и их видов, таких как троллинг, кибербуллинг и др.

В статье обобщены проблемы, изучены их особенности на примере узбекского онлайн-сегмента и разработаны предложения по их искоренению.

Ключевые слова: информационно-психологическое воздействие; интернет; социальные сети; тролли; кащенизм; фишинг; общество; государство; гражданин.

Аннотация. Мақолада ижтимоий тармоқларда ахборот-психологик хавф ва унинг Ўзбекистон мисолида жамият ва шахсга салбий таъсири масалалари ўрганилган. Мавзунинг долзарблигини шунда кўришимиз мумкинки, мамлакатимизда ахборот-психологик хавфсизлик масалалари кўп ҳолларда алоҳида давлат ёки минтақавий-ҳудудий даражада ўрганилиб, жамиятнинг ажралмас бир қисми сифатида шахс хавфсизлиги масалалари эътибордан четда қолмоқда.

Ахборий жамиятда давлат ва жамият хавфсизлиги масалаларининг долзарблиги бир томондан ҳозирги замонда жамият ҳар қандай ахборотни истеъмол қилишга тайёрлиги билан билан белгиланса, иккинчи томондан ахборотга бўлган эҳтиёжнинг мунтазам равишда ортиб боришида ва ижтимоий муҳофаза тизимида ахборий ҳимоя механизмларининг шаклланишида кўринади.

Бугун шахснинг ижтимоий тармоқлардаги хавфсизлиги шахс, жамият ва давлат манфаатлари кесимида ҳамда ахборий соҳада уларнинг мувофиқлиги ахборий-психологик хавфсизлик масалаларини янада долзарблаштирди. Ижтимоий тармоқлар фойдаланувчисининг хавфсизлигини таъминлашни нафақат фойдаланувчининг ўзи, балки мувофиқ давлат органлари ҳам ўз зиммаларига олиши лозим. Бўлмаса, жамиятда парокандалик ва нотинчликни келтириб чиқарувчи кучлар майдонга чиқиб, мазкур жараёнларни фаоллаштиришга хизмат қилишади. Мазкур жараёнларнинг оқибатларини кейин назорат қилиб бўлмаслиги мумкин. Шу сабабли ҳар қандай виртуал хавфга қарши кураш учун зарур чора-тадбирларни ишлаб чиқиш муҳим аҳамият касб этади.

Бугунги ахборот даврида хавфсизликни таъминлаш маълум даражада глобаллашиб, таҳдидларнинг кўлами ҳам кенгаймоқда. Демак, интернетдаги ахборий хуружлар тобора кучайиб, уларни ўрганиш, олдини олиш борасида чора-тадбирлар ишлаб чиқиш ниҳоятда муҳим. Мақолада муаллиф ахборот –психологик хавфнинг олдини олишга қаратилган илмий қарашларни таснифлаш ва тизимлаштиришга ҳаракат қилади.

Бугунги кунда ижтимоий тармоқлардаги ахборот-психологик хавфлар ва уларнинг турлари бўлган троллинг, кибербуллинг, кашенизм ва бошқалар деярли ўрганилмаган. Бу эса янгидан янги ахборот хавфларини келтириб чиқармоқда. Мазкур мақолада уларнинг хусусиятлари ўзбек онлайн ахборот сегменти мисолида ўрганилиб, мавжуд муаммолар умумлаштирилган ва бартараф этиш бўйича таклифлар ишлаб чиқилган.

Калит сўзлар: ахборот-психологик таъсир; интернет; ижтимоий тармоқлар; троллар; кашенизм; фишинг; давлат; жамият; фуқаро.

Abstract. The article studies the types of information-psychological threats in social networks and their negative impact on the individual and society on the example of Uzbekistan. Currently, issues of information and psychological security in our country are being considered in relation to society or the state. The personal safety of a citizen of Uzbekistan remains aloof. Given the fact that ensuring information security is global in nature, the types of information and psychological threats are also increasing. The relevance of the security problem of the state and society in the information sphere is currently determined on the one hand, by the influence of various changes arising in modern society that generate the need for information no matter what it is, as well as by an increase in the need, in a broad understanding of the meaning of this phenomenon, in the social -state protection, the formation of information protection mechanisms.

Today, personal safety in social networks as a set of balanced interests of the individual, society and the state, finding their coordinated balance in the information sphere actualized the problems of information and psychological security. Ensuring the safety of the user of social networks should be the appropriate state bodies. Otherwise, the mechanisms that create the prerequisites for the activation of processes that can cause a commotion and the destruction of society come into effect. The consequence of this process may be uncontrollable.

Therefore, the timely development of the necessary measures to counter various virtual threats is of great importance. Today, the information and psychological threats in social networks by Uzbek scientists are practically not studied. The author made an attempt to classify and systematize the existing scientific views on the problems of counteracting the information-psychological impact of the user in social networks, which today are practically not punishable. It is this fact that gives rise to the emergence of new threats and their types, such as trolling, cyberbullying, infologema, mobbing, docking, bating and others.

The scientific article summarizes the problems, explores their features on the example of the Uzbek online segment, and develops proposals for their eradication.

Keywords: information and psychological impact; Internet; social networks; trolls; cashenism; phishing; society; state.

Введение. Поговорка «если тебя нет в социальных сетях, то тебя нет и в реальной жизни» появилось совсем недавно, но она показывает суть современного человека. Ведь сегодня практически половина населения земного шара расходует свое время иногда с пользой, а зачастую впустую «сидя» в социальных сетях. Информация в сетях небезопасна. Сначала определимся, что такое социальная сеть. «Социальной сетью является интерактивный многопользовательский ресурс, который наполняется информацией участников сети. Ресурсом является автоматическая социальная среда, которая позволяет общаться с группой участников, что объединены общими интересами» (13).

Учитывая формат, специфику, постоянную аудиторию в социальных сетях, многие страны вырабатывают определенный подход к классификации вызовов и угроз. Так, в 2018 году королевская

прокурорская служба Великобритании выпустила руководство по классификации уголовно наказуемых действий в интернете (2, 47). Среди них «моббинг — массовая травля одного человека группой людей, часто под оскорбительными хештегами», «доксинг — публикация чужих конфиденциальной информации без ведома пользователя», «бэйтинг — унижение пользователей женского пола под различными предлогами их «неэтического» сексуального поведения» (2, 48). В настоящее время эти угрозы принимают новый оборот, ответвляя от себя более мелкие направления. В этом плане система психологической защиты пользователя включает следующие основные направления ее формирования и функционирования: 1) социальный (в масштабах общества), 2) групповой (в рамках различных социальных групп) и 3) индивидуальный. На индивидуальном уровне информационно-психологическая защита реализуется посредством формирования регулятивного комплекса алгоритмов информационного поведения пользователя, которые образуют психологическую самозащиту.

В Узбекистане развитие информационных технологий и их внедрение во все сферы деятельности общества предполагает внедрение систем обеспечения информационной безопасности. «Основное желание киберпреступника – получить выгоду от реализации угроз, а чем больше возможностей предоставляют технологии, тем больше возможности у них (киберпреступников) осуществить свои намерения» (5). В последние годы в Республике Узбекистан обеспечение информационной безопасности осуществляется по следующим направлениям. Это:

1. Совершенствование и развитие нормативно-правовой базы.
2. Разработка и внедрение программного обеспечения по информационной безопасности.
3. Международное взаимодействие и обмен передовым опытом с другими странами (6). Несмотря на вышеперечисленное, до сих пор остро стоят вопросы разработки и координации необходимых мер в сфере информационной безопасности. И к сожалению, «сегодня не существует единого координационного центра по вопросам кибербезопасности, объединяющего отделы обеспечения информационной безопасности операторов и провайдеров сетей, передачи данных, мобильной связи, государственных учреждений, хозяйствующих субъектов и других заинтересованных в реагировании на возможные инциденты информационной безопасности» (6).

Обзор работ по теме. Исследованию теоретических вопросов информационной безопасности, а также информационных угроз в социальных сетях посвящены труды зарубежных ученых (М. Б. Ислам, Р. Ланелла, Я. Ким, А.В. Манойло, А.С. Панарина, И. С. Мельника, М. С. Вершинина, С.Г. Кара-Мурзы), а также узбекских исследователей (Г. Алимова, А. Жарова, Г. Жураев и др.). Основываясь на этих работах, более подробно остановимся на ведении информационно-психологического воздействия в социальных сетях.

Информационная-психологическую безопасность обеспечивают мероприятия, принимаемые меры со стороны государства, общества и частного лица, которые во всем сопутствуют информационным технологиям. Информационная безопасность – это постоянный и совершенствующийся процесс обеспечения безопасности.

Сегодня специалисты по информационной безопасности востребованы практически во всех сферах деятельности человечества.

Все сферы деятельности человека в любом современном государстве нуждаются в высококвалифицированных специалистах по защите информации. В наше время информация обеспечивает жизнедеятельность любой организации, компании, фирмы, гражданина. И если организации, имея в своем штате хороших специалистов по информационной безопасности, уже имеют какую-то защиту, то обычный пользователь является самым незащищенным в процессе обеспечения безопасности. В настоящее время 63% населения Узбекистана «сидит» в социальных сетях, получая оттуда практически всю необходимую информацию.

И часто именно они становятся жертвами различного вида троллинга, кащенизма или кибербуллинга. К сожалению, простой пользователь без специального образования или каких-либо навыков работы с компьютером, сетью интернет является беззащитной жертвой угроз информационной безопасности. Поэтому неудивительно, что они зачастую становятся жертвами киберпреступников. Даже если атака направлена на организацию, то в итоге жертвой все равно становится пользователь. К сожалению, на данный момент ситуация в Республике Узбекистан складывается не самым благоприятным образом для них.

В предлагаемой статье материалом исследования информационно-психологических угроз послужили социальные сети, наиболее популярные в Республике Узбекистан.

Результаты и обсуждение. В настоящее время узбекские пользователи сети Интернет в основном предпочитают такие социальные сети, как Фейсбук, Инстаграм, Одноклассники, Твиттер, Вконтакте. Анализируя информационные угрозы в них, можно выделить такие виды киберпреступлений, как кибербуллинг и троллинг. Различия их от реальных преступных посягательств на личность человека, имидж общества или государства обусловлены особенностями интернет-пространства: анонимностью, возможностями фальсификации, доступностью жертвы в любом месте и в любое время, наличием большой аудитории. В последние годы в Узбекистане получило распространение общественно опасное посягательство на личность несовершеннолетних в виртуальной среде, как кибербуллинг (cyberbullying) – подростковый террор, который получил свое название от английского слова bull — «бык» (агрессивно нападать, бередить, задирать, придираться). В молодежном сленге появился глагол аналогичного происхождения — быковать (9). Кибербуллинг — это нападения с целью нанесения психологического вреда, которые осуществляются через различные платформы передачи информации: электронную почту, сервисы мгновенных сообщений, чаты, социальные сети, web-сайты, а также посредством мобильной связи и интернета. Основная особенность — многократное повторяемость агрессивного поведения, которая ставит перед собой цель навредить человеку и базируется на дисбалансе власти (физической силы, социального статуса в группе) (9). Троллинг — это «размещение в социальных сетях, форумах провокационных сообщений с целью вызвать флейм, конфликты между участниками, взаимные оскорбления и т.п. ...» (1, 32). «Задача тролля состоит в том, чтобы превратить спокойный тред в ярый спор, конфликт, в который ввяжется как можно большее количество читателей, а изначальная тема разговора будет забыта напрочь» (1, 32).

Еще один новый и значимый вид информационной угрозы в социальных сетях — кащенизм. Это своеобразное общение в

чатах или в эхо-конференциях, «характеризующийся провокационными, главным образом прасемитскими, антисемитскими, националистическими, агрессивно-мещанскими или психиатрическими высказываниями и ситуационной насмешкой над собеседником» (3). Кащенизм влечет за собой провоцирование обсуждаемой темы, не являющейся темой чата или конференции; вызывание различных, противоречивых друг другу споров, с целью увеличения бессмысленных сообщений; провоцирование собеседников на негативную дискуссию, возмущение; выставление собеседника в негативном свете, обвиняя его радикалистом или экстремистом. Бывший топ-менеджер Twitter Дик Костоло высказался на эту же тему: «Мы годами проигрываем войну с троллингом на нашей платформе. Мы теряем основного пользователя, не решая проблему, с которой люди сталкиваются каждый день. Мне стыдно за то, что мы не справились с этим во время моего пребывания на посту генерального директора» (3). Костоло отметил, что «один из источников бед современного общества — игнорирование отношения к психологическому насилию» (3). Агрессия, проявленная в социальных сетях, не наносит пользователю физических повреждений, с которыми можно было бы обратиться в правоохранительные органы с жалобой, но оставляет после себя моральную избитость. И хотя в законодательстве различных стран мира прописано административное или уголовное наказание за психологическое насилие, точного определения данного понятия до сих пор не существует. В законодательных документах различного уровня предусматривается ответственность или наказание за прямую угрозу физической расправы человека, и поэтому наказать правонарушителей, которые наносят психологический вред, очень трудно.

«То, что люди, подвергающиеся психологическому насилию, нуждаются в защите не меньше тех, на кого посягают физически, — факт, признанный мировым сообществом», — говорит Джошуа Франко, заместитель директора Amnesty Tech, подразделения правозащитной организации Amnesty International. — Это отражено в тексте нескольких международных конвенций, к примеру, в Стамбульской конвенции о противодействии насилию против женщин. Там есть даже особое упоминание о проявлениях психологического насилия в интернете» (3). В настоящее время можно классифицировать несколько видов кибербуллинга.

— киберпреследование, то есть скрытое выслеживание заранее намеченной жертвы, чтобы организовать нападение, избиение, нанесение телесного повреждения или изнасилование;

— хеппислеппинг (happy slapping — счастливое хлопанье, радостное избиение) — это видеоролики с записями сцен насилия, взятых из реальной жизни;

— кибермошенничество — кража личных данных пользователя с помощью различных технических средств. В настоящее время для кражи личной информации пользователя применяются различные и наиболее сложные фишинговые схемы. Фишинг — это вид онлайн-мошенничества для получения доступа к конфиденциальным данным пользователей. Здесь схема очень проста. Хакер рассылает сотни сообщений от имени популярных брендов, звезд шоу-бизнеса, государственных деятелей, а также личных сообщений внутри различных сервисов, например, от имени банков (Миллий банк,

Капитал банк, Халк банки), сервисов (Rambler, mail.ru) или внутри социальных сетей (Facebook, Instagram, Одноклассники.ru). В письме часто указывается прямая ссылка на фишинговый сайт. Простой, технически невооруженный пользователь внешне не сможет отличить его от настоящего. После того «как пользователь, попав на «крючок», переходит на поддельную страницу, мошенники пытаются различными психологическими приёмами побудить пользователя ввести на поддельной странице свои логин и пароль, которые он использует для доступа к определенному сайту, что позволяет мошенникам получить доступ к аккаунтам и банковским счетам» (7).

Все вышеперечисленные виды информационных угроз наносят вред информационной безопасности личности, общества, государства. Это выражается в следующих формах:

— «причинение вреда физическому и психологическому оровью человека;

— блокирование на неосознаваемом уровне свободы человека,

— искусственное привитие пользователю синдрома зависимости;

— утрата способности к политической, культурной, равственной, социальной самоидентификации человека;

— манипуляция и управление общественным сознанием;

— разрушение единого информационного и духовного ространства страны, традиционных устоев общества и общественной равственности, а также нарушении иных жизненно важных интересов ичности, общества и государства» (5).

Отдельного внимания заслуживает вопрос форм информационного воздействия на общества и государства в целом. К таким методам относятся:

«— навязывание своей политической воли через идеологическую, психологическую обработку населения, вооруженных сил, руководства страны для создания требуемого общественного мнения;

— изменение традиционных укладов, национальных ценностей, образа жизни, разобщение народа, уничтожение морально-политического потенциала общества и разрушение государства изнутри путем идеологической революции, разрушения национального самосознания, размывания чувства патриотизма, культуры, традиций, исторической памяти, подрыва духовно-нравственных устоев» (5).

Информационные угрозы в социальных сетях в данном процессе провоцируют пользователей на самоуничтожение, разрушая духовные ценности и культурные устои, что приводит к различным социальным волнениям и наносить значительный финансовый и имиджевой ущерб государству. Например, в 2018 году заместитель директора Агентства информации и массовых коммуникаций (АИМК) при администрации президента Узбекистана Наргиза Рахимова подверглась информационной травле со стороны интернет-троллей и представителей религиозного сегмента после неосторожной публикации на странице «Озодлика» в Facebook комментария на тему многоженства у мусульман. Все началось в преддверии 8 Марта, когда пользователь Хаёт Бахтиёр угли написал на странице радио в Facebook комментарий в защиту многоженства. «Только мужики-тряпки, которые не смогут справиться даже с одной женой, и женщины-стервы, которые сидят на шее своих мужей как на ишаке, выступают против многоженства», — написал Хаёт Бахтиёр угли. Ответный комментарий Наргизы Рахимовой был резок. «Наш пророк не брал

вторую жену при жизни нашей матери Хадичи. Не знаю, может, в то время он был тряпкой, может, наша мать Хадича была стервой, это вы лучше знаете. Хазрат Али тоже не брал вторую жену при жизни нашей матери Фотимы. Это обстоятельство очень смешное, конечно» (11). После этого в социальных сетях появились сотни текстовых и видеокомментариев, направленных против государственной служащей. Некоторые пользователи открыто пригрозили ей и ее семье смертью. В данном деле, анализируя сложившую ситуацию, эксперты по интернет-троллингу обнаружили ряд фейковых аккаунтов, которые сообщают, что якобы на самом деле заместитель директора АИМК не сожалеет о сказанном и называет оппонентов по спору идиотами. В узбекоязычных Telegram-каналах появились посты об активности троллей, содержащие десятки доказательств в виде скриншотов с однотипными текстами против чиновницы. Онлайн-насилие в отношении женщин считается глобальной проблемой, а женщины-чиновники, выступившие с заявлением, противоречащим мнению мужчин, в большинстве случаев подвергаются угрозам и негативным нападкам. К сожалению, число таких угроз в узбекском сегменте интернет-пространства всего лишь за последние два года выросло в несколько раз, что показывает об усилении активности троллей не только в социальных сетях, но и в домене uz.

Анализируя угрозы в социальных сетях, нельзя не упомянуть о несанкционированном входе в аккаунты пользователей. Для осуществления данной угрозы злоумышленник может использовать подбор или перехват учётных данных пользователя, ложное восстановление его пароля с использованием секретного вопроса и применить другие способы. Многие крупные социальные сети затрудняют такие атаки, применяя схемы двухфакторной аутентификации, блокирование учётной записи при попытке подбора пароля и другие схемы защиты. Последствия успешной атаки для владельца учётной записи могут быть самыми разными, а именно:

— кража личных данных владельца, включая личную переписку, фотографии и т.п.;

— использование профиля в мошеннических целях путём эксплуатации доверия друзей атакованного пользователя;

— дискредитация владельца профиля;

— деанонимизация владельца профиля» (8).

Кроме перечисленных «традиционных» угроз, пользователь социальных сетей сталкивается со специфической проблемой безопасности личных данных, а именно «неявной утратой контроля над личной информацией». Выше упоминалось косвенное получение сведений о пользователе путём анализа личных данных его друзей. Другим примером косвенного извлечения сведений является получение информации о перемещениях или излюбленных местах пользователя через анализ метаданных его фотографий, размещенных на его страничках. Некоторые социальные сети предоставляют функцию поиска фотографий, сделанных в области с указанными координатами, что позволяет, например, выявлять учётные записи пользователей, проживающих или работающих по заданному адресу. Другой путь утраты контроля за личными сведениями, а именно «вечное» хранение данных, характерен для многих информационных сервисов. У пользователя социальных сетей нет никакой возможности удостовериться в реальности удаления личных данных, удаляемых пользователем. Так, например, политика использования данных

Facebook гласит: «Мы храним данные столько времени, сколько это необходимо, чтобы обеспечить функционирование продуктов и услуг, в том числе описанных выше, для вас и других пользователей. Информация, связанная с вашим аккаунтом, будет храниться до его удаления или же до того момента, когда нам больше не будут нужны эти данные для предоставления продуктов и сервисов» (10). Активные пользователи социальных сетей нередко сталкиваются с нежелательным разглашением информации третьими лицами. Например, пользователь может быть упомянут в публикации другого пользователя, может быть отмечен на фотографии, опубликованной им. Негативные последствия подобного могут быть разнообразными: проблемы на работе или в семье из-за вскрытия утаиваемых фактов.

Согласно данным, в Узбекистане сегодня насчитывается 15 миллионов интернет-пользователей, из которых 80% используют мобильный интернет. «Самыми популярными у узбекских интернет-пользователей социальных сетей являются Odnoklassniki.ru, Facebook и Vk.ru. Так, например, два миллиона узбекских пользователей регулярно посещают социальную сеть ok.ru, а аудитория сети Facebook вместе с Instagram составляет более 1 млн. 600 тысяч пользователей» (8).

Доктрина информационной безопасности Узбекистана обозначает следующие виды угроз информационной безопасности:

— «угрозы конституционным правам и свободам человека в области информационной деятельности, индивидуальному, групповому и общественному сознанию граждан Республики Узбекистан;

— угрозы информационному обеспечению внутренней и внешней государственной политики Узбекистана;

— угрозы развитию отечественной индустрии информации, включая индустрию средств информатизации, телекоммуникации и связи, обеспечению потребностей внутреннего рынка в ее продукции и выходу этой продукции на мировой рынок, а также обеспечению накопления, сохранности и эффективного использования отечественных информационных ресурсов;

— угрозы безопасности информационных и телекоммуникационных средств и систем, как уже развернутых, так и создаваемых на территории Узбекистана.

— К угрозам конституционным правам и свободам человека и гражданина в области духовной жизни и информационной деятельности, индивидуальному, групповому и общественному сознанию, духовному возражению Узбекистана относится в числе прочего:

— противоправное применение специальных средств воздействия на индивидуальное, групповое и общественное сознание;

— манипулирование информацией (дезинформация, сокрытие или искажение информации)» (10).

Другие распространённые проблемы, «кросс-сайтовый скриптинг» и распространение вирусов и «червей», реализуются с помощью средств информационного обмена в социальных сетях, а именно: публикаций на личных страницах и на страницах групп и личных сообщений. Успех «кросс-сайтового скриптинга» в социальные сети может приводить к выполнению различных действий от лица пользователя (https://xakep.ru/2011/03/10/55008/), подменять ссылки

(https://xakep.ru/2008/05/26/43751/), выполнять иные воздействия на пользователя.

Заключение. Информационные угрозы в социальных сетях встречаются очень часто. Данная проблема требует постоянного серьезного изучения для обеспечения эффективности реализации государственной политики в сфере информационной безопасности. «В целом же, политическая предвзятость руководства социальной сети, легкодоступность личных данных пользователей и широкие возможности проведения политических рекламных кампаний и продвижения нужной информации в социальной сети, а также развитой механизм таргетирования пользователей приводят к тому, что пространство социальной сети легко может использоваться и используется для проведения информационно-психологических операций» (12, 47).

Сегодня необходимо создание современной системы противодействия информационным угрозам в социальных сетях и налаживание сотрудничества между развитыми государствами в этом направлении, а также создание информационно-аналитических организаций, которые должны проводить мониторинг информационных угроз не только в государственных сайтах, но и в социальных сетях. Они должны содействовать выработке методов противодействия перечисленным угрозам и реализации оптимальных моделей безопасности для каждой страны.

Использованная литература

1. Акулич М.М. Троллинг в социальных сетях: возникновение и развитие// Вестник РУДН, серия Социология. — 2012. — № 3. С. 30–36. — URL: https://cyberleninka.ru/article/n/trolling-v-sotsialnyh-setyah-vozniknovenie-i-razvitie/viewer

2. Бабенко М. Скрытые угрозы в социальных сетях. Электронный ресурс. http://cripo.com.ua/processes/skrytye-ugrozy-v-sotsialnyh-setyah/

*3.*Зона беззащитности. Скрытые угрозы, которым дети и взрослые подвергаются в социальных сетях. Электронный ресурс. https://osvitanova.com.ua/posts/2389-zona-bezzashchytnosty-skrytye-uhrozy-kotorym-dety-y-vzroslye-podverhaiutsia-v-sotsyalnykh-setiakh

*4.*Виды онлайн угроз, представляющих опасность для жизни, физического, психического и нравственного здоровья и полноценного развития ребенка. Электронный ресурс. https://74205s25.edusite.ru/DswMedia/vidy_onlajn-ugroz.pdf

5.Информационно-психологическая безопасность несовершеннолетних в сети Интернет. Электронный ресурс. https://infourok.ru/informacionnopsihologicheskaya-bezopasnost-nesovershennoletnih-v-seti-internet-1798086.html

6.Ишимбаев,Э. Угрозы информационной безопасности. Тенденции, пути, средства и методы борьбы с ними. Электронный ресурс. http://infocom.uz/2009/12/02/ugrozyi-informatsionnoy-bezopasnosti-tendentsii-puti-sredstva-i-metodyi-borbyi-s-nimi/

7. Ковалева, Н.Н. Информационное право России. Учебное пособие. Электронный ресурс. https://knigi.news/informatsionnoe/informatsionnoe- pravo-rossii-uchebnoe.html

8.Курилкин, А. В. (2019) Проблемы информационно-психологического манипулирования в пространстве сети Facebook.

Электронный ресурс. http://www.vestnik.vsu.ru/pdf/history/2019/02/2019-02-13.pdf
9. Ненашев, С.М. (2016) Информационно-технологическая и информационно-психологическая безопасность пользователей социальных сетей. Электронный ресурс. https://cyberleninka.ru/article/n/informatsionno-tehnologicheskaya-i-informatsionno-psihologicheskaya-bezopasnost-polzovateley-sotsialnyh-setey
*10.*Опубликованы самые популярные сервисы, приложения и телефоны интернет-пользователей Узбекистана. Электронный ресурс. http://infocom.uz/2018/01/22/opublikovany-samye-populyarnye-servisy-prilozheniya-i-telefony-internet-polzovatelej-uzbekistana/
*11.*Узбекские спецслужбы взяли под круглосуточную охрану дом чиновницы после неосторожной публикации о пророке Мухаммеде. Электронный ресурс. https://zen.yandex.ru/media/id/5b02a8b27425f529296bcf38/uzbekskie-specslujby-vziali-pod-kruglosutochnuiu-ohranu-dom-chinovnicy-posle-neostorojnoi-publikacii-o-proroke-muhammede-5c8764684f313200b3713daf
12.Чеботарева А.А. Правовое обеспечение информационной безопасности личности в глобальном информационном обществе. Диссертация на соискание ученой степени доктора юридических наук. Москва, 2017. — 473 с.
13. https://spravochnick.ru/informacionnaya_bezopasnost/zaschita_informacii/zaschita_informacii_v_socsetyah

References

1. Akulich M.M. *Vestnik RUDN, seriya Sotsiologiya*, 2012, No 3, pp. 30–36, available at: https://cyberleninka.ru/article/n/trolling-v-sotsialnyh-setyah-vozniknovenie-i-razvitie/viewer
2. Babenko M. available at: http://cripo.com.ua/processes/skrytye-ugrozy-v-sotsialnyh-setyah/
3. https://osvitanova.com.ua/posts/2389-zona-bezzashchytnosty-skrytye-uhrozy-kotorym-dety-y-vzroslye-podverhaiutsia-v-sotsyalnykh-setiakh
4. https://74205s25.edusite.ru/DswMedia/vidy_onlajn-ugroz.pdf
5. https://infourok.ru/informacionnopsihologicheskaya-bezopasnost-nesovershennoletnih-v-seti-internet-1798086.html
6.Ishimbaev E. available at: http://infocom.uz/2009/12/02/ugrozyi-informatsionnoy-bezopasnosti-tendentsii-puti-sredstva-i-metodyi-borbyi-s-nimi/
7. Kovaleva N.N. available at: https://knigi.news/informatsionnoe/informatsionnoe-pravo-rossii-uchebnoe.html
8. Kurilkin A. V. available at: http://www.vestnik.vsu.ru/pdf/history/2019/02/2019-02-13.pdf
9. Nenashev, S.M. available at: https://cyberleninka.ru/article/n/informatsionno-tehnologicheskaya-i-informatsionno-psihologicheskaya-bezopasnost-polzovateley-sotsialnyh-setey
10. http://infocom.uz/2018/01/22/opublikovany-samye-populyarnye-servisy-prilozheniya-i-telefony-internet- polzovatelej-uzbekistana/
11.https://zen.yandex.ru/media/id/5b02a8b27425f529296bcf38/uzbekskie-specslujby-vziali-pod-kruglosutochnuiu-ohranu-dom-chinovnicy-posle-neostorojnoi-publikacii-o-proroke-muhammede-5c8764684f313200b3713daf

12. Chebotareva, A.A. *Pravovoe obespechenie informatsionnoi bezopasnosti lichnosti v global'nom informatsionnom obshchestve* (Legal support of personal information security in the global information society), Doctor's thesis, Moscow, 2017, 473 p.
13.https://spravochnick.ru/informacionnaya_bezopasnost/zaschita_informa cii/ zaschita_informacii_v_socsetyah