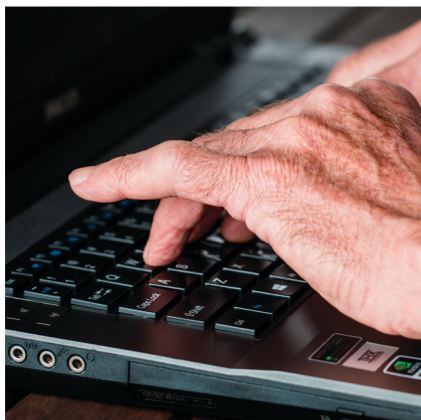


ОБЗОР.НЦПТИ

Выпуск № 1 (16)

Март 2019



В.С. Жученко
С.А. Чурилов

Терроризм как явление
реальное и новостное:
особенности работы СМИ

И.С. Мальшева
М.В. Шихова

Игра-квест «Ангитеррор»

К.А. Тюрин

Нечеткое хэширование
в задачах информационной
безопасности

18+

Россия, г. Ростов-на-Дону
тел./факс: (863) 201-28-22
нцпти.рф





Обзор.НЦПТИ № 1 (16)
Издание зарегистрировано Федеральной
службой по надзору в сфере связи,
информационных технологий и массовых
коммуникаций (Роскомнадзор).

Свидетельство о регистрации СМИ
ПИ № ФС 77-52390 от 28.12.2012
ISSN 2411-0124.

Учредитель: федеральное государственное
автономное научное учреждение
«Научно-исследовательский институт
«Специализированные вычислительные
устройства защиты
и автоматика» (ФГАНУ НИИ
«Спецвузавтоматика» Минобрнауки России).
Издатель: Национальный центр
информационного противодействия
терроризму и экстремизму
в образовательной среде и сети Интернет.
При поддержке: Минобрнауки России;
Регионального общественного центра интернет-
технологий (РОЦИТ); Представительства в
Ростовской области Фонда содействия
инновациям.

Распространяется бесплатно.

Главный редактор:
Яровой Анатолий Владимирович.

Иллюстрации предоставлены авторами
публикаций.

Редколлегия:
Быкадорова Александра Сергеевна, кандидат
филологических наук;
Гуфан Константин Юрьевич, кандидат
физико-математических наук;
Кожанова Екатерина Владимировна,
ответственный секретарь;
Непейвода Кира Михайловна, кандидат
филологических наук;
Селин Роман Николаевич, кандидат
технических наук;
Сериков Антон Владимирович, кандидат
социологических наук, доцент;
Хади Роман Ахмедович, кандидат технических
наук, профессор АВН.

Тематические направления:
04.00.00 Социология;
11.00.00 Политика. Политические науки;
14.00.00 Народное образование. Педагогика;
19.00.00 Массовая коммуникация.
Журналистика. Средства массовой
информации;
20.00.00 Информатика.

Мнение редакции может не совпадать с
мнением авторов.

Адрес редакции: 344011, г. Ростов-на-Дону,
ул. Города Волос, 6, тел.: (863) 201-28-22.
Адрес типографии: 344000, г. Ростов-на-Дону,
пл. Гагарина, д. 1, ООО «ДГТУ-Принт»,
тел.: (863) 226-85-10, (928) 102-36-99.
Тираж: 150 экз.
Заказ № 18/4
Дата подписания в печать
По графику: 29.03.2019
Фактическая: 29.03.2019

От редактора

Яровой Анатолий Владимирович – главный редактор, заместитель директора Национального центра информационного противодействия терроризму и экстремизму в образовательной среде и сети Интернет по связям с общественностью

Не так часто приходится анонсировать материалы выпуска, одновременно отражающие интересы и молодых наших читателей, и тех потребителей информации, кому за 30-40, а то и 50+... Я имею ввиду, во-первых, публикацию об удачном эксперименте, представляющем интерес для молодежной аудитории, который предлагают креативные мурманчане, разработавшие игру-квест «Антитеррор», а во-вторых, статью студентов-социологов ЮФУ об опыте исследования адаптации граждан старшего поколения к общению в социальных сетях.

И в первом и во втором случаях востребованность несомненна, ибо важность поднимаемых авторами тем бесспорна. Если говорить о набирающей популярность интерактивной игре-квест, с цепочкой загадок и головоломок, развивающей у участников интеллектуальные, психологические и физические способности, то всякая новая её разновидность, безусловно, интересна, а тем более такая тема как противостояние терроризму.

Но вот уж кто явно обделен вниманием со стороны разработчиков информационных технологий - это люди старшего поколения, с завистью глядящие на внуков-«миллениалов» и мечтающие о свободном владении навыками интернет-пользователей, которые позволили бы вести активное общение с друзьями-ровесниками, имеющими массу свободного времени и не утратившими интереса к жизни во всех её проявлениях. При этом для многих мало понятны особенности, которыми изобилует скрытая часть машины интернета: от угрозы получить негатив со стороны незнакомых людей и взлома страниц в аккаунтах, до необходимости пользоваться паролями и способах охранять личное пространство от злоумышленников.

Очевидно, что исследование самопрезентации старшего поколения в социальных сетях, проведенное учащимися ростовского университета, весьма актуально, ибо позволяет оценить ситуацию с виртуальным общением людей старшей возрастной группы и

спрогнозировать задачи по их коммуникации.

Не менее полезен результат, полученный в Мурманской области и позволяющий с помощью смоделированных ситуаций обучать участников игры -квеста правильным действиям в случаях угрозы террористического акта, а также основам противо-

действия экстремистской пропаганде.

Впрочем, остальные материалы, публикуемые в этом выпуске, рассматривающие проблемы профилактики в молодежной и образовательной среде таких явлений, как терроризм, экстремизм, ксенофобия, также интересны и, надеюсь, полезны.



И.И. Сидоров



ЖУРНАЛ «ОБЗОР.НЦПТИ» ПЛОЩАДКА С 2013 ГОДА

Объединяет специалистов по информационной безопасности, экспертов в области защиты данных и образовательных технологий со всей России

Распространение тиража журнала

Журнал - это площадка для обмена мнениями между экспертами, профессионалами и управленцами

Москва

51%

Ростовская область

23%

Воронежская область

2%

Республика Дагестан

2%

КБР

2%

Крым

2%

Северная Осетия

2%

Орловская область

2%

Ставропольский край


7%

Краснодарский край

7%

 Формат - А4

 Объем - 50 полос

 Периодичность выхода - четыре раза в год

 Тип издания: отраслевой исследовательский журнал

В «ОБЗОР.НЦПТИ» РАЗМЕЩАЕТСЯ МОДУЛЬНАЯ РЕКЛАМА

Требования к модулям:

Рекламные модули принимаются в формате .tiff (не менее 300 dpi) или .cdr, CMYK

Рекламные тексты принимаются в формате .doc, .docx, табличные данные - в формате .xlsx

По вопросам публикации модульной рекламы обращайтесь в редакцию журнала:
тел.: (863) 201-28-22, e-mail: info@ncpti.ru

Содержание

8

**ЖУЧЕНКО ВИКТОРИЯ СЕРГЕЕВНА
ЧУРИЛОВ СЕРГЕЙ АНАТОЛЬЕВИЧ**

Терроризм как явление реальное и новостное: особенности работы СМИ (к постановке проблемы)

14

ПОТАПОВА ЛЮДМИЛА АЛЕКСАНДРОВНА

Актуализация отдельных методов профилактики распространения идеологии экстремизма и терроризма в молодёжной среде

25

**САФРОНОВА АНАСТАСИЯ НИКОЛАЕВНА
МОЛЧАНОВ НИКОЛАЙ АЛЕКСЕЕВИЧ**

Реально-виртуальная воспитательная среда вуза как профилактическое средство противодействия социально-разрушающим провокациям современного общества

31

**ИВЧЕНКО АЛИСА АЛЕКСАНДРОВНА
КАДИЕВА ДАРЬЯ РУСЛАНОВНА
КОНИВЦОВА АНАСТАСИЯ МИХАЙЛОВНА
ПЛЯСОВА АНАСТАСИЯ ВЛАДИМИРОВНА
САРКИСЯН НЕЛЛИ ЛЕВОНОВНА**

Использование персональных данных в самопрезентации личности (старшего поколения) в социальных сетях



40

ТЮРИН КАЙ АНДРЕЕВИЧ

Нечёткое хэширование в задачах информационной безопасности

62

**КУДРЯВЦЕВ НИКИТА АЛЕКСАНДРОВИЧ
ХАСЕИНОВ ЭМИН ЯХЬЯЕВИЧ**

Проблемы противодействия религиозному экстремизму в России

54

**ДЁШИНА ЕКАТЕРИНА ИГОРЕВНА
МЕРКУЛОВА АНАСТАСИЯ НИКОЛАЕВНА**

Молодёжь как социально-демографическая группа, наиболее подверженная влиянию экстремизма и терроризма в сети Интернет

70

**МАЛЫШЕВА ИРИНА СЕРГЕЕВНА
ШИХОВА МАРИНА ВАЛЕРЬЕВНА**

Игра-квест «Антитеррор» как положительный опыт профилактики терроризма и экстремизма в молодёжной среде



Терроризм как явление реальное и новостное: особенности работы СМИ (к постановке проблемы)

Жученко Виктория Сергеевна — аналитик Национального центра информационного противодействия терроризму и экстремизму в образовательной среде и сети Интернет, аспирант Южного федерального университета, г. Ростов-на-Дону

Чурилов Сергей Анатольевич — директор Национального центра информационного противодействия терроризму и экстремизму в образовательной среде и сети Интернет

Терроризм – одна из главных международных угроз XXI века. С распространением интернет-коммуникаций, развитием других видов связи и передачи информации, к сожалению, усилилась роль средств массовой информации в воздействии терроризма на массовое сознание. Американский аналитик Брюс Хоффман пишет, что «предназначение теракта – передать определённое послание» [1], и с этой точки зрения СМИ определённо играют ключевую роль.

Вслед за Г. Маккормиком, современные исследователи всё чаще обращают внимание на проблему, которую отметил в свое время ещё русский анархист Павел Турчинин, заявляя, что «динамит помогает борцам за свободу совершать более масштабные акции, а пресса – делать их более громкими» [2]. Вли-

яние СМИ на терроризм, безусловно, должно изучаться, однако, слабоизученной остается другая, не менее важная проблема – способность СМИ трансформировать в общественном сознании само представление о явлении терроризма. Другими словами, важно не только «как» обществу транслируют терроризм, но и «что» под ним подразумевают.

В изучении данной проблемы большую роль играют количественные данные. Так, международной группой экспертов под эгидой Института экономики и мира Сиднейского университета в Австралии разработан индекс терроризма (Global Terrorism Index) для оценивания уровня террористической угрозы в разных странах мира. В составленный в 2018 году



рейтинг было включено 163 страны, которые охватывают 99,7% населения мира. Согласно списку, самый высокий рейтинг у Ирака (9,75), Афганистана (9,39), Нигерии (8,66), Сирии (8,32) и Пакистана (8,18). США занимают 20 место, Великобритания – 28, Франция – 30 [3].

К похожим выводам приходят и в других исследованиях, проведенных уже, например, в Мэрилендском университете (США). Ученые проанализировали свыше 113 тысяч террористических атак по всему миру, с 1970 по 2012 годы, и создали базу данных Global Terrorism Database.

Было выявлено, что наиболее подверженной нападениям является Колумбия, а на 10% стран мира приходится 75% террористических атак. Интересен и другой вывод: большинство атак совершаются не международными террористическими организациями, а гражданами стран, в которых произошел теракт [4].

В то же самое время, если проследить повестку европейских и российских СМИ, в большей степени освещаются террористические акты, произошедшие в европейских странах или в Северной Америке. 18 января 2019 года в Ко-

лумбии в Бооте произошел теракт в школе полиции, погиб 21 человек. Если в российском медиапространстве о взрыве сообщили такие ведущие СМИ, как «РИА Новости», «ТАСС», «Российская газета», REGNUM, и писали о ходе расследования и судьбе жертв вплоть до 21 января, то в Великобритании происшествию не было уделено особого внимания. The Guardian сообщила о теракте в разделе новостей Американских континентов, а The Washington Post пропустила данную новость. Похожая ситуация сложилась и во французских изданиях: если Le Figaro информировала о произошедшем теракте, причем неоднократно, то другая ведущая газета Le Monde не сочла его достаточным для публикации информационным поводом.

Показательно и то, что, например, запрос «терракты в Афганистане» «в поисковой системе Яндекс на 14 февраля 2019 года выдает 13 миллионов результатов, «терракты в Ираке» – 14 миллионов результатов, в Сирии – 19 миллионов, во Франции – 21 миллион результатов, в Германии – 29 миллионов, в США – 35 миллионов, в России – 58 миллионов.

Говоря о том, как именно СМИ сегодня освещают террористические акты, стоит отметить, что наблюдается поворот в сторону более профессиональной журналистики. Сегодня сложно представить себе ситуацию, которая

произошла в 2002 году при захвате террористами театрального центра на Дубровке в Москве, когда перемещения спецназа и милиции транслировались по телеканалам. После этого теракта в 2003 году VII съездом Союза журналистов России были одобрены «Этические принципы профессионального поведения журналистов, освещающих акты терроризма и контртеррористические операции». Индустриальным комитетом СМИ принята «Антитеррористическая конвенция», а в 2005 году руководителями телеканалов Первого канала, России, НТВ, ТВЦ, СТС, REN TV подписана Хартия телеведущих против насилия и жестокости.

Согласно вышеперечисленным документам, журналисты и репортеры обязались не предоставлять террористам возможность выхода в прямой эфир, сообщать правоохранительным органам о фактах получения информации о готовящихся терактах, избегать прямых контактов с террористами, не допускать монтажа фото- и видеоматериалов, который может исказить представление читателей и телезрителей о реальных событиях, избегать идентификации родственников и друзей лиц, пострадавших от теракта, без их согласия и т.д.

Данные меры способствовали переходу СМИ в сфе-



ре освещения террористических актов на качественно новый уровень. Однако стоит отметить и тот факт, что спустя время некоторые пункты принятых документов стали забываться журналистами. Например, запрет отождествления терроризма с какой-либо конкретной религией, расой или национальностью. Наблюдается тенденция придания террористу «типичного» образа. Этот вопрос исследовал в 2014 году к.ф.н., доцент кафедры периодической печати Уральского федерального университета В.М. Амиров. Он проанализировал материалы таких СМИ, как «Известия», «Независимая газета», «Комсомольская правда» и «Аргументы и факты» различных периодов, освещающих вопросы терроризма, и пришел к выводу, что совре-

менные печатные СМИ активно указывают на религиозно-этническую подоплёку [5]. В частности, если рассматривать теракты в Беслане, Каспийске и в Москве (на Дубровке), то по отношению к террористам использовались следующие топонимы: террористы, боевики, вооружённые бандиты. Освещая теракты в Волгограде в 2013 году, журналисты употребляли следующие выражения: «все погибшие являются русскими и православными», «уроженец Узбекистана»; «шахидка, уроженка Дагестана»; «дагестанская бандгруппа», «внешность у меня откровенно славянская, максимум скандинавская, и это только играло мне на руку – на террориста я никак не смахивал».

Говоря о субъективности СМИ, стоит отметить и другую проблему – причисление

к терроризму преступлений, которые носят иной характер. Разношерстность в формулировках журналистов в этом вопросе очень часто объясняется неоднозначностью трактовок правоохранительными и государственными органами. Ярким примером является массовое убийство в Мюнхене 22 июля 2016 года. Полиция, прокуратура и Министерство внутренних дел Баварии расценили преступление как амок, в то время как Федеральное управление юстиции Германии назвало произошедшее терактом.

В России к данному вопросу более последовательное и категоричное отношение, но возникают и сложности. Например, массовое убийство в Керченском политехническом колледже изначально рассматривалось как теракт, позже было переклассифицировано в «убийство двух и более лиц общеопасным способом».

Подобные инциденты наглядно демонстрируют и различие подачи информации официальными и неофициальными или оппозиционными СМИ. В частности, кандидат исторических наук МГУ Д.Ю. Базаркина, изучая коммуникационный эффект терроризма, на примере терактов в Мадриде 11 марта 2004 года отмечает сложную ситуацию, в которую было поставлено испанское правительство. Принимая во внимание, что теракт произошел накануне парламентских выборов, она

выделяет активность оппозиционных СМИ в качестве дополнительного фактора, осложняющего кризисную коммуникацию властей [7, с. 140]. Создание атмосферы неопределённости в обозначении виновников теракта спровоцировало ещё большую панику среди населения, вылившуюся в массовые демонстрации, обвиняющие правительство во лжи.

Таким образом, СМИ не просто транслируют и освещают ситуацию, но и задают направление формирования общественного мнения, и, зачастую, не только в сторону его полного неприятия. Террористический акт преподносится как явление не только политическое, но и национальное, религиозное. Однако закон гласит: «терроризм – идеология насилия и практика воздействия на принятие решения органами государственной власти, органами местного самоуправления или международными организациями, связанные с устрашением населения и (или) иными формами противоправных насильственных действий» [6]. Это свидетельствует о том, что несмотря на поворот в сторону более профессионального и ответственного освещения тематики терроризма, проблемы в сфере разграничения терроризма как реального явления и информационного повода всё ещё существуют.



Проанализировав вышеупомянутые материалы, можно говорить о том, что в глобальном плане, при освещении ведущими СМИ тематики терроризма, иногда наблюдается искажение масштабов и смещение общего вектора трансляции в сторону Европы и американских континентов. В качественном плане, среди российских СМИ происходит, с одной стороны, уход от непрофессиональных тактик освещения террористических актов журналистами, с другой – наблюдается формирование «типичного» образа террориста, которому присущи национальные и религиозные характеристики.

Литература:

1. Хоффман Б. Терроризм – взгляд изнутри. М.: У-Фактория, 2003. 264 с.

2. McCormick G.H. Terrorist decision making // Department of Defense Analysis, Naval Postgraduate School, Monterey, 2003.

3. Institute for Economics and Peace. Global Terrorism Index 2018: Measuring the impact of terrorism, Sydney, November 2018.

4. Understanding Terrorism and the Terrorist Threat / Coursera. University of Maryland, College Park. 2018.

5. Амиров В.М. Новые тенденции в освещении актов терроризма российскими печатными СМИ // Политическая лингвистика. 2014. С. 128-130.

6. Федеральный закон № 35 «О противодействии терроризму» от 06.03.2006 // Российская газета. 10.03.2006.

7. Базаркина Д.Ю. Коммуникационный эффект терроризма на примере терактов в Мадриде 11 марта 2004 года // Государственное управление. Электронный вестник. 2014. № 43. С. 135 – 152.

Актуализация отдельных методов профилактики распространения идеологии экстремизма и терроризма в молодёжной среде

(опыт НИЛ «Научно-методическое обеспечение профилактики экстремизма и ксенофобии в системе российского образования» МГПИ имени М.Е. Евсевьева)

Потапова Людмила Александровна — кандидат юридических наук, заведующая кафедрой правовых дисциплин, эксперт научно-исследовательской лаборатории «Научно-методическое обеспечение профилактики экстремизма и ксенофобии в системе российского образования» МГПИ, г. Саранск

Формирование в педагогическом вузе антиэкстремистской образовательной среды представляет отдельную задачу, с одной стороны, направленную на обеспечение безопасности в образовательной организации, а с другой – на подготовку работников системы образования, способных в соответствии с ФГОС формировать у обучающихся российскую гражданскую идентичность в поликультурном социуме и развивать способность противостоять идеологии экстремизма, национализма, ксенофобии, дискриминации по социальным, религиозным, расовым и национальным признакам [1].

Экстремизм как идеология и его крайняя форма – терроризм имеют давнюю историю, но его современные формы существенно отличаются от исторических: многомиллиардным финансированием, высоким уровнем специализированной подготовки активных членов, наличием современной инфраструктуры, использованием новейших систем оружия, активным привлечением в свои круги наемников, интернациональным объемом угрозы. Необходимость координации образовательного вектора определяется уровнем идеологической обра-



ботки и вовлечённости молодёжи в экстремистские организации. Так, по данным Института стратегических и международных исследований, в рядах религиозно-экстремистских и террористических организаций находится около 300 тысяч представителей молодого поколения, не достигших 18 лет. Директор Института стратегических и международных исследований Владимир Норов подчеркнул, что проблема радикализации молодёжи проходит на фоне нерешённых социальных, культурных и нравственных вопросов [2]. По данным Брукингского института, в Твиттере может насчитываться до 90 тыс. аккаунтов, которые так или иначе связаны с ИГ («Исламское государство» - запрещённая в России организация). Каждый из них имеет в среднем по тысяче читателей. Существенная часть посетителей данных интернет-ресурсов – юноши и девушки до 18 лет [3].

Правоохранительными органами неоднократно отмечался

факт особого внимания экстремистских и террористических организаций к образовательным организациям и особенно к высшему образованию. Например, в вузах «участились попытки вербовок студенческой молодёжи в так называемое «Исламское государство» – ДАИШ, различные структуры неонацистского толка, квазирелигиозные секты», что определяется недостаточным пониманием образовательными организациями остроты данной проблемы и осуществлением конкретных направлений работы [4, с.4]. Все это происходит на фоне непрерывного роста в Российской Федерации количества зарегистрированных преступлений экстремистской направленности: в 2012 году – 696; в 2013 году – 896; в 2014 году – 1034; в 2015 году – 1308; в 2016 году увеличилось на 9,1%; в 2017 году увеличилось на 4,9 % [4].

Образовательные организации в России, высоко оценивая уровень угрозы экстремизма и терроризма, по-разному решают вопрос о противодействии.

В Мордовском государственном педагогическом институте имени М.Е. Евсевьева с 2009 года этим направлением занимается научно-исследовательская лаборатория «Научно-методическое обеспечение профилактики экстремизма и ксенофобии в системе российского образования» (руководитель НИЛ – доктор исторических наук, профессор А.В. Мартыненко). Многолетний опыт работы в области профилактики экстремистской и террористической идеологии в молодёжной среде основывается преимущественно на ценностно-ориентированном подходе. В процессе организации образовательной, научно-исследовательской и воспитательной деятельности применяются личностно-ориентированные технологии, учитывающие различные индивидуальные потребности участников и направленные на формирование религиозной и межнациональной терпимости, патриотизма и здорового образа жизни. Здесь каждое направление работы имеет равное и большое значение.

Деятельность, основанная на методе включения образовательных механизмов, должна вестись с учетом того факта, что в основе любых форм девиаций, ведущих к активной деструктивности, лежат представления об обществе, государстве и личности.

Данное представление должно формироваться в результате конструктивного взаимодействия между субъектами

непрерывного образовательного процесса (семьи, общества, государства, образовательных, научных, традиционных религиозных и иных общественных организаций, организаций культуры и спорта, СМИ, бизнес-сообществ), что и отражено в качестве приоритетного направления в Стратегии развития воспитания в Российской Федерации на период до 2025 года [5]. Учебно-методическая литература, которая используется в процессе обучения в школах и вузах, должна проходить экспертизу на экстремизм и, как предлагает глава комитета Госдумы по развитию гражданского общества, вопросам общественных и религиозных объединений Сергей Гаврилов, «экспертиза должна быть установлена законодательно» [6]. К слову, одним из первых был учебник для 8 класса средней общеобразовательной школы «Основы исламской культуры», автор которого – руководитель НИЛ МГПИ профессор А.В. Мартыненко [7]. А в 2017 году в издательстве «Юрайт» вышел учебник, рекомендованный УМО ВО «Профилактика экстремизма в молодёжной среде», разработанный сотрудниками НИЛ МГПИ, под общей редакцией профессора А.В. Мартыненко [8].

В последнее время специализированные группы и сообщества сети Интернет оказывают воздействие на подростковое мышление и мироощущение, предлагая «иной мир» взамен проблемам в семье и школе.

Часто вовлечение идет под маской игровой интриги («Розовый пони», «Синий кит», «Большая игра. Сломай систему», «Аватар»), рассчитанной на разные возрастные группы детей, при этом ставка делается на социально-психологические, физиологические и демографические особенности данной возрастной группы, наиболее восприимчивой к идеологическому воздействию и подверженной максимализму и радикальным настроениям.

В данном случае отдельные исследователи видят необходимость превенции экстремизма несовершеннолетних (А.А. Реан, Л.А. Редуш, Я.Л. Коломинский, Е.М. Дубровская) и проведения специальной коррекционной работы с «группой риска», склонной к экстремизму (Ю.М. Антонян, Е.Н. Юрасова, Т.В. Семеновских). Важным признается непрерывность превенции и учет возрастных особенностей обучающихся. Среди рекомендуемых методов эффективными признаются: метод диагностики (любая профилактическая работа должна начинаться с анализа исходной ситуации), метод кейс-стади (актуализация ценностных ориентировок посредством рассмотрения конкретных практических ситуаций), метод рефлексии (мониторинг мышлений обучаемых о своем внутреннем состоянии) [9, с. 8].

В дошкольном образовании проведение профилактических мероприятий ориентировано на

факт интенсивного формирования психики ребенка на основе предпосылок, заложенных в детстве. В этом периоде при участии взрослых, которые организуют, контролируют и оценивают поведение ребенка, игровые методы, как никакие другие, могут помочь сформировать у ребенка начальные представления об обществе, государстве и личности. Например, занятие-игра «Права сказочных героев» (за основу берутся сюжеты из книг Ш. Перро «Красная Шапочка», А. Толстого «Золотой ключик, или Приключения Буратино», русские народные сказки «Заюшкина избушка», «Гуси-лебеди», «Маша и медведь», «Три медведя» и др.). В начальном общем образовании следует обратить внимание на формирование социально значимой роли – статуса учащегося с определенным кругом прав и обязанностей.

Интеллектуально-правовая игра «Юридическая азбука» может способствовать формированию правовой культуры, развитию умения работать в группе, формированию межличностных отношений уважения и солидарности, законности как нравственной основы поведения в социальных конфликтах. Содержание игры включает в себя следующие игровые элементы:

- 1) «Имею право, но обязан»,
- 2) «Попробуй, угадай»,
- 3) «Правовые ребусы»,
- 4) «Компьютерные пазлы»,
- 5) «Детектив» и др. [10, с.112].

В основном и среднем общем образовании следует учитывать, что в возрасте от 13 до 22 лет в силу психологических и социальных факторов подростки наиболее часто попадают в поле зрения активистов экстремистских организаций. Наиболее оптимальными формами являются: тренинги, ролевые игры, конкурсы творческих работ (рисунки, стенгазеты, видеоролики, постеры и т.д.), обсуждение кинофильмов, участие в добровольных школьных обществах, тематические смены в летних лагерях.

Научно-исследовательское направление наиболее успешно реализуется в среднем и высшем профессиональном образовании, где профилактическая работа концентрируется на базе научных сообществ исследователей и в форме постоянно действующих лабораторий по изучению проблем деструктивного поведения, ведущего к экстремизму. Так, в научно-исследовательской лаборатории МГПИ представлен широкий спектр специалистов по отечественной истории (профессор Т.Д. Надькин, доценты С.С. Еремина и Н.А. Милёшина), этнологии (профессор Н.Ф. Беляева), исламоведению (профессор А.В. Мартыненко), юриспруденции (доцент Л.А. Потапова), психологии (доцент Е.В. Царева). Деятельность лаборатории отличается разноуровневым подходом к изучению проблемы деструктивного состояния молодёжи (историческим, юриди-

ческим, психологическим и т.д.) и апробацией результатов в образовательных организациях и на региональных, всероссийских и международных конференциях. Они прошли в Саранске, Казани, Санкт-Петербурге, Тюмени, Саратове, Ханты-Мансийске. Кроме того, результаты работы НИЛ получили освещение за рубежом: на конференциях в Венгрии (Н.Ф. Беляева), в Армении (Л.А. Потапова, Н.А. Милёшина), Египте, Турции, Израиле, Швейцарии (А.В. Мартыненко) [11, с. 81]. Работа с молодёжью строится путем актуализации и активизации молодёжных общественных движений, программ, конкурсов, олимпиад, дискуссионных клубов, волонтерских движений, проектов и т.д. Научные исследования на базе лаборатории показали степень важности и своевременности проводимых мероприятий [12, с. 5].

Важным направлением в работе является научно-образовательное сотрудничество с правоохранительными органами, образовательными организациями и научными центрами страны. Тесное сотрудничество в решении поставленных задач профилактики экстремизма установлено с Пензенским и Нижегородским университетами, Саратовской государственной юридической академией, Московским государственным техническим университетом имени Н.Э. Баумана. В этом ключе межвузовское взаимодействие привело к организации

ежегодного молодёжного международного форума «Мир без экстремизма», и обеспечивает наличие на форуме интересных дискуссионных площадок, обсуждение инновационных идей, обмен опытом в сфере противодействия экстремизму и терроризму.

Одно из научных направлений деятельности связано с проведением экспертизы по делам об экстремизме. Доктор исторических наук, профессор А.В. Мартыненко с 2002 г. осуществляет экспертную деятельность в рамках Сети этнологического мониторинга и раннего предупреждения конфликтов Института этнологии и антропологии РАН. Сотрудники лаборатории по запросам правоохранительных органов проводят экспертизу аудио-, видео- и печатных материалов на выявление признаков экстремизма. В качестве методики исследования используется: эмпирико-индуктивный метод анализа материалов, предположительно являющихся экстремистскими; психолингвистический и культурологические подходы к анализу исследуемых текстов; юридико-догматический подход к определению процессуального статуса эксперта (специалиста). В силу расплывчатой формулировки понятия экстремизма в Федеральном законе Российской Федерации от 25 июля 2002 года № 114-ФЗ «О противодействии экстремистской деятельности» проведение экспертизы представляет опреде-

лённые трудности. Однако члены лаборатории, проводящие экспертизу, понимают, что результативность деятельности правоохранительных органов, осуществляющих противодействие тому или иному антиобщественному и противоправному явлению, во многом зависит от их способности своевременно и четко выявить признаки экстремизма.

Сотрудничество с правоохранительными органами продолжается и в рамках реализации проектов. Таким примером является совместная реализация государственной программы Республики Мордовия «Противодействие злоупотреблению наркотиками и их незаконному обороту» на 2014-2020 годы».

В МГПИ в рамках этого сотрудничества создано и действует студенческое антинаркотическое движение – САД МГПИ. Данное направление реализуется совместно с Управлением по контролю за оборотом наркотиков МВД по Республике Мордовия и Государственным комитетом Республики Мордовия по делам молодёжи.

Воспитательная деятельность. В реализации данного направления особенно актуально сотрудничество образовательных организаций, государственных органов и институтов гражданского общества, задача которых заключается в проявлении повышенной бдительности и демонстрации активной гражданской позиции [13, с.103].

В этой связи представляется важным открытие 7 февраля 2019 года в МГПИ им. М.Е. Евсевьева Центра духовно-нравственной культуры и воспитания. Ректор МГПИ Марина Антонова отметила значение создания этого инновационного подразделения для объединения усилий представителей образовательных, религиозных, общественных организаций в деле духовно-нравственного воспитания подрастающего поколения. В работе Центра используются дискуссионные методы как основа активного обучения и воспитания. Дискуссионный клуб «Диалог конфессий» организовал работу круглого стола «Традиционные религии против экстремизма», в котором приняли участие представители Саранской епархии Мордовской митрополии РПЦ, Центрального духовного управления мусульман Республики Мордовия, ученые, преподаватели, студенты. Обсуждались вопросы, связанные с ролью традиционных конфессий в духовно-нравственном просвещении российского общества, в том числе в профилактике всех разновидностей экстремизма и ксенофобии в молодёжной среде. Участники дискуссии пришли к общему выводу о необходимости усиления сотрудничества Русской православной церкви и российской мусульманской уммы (общины) в сфере укрепления межэтнической и межконфессиональной толерантности в

России и, в частности, в Республике Мордовия.

Особого внимания заслуживает воспитательная работа со студентами-иностранцами в МГПИ им. М.Е. Евсевьева в условиях приоритетного проекта «Экспорт образования». Реализация данного проекта (с мая 2017 года по ноябрь 2025 года) направлена на повышение привлекательности российских образовательных программ для иностранных граждан на международном образовательном рынке. В результате реализации проекта количество иностранных студентов, которые обучаются по очной форме в российских вузах, должно вырасти с 220 тыс. человек в 2017 году до 710 тыс. в 2025 году. Количество иностранных школьников, прошедших обучение по программам дополнительного образования, должно вырасти в 2025 году по сравнению с 2016 годом вдвое [14]. Увеличение потока иностранных студентов (а в МГПИ – это студенты-туркмены), обладающих своеобразными этнокультурными особенностями, отличными от менталитета и стиля жизни мордвы, может привести к межэтнической разобщённости (местные жители не принимают образ жизни и культуру иностранцев, а иностранцы стремятся сохранить свою самобытность, в том числе и в условиях студенческих общежитий). Всё вышесказанное требует применения методов социализации в процессе организации комплекса воспитательных мероприятий:

а) занятия по формированию поликультурной личности (ознакомление с культурой, обычаями и традициями народов России, участие в национальных праздниках и т.п.);

б) занятия по формированию толерантности (уроки по привитию навыков позитивного диалога с окружающими);

в) занятия по формированию патриотически настроенной личности («уроки патриотизма»);

г) занятия по формированию законопослушной личности (ознакомление с основами международного и российского законодательства);

д) занятия по формированию культуры здорового образа жизни и безопасному поведению (занятия по снятию психологического напряжения, оказание медпомощи, основы этикета работы и ответственности в случае неправомерного поведения в сети Интернет).

Развитие кадрового потенциала вуза – это важнейший фактор, а для педагогического вуза ещё и развитие профессионализма тех, кто завтра будет обеспечивать формирование у обучающихся гражданской идентичности в поликультурном социуме и развитие способностей противостоять идеологии экстремизма, национализма, ксенофобии, дискриминации по социальным, религиозным, расовым и национальным признакам. Кадровое и организационное обеспечение деятельности по противодействию идеологии экстремиз-

ма и терроризма предполагает создание образовательных центров для подготовки специалистов по профилактике экстремизма в молодёжной среде, тренинги и семинары для должностных лиц, занимающихся проблемами воспитания молодёжи.

В НИЛ МГПИ им. М.Е. Евсевьева были разработаны дополнительные образовательные программы, направленные на формирование компетенций, предусмотренных Профессиональным стандартом «Педагог». С 2009 года реализуется разработанная Т.Д. Надькиным, А.В. Мартыненко и Л.А. Потаповой дополнительная образовательная программа повышения квалификации «Профилактика ксенофобии и экстремизма в образовательных учреждениях (международный и российский опыт)» [15, с. 10]. Основными методами работы НИЛ, направленными на формирование дополнительных компетенций по противодействию экстремизму в молодёжной среде, явились инструктаж, ротация, ученичество и наставничество. Членами НИЛ, доцентами Н.А. Милёшиной, А.Ю. Куприяновым и С.С. Ерёминной были разработаны учебный процесс вуза элективные курсы соответственно «Патриотическое воспитание в современной России и его роль в формировании толерантности современного общества» и «Православная культура в контексте формирования толерантности» [16, с. 93; 17, с. 88].

Второе направление работы – подготовка работников системы образования, способных сформировать у обучающихся устойчивый иммунитет к экстремистским атакам. В этом направлении активно используются проектные методы организации различных исследований и методы специальной подготовки.

Так, показателен проект «Патриотический десант», разработанный в НИЛ МГПИ доцентом С.С. Ереминой и аспирантом А.П. Чернышовым, направленный на патриотическое воспитание школьников, причем посредством студенческого наставничества. Активные участники «Патриотического десанта» разрабатывают и проводят в школах «Уроки мужества», концерты патриотической песни, квесты, нацеленные на расширение и углубление исторических знаний, формирование гражданской ответственности, патриотизма, толерантности. Особенно интересны акции – «Туристические тропы» с целью путешествия по памятным историческим местам, а также акции по ремонту памятников и уборке прилегающих территорий, встречи с ветеранами войны и членами их семей, работа со своими родословными в архивах.

Основные умения приобретаются студентами в рамках педагогической практики и внеурочной работы со школьниками. Так, с 2014 по 2016 гг.

был реализован совместный научно-исследовательский проект «Повседневность в истории», нацеленный на сбор и систематизацию исторических источников о повседневной жизни российского общества в XIX столетии, а с 2017 г. была начата реализация нового проекта «Назад в СССР», рассчитанного на 2017–2019 гг. и направленного на систематизацию и публикацию воспоминаний очевидцев о советской эпохе [18, с. 75]. Подобные проекты позволяют не только прочувствовать историю, исследовать её через чувства, эмоции, переживания, события жизни отдельного человека, но и успешно решать проблемы профилактики экстремистского поведения в молодёжной среде. Проект предполагает общение со своими родственниками – свидетелями советской эпохи, длительную и кропотливую работу по сбору и систематизации воспоминаний, создание сайта, где каждый желающий может оставить свои свидетельства. Максимальная занятость, несколько уровней взаимодействия – класс-школа-вуз-межвузовское общение, постоянные организационные встречи требуют от участников проекта большого приложения сил, но при этом оснащают новыми знаниями, опытом, пониманием жизни. Кроме того, подобные проекты позволяют выявить талантливых школьников, проявляющих высокий уровень эрудиции, организа-

ционные, лидерские качества, педагогические способности и помочь им сделать свой профессиональный выбор. Данная работа, с одной стороны, совершенствует профессиональные компетенции будущих педагогов, с другой – имеет огромное воспитательное воздействие как на школьников, так и на студентов.

Важным направлением является работа студенческих педагогических отрядов МГПИ, которые успешно функционируют в рамках организации детского отдыха и оздоровления. Периодически корпусу вожатых приходилось сталкиваться с ситуациями асоциального поведения подростков.

Так, в НИЛ МГПИ возникла идея разработки специальной программы подготовки вожатых и воспитателей для организации работы с подростками с девиантным поведением. Апробация таких смен началась в 2014 г. на базе детских оздоровительных лагерей Республики Мордовия и сразу показала высокие результаты. Обеспечив всестороннюю занятость школьников в каникулярный период, участники педагогических отрядов не только выполнили свою основную функцию, но и приобрели уникальный опыт работы с детьми девиантного поведения.

В целом, предложенные и апробированные в НИЛ «Научно-методическое обеспечение

профилактики экстремизма и ксенофобии в системе российского образования» МГПИ имени М.Е. Евсевьева методы профилактики распространения идеологии экстремизма и терроризма в молодёжной среде – это реальная возможность предотвратить распространение угрозы экстремистских течений в современном российском обществе. Эффективность достигается постоянным и систематическим взаимодействием государственных органов и институтов гражданского общества с образовательными организациями различных уровней в рамках образовательной деятельности, научно-исследовательского сотрудничества, воспитательной работы, педагогической практики и регулярным повышением квалификации педагогических кадров.

Литература:

1. Приказ Министерства образования и науки РФ от 17 мая 2012 года № 413 «Об утверждении федерального государственного образовательного стандарта среднего общего образования». URL: <http://base.garant.ru> (дата обращения: 10.01.2019).
2. Владимир Норов: идеи «просвещённого ислама» – новая модель для мусульманского мира. URL: <https://anhor.uz/society/norov> (дата обращения: 09.02.2019).
3. Европа будет блокировать аккаунты джихадистов в соцсетях. URL: <https://www.euromag.ru/articles/evropa-budet-blokirovat-akkauny-dzhihadistov-v-socsetjah/> (дата обращения: 03.02.2019).

4. Портал правовой статистики Генеральной Прокуратуры РФ. URL: <http://crimestat.ru/analytics> (дата обращения 19.12.2018).
5. Приказ Министерства образования и науки РФ от 17 февраля 2017 года № 162 «Об утверждении качественных и количественных показателей эффективности реализации Стратегии развития воспитания в Российской Федерации на период до 2025 года» URL: <http://base.garant.ru>.
6. Учебную литературу надо проверять на экстремизм. URL: <https://www.pnp.ru/social/uchebnyu-literaturu-nado-proveryat-na-kstremizm.html>
7. Мартыненко А.В. Основы исламской культуры. Учебник для 8 класса общеобразовательных учреждений. Саранск: Издательство Историко-социолог. ин-та Мордовского ун-та, 2006. 116 с.
8. Профилактика экстремизма в молодёжной среде: учебное пособие для вузов / Под общей ред. А.В. Мартыненко. М.: Юрайт, 2017. 221 с.
9. Предупреждение вовлечения молодёжи в террористические и экстремистские организации: методические рекомендации. Антитеррористический центр государств – участников СНГ. СПб.: Русь, 2016. – 64 с.
10. Левина М.А., Потапова Л.А. К вопросу об организации воспитательной работы по профилактике экстремизма в ученической среде / Мир науки и образования. 2017. № 2 (II). С. 8-12.
11. Мартыненко А.В., Надькин Т.Д. Современные вызовы Российскому государству как фактор дестабилизации регионального социума (на примере Республики Мордовия) // Известия высших учебных заведений. Поволжский регион. Гуманитарные науки. 2016. № 3. С. 81–89.
12. Потапова Л.А., Черевко Н.А. О правовых механизмах противодействия молодёжной экстремистской деструктивности в условиях образовательной организации (практика регионального вуза) // Сборник статей Международного научно-практического конкурса. Юрист года. 2017. С.112-114.
13. Потапова Л.А. Функции гражданского общества по предотвращению проявлений экстремизма в молодёжной среде // Гуманитарные науки и образование. 2011. № 3 (7). С. 102–104.
14. О приоритетном проекте «Экспорт образования» URL: <http://government.ru/info/27864/>
15. Потапова Л.А., Актуальные вопросы совершенствования законодательства в области противодействия и борьбы с экстремизмом в Российской Федерации // Гуманитарные науки и образование. 2010. № 3. С. 106–110.
16. Милёшина Н.А. Система ценностей российского дворянства XVII – XIX веков в контексте формирования нравственных приоритетов современного общества // Научные проблемы гуманитарных исследований. 2010. № 4. С. 93–101.
17. Милёшина Н.А. Традиции дворянского воспитания и формирование толерантности современной молодёжи // Вестник Чувашского университета. Сер. «Гуманитар. науки». 2009. № 1. С. 74–80.
18. Милёшина Н.А., Потапова Л.А. Сохранение культурно-исторического наследия дворянства в современной России как средство духовно-нравственного воспитания молодёжи // Гуманитарные науки и образование. 2018. № 4 (36). С. 88–94.

Реально-виртуальная воспитательная среда вуза как профилактическое средство противодействия социально-разрушающим провокациям современного общества

Сафронова Анастасия Николаевна — старший преподаватель кафедры «Экономика и экономическая безопасность», Уральский государственный лесотехнический университет, г. Екатеринбург

Молчанов Николай Алексеевич — кандидат педагогических наук, доцент кафедры «Экономика и экономическая безопасность» института экономики и управления, Уральский государственный лесотехнический университет, г. Екатеринбург

Вопрос социальной безопасности, в том числе в виртуальном пространстве сети Интернет, с каждым днем становится всё более актуальным. Связано это с быстрыми социальными изменениями в обществе, которые порождают новые опасности и угрозы, требуют их изучения и незамедлительного устранения. Студенческой молодёжи в первую очередь касаются вопросы социальной безопасности, ведь именно в студенчестве человек переживает становление социальной личности и психофизиологическую зрелость.

Мы рассматриваем проблему в рамках современного общества, которое претерпевает изменения. В настоящее время социальная активность молодё-

жи всё больше разворачивается в новой информационной среде, которой является виртуальное пространство сети Интернет. Д.В. Иванов рассматривает виртуализацию как процесс социальный, «как процесс изменения общества в целом, а не как создание «параллельного виртуального общества» [1].

Современные технологии несут в себе источник грандиозного прогресса. Они являются интегральной возможностью реализации способностей человека, могут обеспечить коммуникативное равенство, интерактивность социального обмена и др. Вместе с тем организаторы социально-разрушающих провокаций всё чаще пытаются подчинить возможности интернет-технологий своим интересам.

В общем смысле социально-разрушающей провокацией можно считать внешнее негативное влияние, направленное на разрушение социализации личности, подавление волевой сферы, эмоционального состояния, подчинение внешней силе [2].

Формирование личности студента под воздействием целенаправленных социально-разрушающих провокаций реальной и виртуальной окружающей среды мы рассматриваем как педагогическую проблему современности.

Учитывая тот факт, что виртуальное пространство сети Интернет становится неотъемлемой частью жизнедеятельности современной молодёжи, считаем необходимым создание виртуальной воспитательной среды, способствующей профилактике социально-разрушающих провокаций со временного общества на основе электронной информационно-образовательной среды вуза и сетевых социальных ресурсов.

Однако и реальная воспитательная среда должна включать набор компонентов воспитательного воздействия на молодёжь.

Таким образом, под определением реально-виртуальной воспитательной среды вуза мы понимаем воспитывающую среду, динамическим компонентом которой является виртуальная реальность единого информационного образовательного пространства, которая увлекает, охватывает молодого человека,

формирует его нравственное поведение и способствует интеграции в реальную жизнь.

Предлагаем следующую структуру модели виртуальной воспитательной среды (рисунок 1).

Структурная модель виртуальной воспитательной среды имеет внешнее и внутреннее содержание. Внешнее содержание определяет воспитательные цели, принципы, задачи, функции, условия, технологии и результат. Элементы внешнего содержания служат основой для организации модели виртуальной воспитательной среды и определены положениями информационно-средового подхода. Внутреннее содержание модели включает обучающихся и преподавателя как субъектов воспитания; взаимодействие субъектов воспитания; средства коммуникации, методику воспитания. Внутренние элементы являются обеспечивающими функционирование модели виртуальной воспитательной среды.

Воспитательная профилактическая деятельность в виртуальной среде может обеспечиваться такими информационными ресурсами, как официальный сайт вуза, социальные сети, электронная почта и т.п.

Функциональная составляющая заключается в обеспечении воспитательной деятельности в виртуальной среде продуктивным содержанием при использовании современных информационных технологий. Реализуется воспитательная деятельность воспитательной методикой.



Субъектами взаимодействия в предложенной модели являются обучающиеся и преподаватель. Взаимодействие субъектов обеспечивается активным включением в воспитательный процесс на основе субъект-субъектных отношений, что отражает:

- осознание личной причастности субъекта к профилактической деятельности по противодействию социально-разрушающим провокациям современного общества;
- понимание воспитательной профилактической деятельности как совместной для достижения общей цели;
- партнерские отношения между субъектами воспитательной профилактической деятельности.

Следуя основам субъект-субъектных отношений, деятельность

преподавателя и студентов основана именно на постоянном взаимодействии.

Организация виртуальной воспитательной среды вуза предполагает использование информационных технологий в интеграции с традиционными подходами к воспитанию.

Информационно-коммуникативными методами в виртуальной воспитательной среде могут быть такие, как проблемное обсуждение ситуации, онлайн-брифинг, веб-конференция. Указанные методы проводятся в форме чата [3].

Используя чат, предлагается применять метод проблемного обсуждения ситуации. Проблемное обсуждение ситуации как метод воспитательного взаимодействия запускает мыслительный процесс участников и способ-

Рис. 1. Структура модели виртуальной воспитательной среды

ствуется побуждению желания выйти из заданной ситуации и снять противоречие. В проблемной ситуации важно сформулировать задание для участников процесса для исследования пути её решения [4]. В нашем случае указанный метод позволяет побудить студента к самостоятельному рассуждению, обмену мнениями, активному поиску ответа на конкретные вопросы по проблеме противодействия социально-разрушающим провокациям современного общества.

С целью внедрения предложенной модели реально-виртуальной воспитательной среды вуза со студентами Уральского государственного лесотехнического университета (далее – УГЛТУ) проводились воспитательные мероприятия, которые включали активные коммуникативные методы с применением современных информационных технологий [5].

Одной из воспитательных технологий виртуального пространства по противодействию социально-разрушающим провокациям современного общества является создание блока инновационной воспитательной деятельности на площадке официального сайта УГЛТУ [6].

Идее создания указанного блока послужила разработка онлайн-квеста для студенческой молодёжи по определению подверженности к социально-разрушающим провокациям современного общества. Онлайн-квест – это проблемные задания с элементами ролевой игры, для вы-

полнения которого используются ресурсы сети Интернет [7]. Студентам предлагается пройти поэтапно несколько заданий, в результате чего они получают данные с показателями подверженности к социально-разрушающим провокациям современного общества.

Студент знакомится с информацией по заданной тематике, после чего переходит к выполнению заданий. Для выполнения заданий необходимо заполнить поля регистрации для фиксации участия в онлайн-квесте конкретного студента. Отметив все пункты, студент получает результат своего уровня подверженности конкретной провокации. После прохождения одного задания студент переходит к следующему. Всего представлено четыре задания по темам алкоголизма, наркомании, терроризма и сектантства.

Информация о социально-разрушающих провокациях подбрана таким образом, чтобы она помогла студенту задуматься о важности и сложности указанного явления. Стиль текста подбирался с учетом таких факторов, как доступность, легкость восприятия, актуальность для возрастных особенностей. В материалах использовались высказывания специалистов в конкретной области проблемы, цитаты, иллюстрации.

Перед началом онлайн-квеста студентов проинструктировали по прохождению заданий, мотивировали на получение личностного результата по приобретению навыков противодействия социально-разруша-

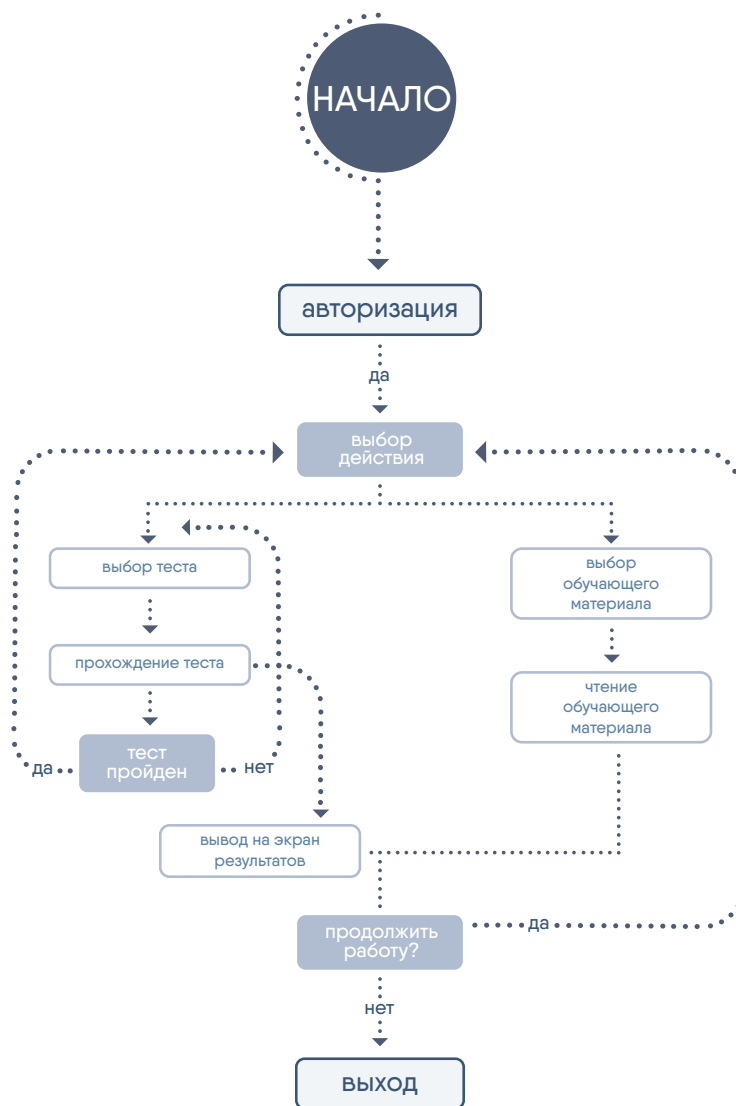


Рисунок 2. Схема выполнения онлайн-квеста по определению подверженности к социально-разрушающим провокациям современного общества.

ющим провокациям в условиях современного информационного общества. На рисунке 2 представлена схема выполнения онлайн-квеста.

Онлайн-квест является методом формирования поведенческого компонента, в результате которого студент должен уметь составлять алгоритм действий

при столкновении с социально-разрушающей провокацией.

Считаем, что данная форма виртуального воздействия имеет воспитательную направленность и формирует у студенческой молодёжи твердую социально-активную позицию, развивает ценностные отношения к себе и своим товарищам.

Организация реально-виртуальной воспитательной среды вуза требует информационно-ресурсного обеспечения, что позволит оптимизировать исследуемое явление за счет активизации участия студенческой молодёжи в разных видах воспитательной деятельности. В первую очередь это связано с развитием материально-технического оснащения образовательного пространства вуза, что предполагает широкое использование интернет-технологий.

Наше внимание к данному аспекту воспитательного процесса связано со следующими факторами:

- оснащённостью средствами информационно-коммуникационных технологий (далее – ИКТ) и обеспечением всем участникам эксперимента доступа к сетевым ресурсам в ходе проведения мероприятий;

- владением средствами ИКТ со стороны студенческой молодёжи (требование ФГОС);

- обеспечением всех участников инструкцией пользования средствами виртуальной воспитательной среды вуза;

- обеспечением обучения студенческой молодёжи использованием средствами воспитательной виртуальной среды вуза.

Реальная среда может обеспечиваться традиционными методами воспитания и осуществляться во взаимодействии со студенческими организациями, деятельность которых направлена на развитие здорового образа жизни, правовую и социальную ответственность, развитие спорта, культуры.

Литература:

1. Иванов Д.В. Виртуализация общества. - СПб.: «Петербургское Востоковедение», 2000. - 96 с.

2. Сафронова А.Н., Вербицкая Н.О., Молчанов Н.А. Формирование готовности обучающихся молодых людей к противодействию социально-разрушающим влияниям в воспитательном процессе современного вуза // Современные проблемы науки и образования. – 2016. – № 6.; URL: <https://scienceeducation.ru/ru/article/view?id=25610> (дата обращения 11.01.2019).

3. Шевелев Н.А., Кузнецова Т.А. Дистанционные образовательные технологии как инструмент индивидуализации обучения // Высшее образование в России. 2008. №8. С. 55-58.

4. Абрамова, И.Г. Активные методы обучения в системе высшего образования. / И.Г. Абрамова - М.: Гардарики, 2008. - 368 с.

5. Сафронова А.Н. Теория и методика формирования социально значимых навыков самосохранения здоровья у студенческой молодёжи в условиях реально-виртуальной воспитательной среды вуза // Современные проблемы науки и образования. – 2018. – № 5.; URL: <http://www.scienceeducation.ru/article/view?id=28179> (дата обращения: 22.11.2018).

6. Официальный сайт УГЛТУ. / Основные сведения об Уральском государственном лесотехническом университете. [Электронный ресурс] - режим доступа: <http://www.usfeu.ru/universitet.html>.

7. Лехмус М.Ю. Представление методического материала на тему: «WEB-квесты в учебном процессе». – М.: Прометей, 2018. – 32 с.

Использование персональных данных в самопрезентации личности (старшего поколения) в социальных сетях

Ивченко Алиса Александровна — бакалавр Южного федерального университета, г. Ростов-на-Дону

Кадиева Дарья Руслановна — бакалавр Южного федерального университета, г. Ростов-на-Дону

Конивцова Анастасия Михайловна — бакалавр Южного федерального университета, г. Ростов-на-Дону

Плясова Анастасия Владимировна — бакалавр Южного федерального университета, г. Ростов-на-Дону

Саркисян Нелли Леоновна — бакалавр Южного федерального университета, г. Ростов-на-Дону

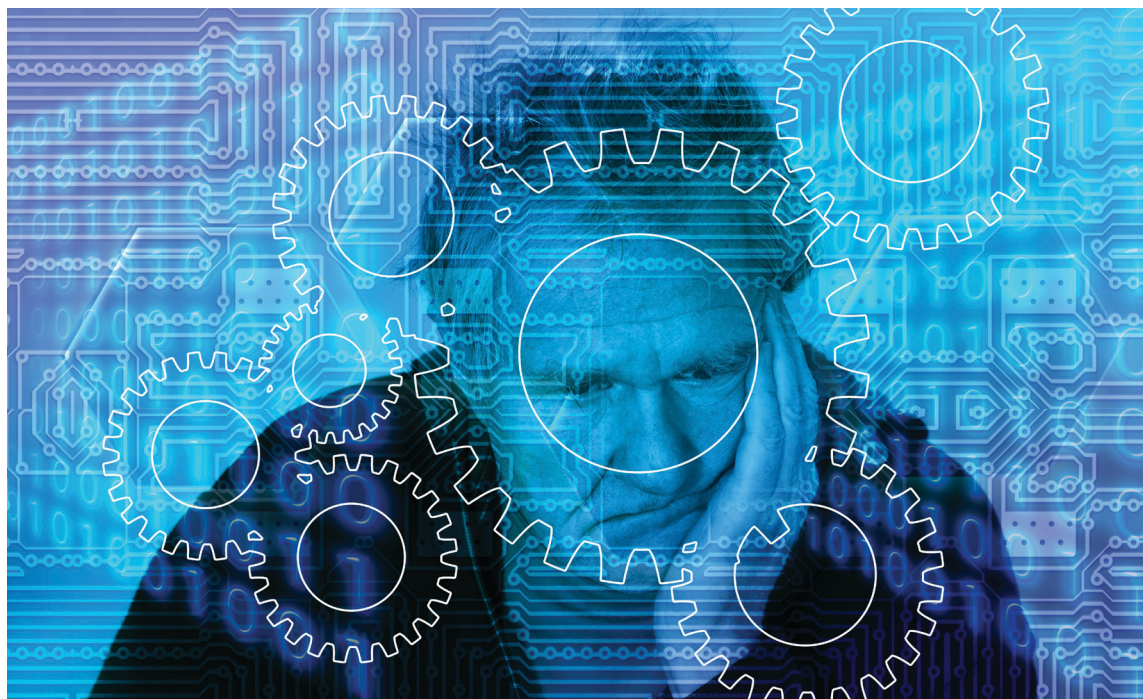
В последнее десятилетие интернет и социальные сети развиваются быстрыми темпами. Создавая личные страницы на различных ресурсах, пользователи не только формируют сообщества внутри них, общаются, обмениваются информацией, но также вынуждены презентовать себя.

Информационное пространство социальных сетей в своем виртуальном выражении является вербальным, в нем в виде опосредованной самопрезента-

ции личности на первый план выходят самоописания, самохарактеристики личных страниц и так далее.

Цель данного исследования заключается в изучении поведения старшего поколения в социальных сетях при самопрезентации их персональных данных.

Нами была выдвинута гипотеза о том, что старшее поколение не в полной мере осознаёт важность грамотного размещения персональных данных



в процессе самопрезентации в социальных сетях.

В интервью, проведённом в рамках данного исследования, принимали участие шесть человек: пять женщин и один мужчина. Все респонденты выделялись по следующим критериям: возраст более 40 лет и использование социальных сетей.

Все опрошенные заявили, что являются пользователями не только социальных сетей, но и интернета в целом. В ответе на вопрос о том, какие социальные сети они используют, респонденты отметили широкий спектр социальных сетей, которыми пользуются. Лидером является социальная сеть «Одноклассники», ею поль-

зуются пять респондентов из шести.

Следующей по популярности социальной сетью является WhatsApp (хотя фактически это не социальная сеть, а мессенджер, но в условиях данного исследования нами принято решение называть WhatsApp и Viber социальными сетями), ей отдают предпочтение три человека из опрошенной группы. Социальной сетью «ВКонтакте» также пользуются три человека. Наряду с WhatsApp, респонденты упоминают также Viber, но пользуются им только два человека из шести.

Социальные сети «Мой Мир», Facebook и Instagram в интервью упоминались по одному разу каждая, что указывает на низкую

пользовательскую заинтересованность ими.

Опрошенные указали, что регистрируются в социальных сетях в основном для общения с родственниками, друзьями и знакомыми, также для того, чтобы узнавать актуальную информацию о событиях, происходящих в жизни родственников, друзей и знакомых. Респонденты пользуются социальными сетями для установления контакта с теми людьми, с которыми они были знакомы когда-то, но потеряли связь.

Несмотря на то, что изначально респонденты регистрируются для общения, они находят и другие способы применения социальных сетей. Например, для поиска информации в тематических группах. Также опрошенные утверждают, что играют в игры в социальных сетях, таким образом «убивая» свободное время. Один из респондентов утверждает, что пользуется социальными сетями в основном по работе, при этом всё же уточняет, что ищет там информацию и может «утонуть» в социальных сетях на долгое время.

Подавляющее большинство респондентов (четверо из шести) при регистрации в социальных сетях попросили помощи у своих родственников: детей или внуков. При этом только двое прошли регистрацию самостоятельно, один из них отмечает, что регистрация заняла у него продолжительное время, то есть вызвала небольшие затруднения.

Все опрошенные отмечают, что по мере знакомства с социальными сетями лучше могут в них ориентироваться. Если регистрироваться впервые им помогли, то в других социальных сетях они завели профиль самостоятельно.

Нельзя дать однозначную оценку паролям респондентов от их страниц в социальных сетях. Трое указывают, что установили несложные пароли. При этом респондент делится конфиденциальной информацией: «У меня, по-моему, стоит номер телефона, что в логине, то и в пароле», - Руслан, 45 лет. Это показывает, что ему не столь важно, взломают его страницу или нет.

Есть и категория людей, старающихся себя обезопасить: они задают пароли, значение которых понятно только им: к примеру, значимые даты, марка первой машины (Светлана, 42 года), особенный набор букв, цифр, понятный только конкретному человеку (Надежда Михайловна, 67 лет).

Та же динамика прослеживается и с указанием своего номера телефона при регистрации. Половину опрошенных этот факт не смутил. Другая половина респондентов нашла в этом возможность для дальнейших мошеннических операций. Респонденты считают, что ввод номера телефона в социальной сети является «каплей в море наших персональных данных» (цитата одного из опрошенных).

Суммируя ответы респондентов на вопрос о том, сколько времени они проводят в соцсетях, можно сказать, что они отдают социальным сетям столько времени, сколько позволяет повседневная загруженность. Работающие люди не отвлекаются на социальные сети в рабочее время, но, если есть свободная минута, они могут уделить её социальным сетям. Старшее поколение не затянато во «всемирную паутину», а рационально подходит к расстановке приоритетов и не ставит нахождение в социальных сетях на первое место.

На вопрос о том, чем респонденты занимаются в социальных сетях, получен широкий спектр ответов. Связано это, прежде всего, с тем, что в настоящее время социальные сети предоставляют широкие возможности для пользователей:

1. В социальных сетях респонденты чаще всего смотрят новости и другую информацию (пятеро) и новости своих друзей (двое).

2. Респонденты прибегают к традиционной функции социальных сетей: четыре респондента общаются с друзьями и родственниками.

3. Два респондента просматривают кулинарные рецепты.

4. Как средство снятия напряжения через игры и смешные видео социальные сети используются двумя респондентами.

5. Работают через социальные сети два респондента.

6. Рубрикой «бесплатные объявления» пользуется один респондент.

7. Просмотр фильмов и прослушивание музыки также находит своё место во время нахождения респондента в социальных сетях. Один респондент указал это в своих ответах.

Ответы на вопрос о скрытии своего аккаунта в социальных сетях разделились среди респондентов. Скрытие профиля в сети объяснялось желанием спрятать личную информацию от чужих глаз, чтобы её могли видеть только те, с кем общается респондент лично. Аккаунт может быть открыт, но в нём не так много информации.

Респонденты сталкивались с личными оскорблениями в сети Интернет, некоторые вынуждены были закрыть свои странички. Чтобы избежать нежелательного общения, респонденты прибегают к смене настоящей фамилии в сети, желая скрыться от навязчивых людей. «Столкнувшись в очередной раз с проблемой «лишних глаз», решила изменить фамилию, чтобы сохранить личное пространство и пользоваться социальными сетями в своё удовольствие», - Светлана, 42 года.

Что касается размещения фотографий в социальных сетях, можно утверждать, что особой угрозы респонденты в этом не видят. Примечательно, что даже у респондентов с закрытым профилем размещена



личная фотография. «У меня стоят мои фотографии, и я не вижу в этом ничего плохого», - Светлана, 42 года.

По мнению респондентов, персональные данные запрашиваются везде и уже не являются секретом. Как правило, они вводят все данные, которые требуются при регистрации. Со временем некоторые убрали личные данные из профиля, либо раскрыли только общую информацию (место обучения, город проживания). «Изначально, при регистрации, я указала практически всё, что предлагалось: и возраст, и город, и место учебы и работы, сейчас же никакой личной информации в моих профилях нет», - Светлана, 42 года.

Что касается характера загруженных фотографий, у взрослой аудитории преобладают семейные снимки. У некоторых пользователей они скрыты, и могут быть доступны только друзьям: «В свободном доступе несколько моих личных фотографий. А фото детей, семьи – в закрытых альбомах, доступны только друзьям», - Арина Вячеславовна, 43 года.

Респонденты размещают мало фотографий в социальных сетях: «Я человек консервативный, мало фотографируюсь, тем более не выкладываю на всеобщее обозрение свои фотографии», - Руслан, 45 лет.

Про отметку геолокации большинство опрошенных не знают и, соответственно, такой функцией не пользуются.

Многие респонденты имеют небольшое количество подписчиков: это, в основном, коллеги по работе, родственники и друзья. По поводу подписки незнакомых людей на свою страницу практически все выразились резко негативно. «Считаю это праздным любопытством, особенно если мы не очень близко знакомы», - Светлана, 42 года. В основном взрослое поколение не понимает, зачем подписываться на людей, с которыми они не знакомы лично.

Все опрошенные среди признаков «активного пользователя социальных сетей» выделяют такой критерий, как «большая продолжительность нахождения в сети». При этом никто не может отнести себя к числу таких пользователей.

«...Активный пользователь – это тот, кто не может без социальных сетей, постоянно в них «зависает», - Надежда Михайловна, 67 лет.

Все респонденты выходят на контакт с другими людьми посредством социальных сетей, но не постоянно, а по необходимости. Это объясняется недостаточным количеством свободного времени у респондентов (двое из шести ведут домашнее хозяйство, остальные работают).

В отношении лайков, комментариев и репостов мнения разделились. Ответы респондентов можно разделить на три группы:

1. «Я в этом плане немного лентяй»: респондентам проще

«лайкнуть» фото, нежели что-то писать самостоятельно;

2. «Я стараюсь»: респонденты оценивают труд других людей (особенно, креативность) посредством лайков, подбадривания, похвалы, репосты бывают редко, лайки – постоянно;

3. Если очень затронет»: пользователи оценивают публикации не часто, только если что-то очень понравится, репостов не делают.

Ответы на вопрос о возможности использования личной страницы в коммерческих целях можно разделить на две категории:

1. «Не хватило фантазии»: не задумывались об извлечении выгоды посредством ведения страницы в социальных сетях;

2. «Хочу, хочу, но руки не доходят»: задумываются об извлечении выгоды, практически это так и не осуществили. Среди причин выделяют лень, неуверенность в товаре, стеснение.

Отношение к покупкам в интернете негативное: пятеро из шести респондентов этим не пользуются и не планируют производить покупки через социальные сети, привязывать карту к аккаунту или заказывать доставку товаров. Среди мер предосторожности выделяют: покупку через проверенные магазины, отзывы знакомых.

Старшее поколение чаще всего использует мобильный телефон для выхода в социальные сети в сравнении с другими видами гаджетов, что можно объяснить желанием подстра-

иваться под существующие достижения прогресса: «Чаще я это делаю с мобильного телефона. Раньше у меня в приоритете был компьютер, но теперь у меня телефон. Он всегда под рукой, это очень удобно», - Надежда Михайловна, 67 лет. Ноутбуком и стационарным компьютером респонденты, как правило, пользуются дома.

Посещая различные странички социальных сетей или просматривая личные блоги, респонденты не задумываются о безопасности своих персональных данных: «...можно сказать, я не принимаю никаких мер безопасности, потому что не задумывалась о возможности взлома камеры именно моего компьютера», - Светлана, 42 года.

В силу недостаточного объема знаний о новейших видах техники и их функционале, респонденты не подозревают о возможных угрозах для их персональных данных.

Размышляя о мерах предосторожности при выходе в интернет с переносных устройств, мы задали респондентам вопрос о подключении к общественным точкам доступа Wi-Fi. Большинство ответивших используют мобильный интернет и просто не знают о том, что существуют способы подсоединения к сетям в публичных местах. Некоторые респонденты при поездках за границу всё-таки пользуются общественным Wi-Fi.

Несмотря на то, что старшее поколение не предпринимает

никаких мер осторожности при выходе в сеть Интернет, они всё же задумываются о том, что их персональной информацией могут воспользоваться злоумышленники.

Надо отметить, что случаи взлома страниц в аккаунтах респондентов были. Важным является то, что после получения негативного опыта респонденты желают обезопасить себя и свои данные, но иногда не знают, какие существуют способы для этого: «А как защищать страницу, я, честно говоря, не знаю. Какие есть возможности защиты страницы?», - Арина Вячеславовна, 43 года.

В первую очередь, респонденты определяют «персональные данные», как имя, дату рождения человека и документы, удостоверяющие его личность. Кроме того, персональными данными опрошенные считают характеристику индивида как единицы в обществе со своими увлечениями, предпочтениями.

Чтобы проанализировать детали исследования и его результаты, было решено провести сравнение со сторонними исследованиями.

В 2015 году в г. Абакане было опрошено 20 пенсионеров, зарегистрированных в социальных сетях [2]. Это исследование подтверждает полученные нами результаты: в большинстве своем респондентам в регистрации помогли дети или внуки, по причине их малой осведомлённости в информационных техно-

логиях. Основными причинами регистрации для старшего поколения (в исследовании 2015 года) в социальных сетях являются общение и любопытство, а также поиск свежей информации. Те же выводы можно сделать и на основе нашего исследования.

Для опрошенных в г. Абакане социальные сети – это источник актуальной информации (40%), способ общения с людьми и свободное времяпрепровождение (по 30%). В нашем исследовании опрошенные ставят на первое место общение, а уже потом получение информации, её поиск и свободное времяпрепровождение.

К негативным аспектам виртуального общения респонденты из г. Абакана отнесли тот факт, что это занимает слишком много времени и вызывает зависимость. Наше исследование не выявило факта зависимости респондентов от социальных сетей.

В исследовании Е.Ю. Крылова [1] прослеживались некоторые черты, характерные и для нашего исследования, например, анонимность участников коммуникаций, что актуально и для нашей группы респондентов, потому что опрошенные тщательно следят за своей анонимностью, скрывают аккаунт от посторонних людей, а в некоторых случаях даже скрывают свою настоящую фамилию.

Подводя итоги, можно сделать ряд выводов. «Однокласс-

ники» и WhatsApp лидируют по количеству зарегистрированных в них респондентов, почти все опрошенные освоили известные социальные сети Интернет: Viber, «ВКонтакте», «Мой Мир», Facebook, Instagram. Они регистрируются в социальных сетях в основном для общения с родственниками, друзьями и знакомыми. Также для того, чтобы узнавать актуальную информацию о событиях, которые происходят в жизни родственников, друзей и знакомых. С регистрацией в социальных сетях старшему поколению помогает молодёжь – их дети или внуки. Связано это, в первую очередь, с тем, что старшее поколение хуже ориентируется в информационных технологиях.

Половина опрошенных респондентов не придает значения паролем, выбирают очень простые, в то время как другая половина заботится об этом и устанавливает пароли, которые могли бы обезопасить их от взлома. Запрос телефонного номера смутил половину опрошенных респондентов, в то время как другая половина спокойно предоставляет эту информацию. Социальные сети не являются приоритетным занятием в жизни старшего поколения.

В ходе исследования было выявлено, что старшее поколение предпочитает закрывать свой аккаунт, так как опасается того, что его могут увидеть посторонние люди и использо-



вать информацию в своих целях.

По поводу размещения личных фотографий взрослые люди отзываются нейтрально. Многие не видят в этом ничего плохого, так как в основном их могут увидеть только близкие люди. Взрослые респонденты не заинтересованы в презентации личных фотографий, предпочитая выкладывать фото с семьёй.

Каждый из опрошенных так или иначе задумывался о том, что злоумышленники могут завладеть их личными данными, поэтому они хотели бы оградить себя от нежелательного воздействия, но не всегда знают, как этого достигнуть.

Подводя итоги вышеизложенного, можно смело утверждать, что пользование социальными сетями не является главной целью в жизни старшего поколения. Эта возрастная категория не одержима постоянным присутствием в социальных сетях в режиме online. Вместе с тем, нельзя отрицать факт прочного вхождения информационных технологий в

жизнь старшего поколения. Они, как и другие возрастные группы, стараются презентовать себя в сети Интернет.

Информатизация и компьютеризация охватывает все слои населения, старшее поколение также находится под влиянием этих нововведений. Однако в силу своего возраста и зачастую отсутствия знаний в данной области, старшее поколение не всегда осознаёт важность защиты своих персональных данных в социальных сетях, что демонстрируют ответы респондентов проведённого исследования. Поэтому можно говорить о полном подтверждении гипотезы данного исследования.

Литература:

1. Крылов Е.Ю. Формирование тактик целенаправленной самопрезентации у студентов в виртуальной среде: автореф. дис. канд. психол. наук. СПб., 2012. 144 с.
2. Миллер О.В. Социальные сети как способ решения проблемы одиночества пожилых людей //Иновационная наука. 2015. № 7-2. С. 157-158.

Нечёткое хэширование в задачах информационной безопасности

Тюрин Кай Андреевич – заместитель заведующего лабораторией ФГАНУ НИИ
«Спецвузавтоматика»

Хэширование (англ. hashing) – преобразование массива входных данных произвольной длины в (выходную) битовую строку установленной длины, выполняемое определённым алгоритмом. Функция, воплощающая алгоритм и выполняющая преобразование, называется «хэш-функцией» или «функцией свёртки» (<https://ru.wikipedia.org/wiki/Хэширование>).

В ходе решения множества прикладных задач возникает необходимость обработки большого количества файлов и данных различного формата. Такие задачи возникают, например, в ходе проведения криминалистических расследований (в том числе инцидентов информационной безопасности), а также при анализе компьютера на предмет наличия вредоносного программного обеспечения.

Одной из типовых задач является определение схожести файлов. Так, известные криптографические хэши (MD5, SHA 1 и т. д.),

а также классические контрольные суммы (CRC и т. д.) облегчают задачу нахождения одинаковых файлов. Так, достаточно один раз посчитать хэш-функцию от файла, чтобы в дальнейшем быстро обнаруживать идентичные ему. При этом нет необходимости проводить побайтовое сравнение, достаточно посчитать хэш от проверяемого файла, сохранить результат в соответствующей базе данных, имеющей относительно небольшой объем, и сравнить его с исходным. При равенстве хэшей с некоторой степенью уверенности можно судить об идентичности файлов, в зависимости от значения уровня коллизий (collision rate [1]) конкретной хэш-функции.

Тем не менее, достаточно незначительно изменить некоторый файл для того, чтобы сильно изменить значение хэш-функции, вычисляемой от него. Эта проблема имеет ещё большую значимость при решении задач поиска вредоносного программного обеспечения, т.к. его авто-



ры используют обфускаторы, меняющие содержимое файлов, а любое такое преобразование приведет к изменению значения хэш-функции.

Этот факт происходит непосредственно из свойств хэш-функции, в частности, из свойства «лавинного эффекта» [1], согласно которому при незначительном изменении входных данных результат хэш-функции значительно изменится. Следовательно, если цель злоумышленника – избежать обнаружения при помощи криптографических хэшей, ему достаточно произвести незначительные изменения вредоносного файла.

Несмотря на это, криптографические хэш-функции повсеместно используются в том числе и для задач обнаружения вредоносного ПО, так как являются чрезвычайно простым и «дешёвым» (в том числе по времени и затратам вычислительных ресурсов) для реализации методом. Так, достаточно посчитать хэш-функцию от одного из экземпляров вредоносного

ПО, после чего все идентичные экземпляры могут быть обнаружены без сложного анализа, лишь за время вычисления хэш-функции.

Стоит отметить, что использование хэширования для обнаружения вредоносных файлов заключается не только в хэшировании всего файла целиком. Так, для обнаружения может быть вычислен хэш от части файла (например, хэш от секции ресурсов или кода), что позволяет обнаружить и обфусцированный код, для чего аналитики выявляют отдельные сигнатуры исполнимых файлов, не изменяемые при обфускации, но характерные для данного семейства вредоносных программ, и считают значения хэш-функций от них.

Кроме того, так как хэш-функции требуют полного совпадения для того, чтобы свидетельствовать об идентичности файлов, а также имеют фиксированную короткую длину, простой является задача организации базы данных хэшей с быстрой операцией проверки

наличия в ней определенного вновь вычисленного хэша. Например, такая компактная база может хранить информацию о тысячах семейств вредоносных программ и позволит осуществлять быстрый поиск по ней.

В то же время остаётся проблема идентификации схожих, но не идентичных файлов. Так, если некоторый экземпляр вредоносного ПО был незначительно изменён для того, чтобы избавиться его от наличия сигнатуры, при помощи которой он может быть обнаружен, большая часть файла останется неизменной.

Данная задача особенно актуальна в современных условиях, когда злоумышленники активно противостоят эффективному методу обнаружения с использованием статистических сигнатур, используя обфускаторы, позволяющие изменить заранее не известную или сложно идентифицируемую аналитиком часть кода, таким образом, не давая возможности описать эту сигнатуру.

В этом случае существует востребованность в наличии метода идентификации таких «схожих файлов». Важно оговориться, что в данном контексте не существует строгого определения «схожести» файлов, и в зависимости от ситуации она может трактоваться по-разному, соответственно, существуют различные пути решения данной задачи. Анализ их по-

священа настоящая работа. В разное время предлагались различные решения задачи определения схожести. В качестве примеров можно привести Коэффициент Жаккара [2] и отпечаток Рабина [3]. Решению этой же задачи служат и нечёткие хэш-функции.

Нечёткие хэш-функции

Аналогично хэш-функциям, нечёткие хэш-функции являются инъективным отображением из множества массивов бинарных данных любого размера в строку определенной длины. Однако, если хэш-функции строятся исходя из требований значительно менять своё значение при незначительном изменении, то нечёткая хэш-функция, наоборот, незначительно меняет своё значение пропорционально объёму изменений в исходных данных. Таким образом, разница между двумя значениями нечётких хэш-функций является метрикой для разницы между соответствующими бинарными данными.

Нечёткие хэш-функции используются в различных задачах: при анализе схожести образцов текста, спам-фильтрах, поиске вредоносных программ и т. п. В зависимости от задач, которые они решают, существуют различные виды нечётких хэш-функций, и различные алгоритмы их реализации. Разные источники предлагают разные способы классификации нечёт-

ких хэшей. Одной из основных классификаций является разделение нечётких хэшей на следующие группы:

- кусочное хэширование (Piecewise hashing);
- контекстно-побуждаемое кусочное хэширование (Context-triggered piecewise hashing);
- выделение статистически маловероятных особенностей (Statistically improbable features);
- алгоритмы блочного перестроения (Block-based rebuilding);
- статистические отпечатки.

Эта классификация основана на деталях работы каждого алгоритма.

Существует также классификация нечётких хэшей по типу информации, используемой для вычисления:

- побайтовые (bytewise) – алгоритм взаимодействует с входными данными исключительно как с потоком байт;
- синтаксические (syntactic) – алгоритм знает синтаксис файла и использует его при хэшировании;
- семантические (semantic) – алгоритм может интерпретировать файл на более высоком уровне, используя смысловые составляющие его частей для хэширования.

Такая классификация позволяет оценивать универсальность/специфичность хэшей, входящих в тот или иной класс.

Далее мы рассмотрим классификацию нечётких хэш-функций, основанную на уровне сложности анализа

связи между блоками исходных данных и контекстной зависимости алгоритма расчета функции от исходных данных. На основе полученной классификации делается вывод о перспективных направлениях для создания новых нечётких хэш-функций.

Кусочное хэширование

Первым типом нечётких хэшей являются алгоритмы кусочного хэширования (piecewise hashing). Данный тип имеет двух основных представителей: ddcfld [4] и md5bloom [5].

Утилита ddcfld

Утилита командной строки под названием ddcfld является расширением утилиты dd (программа, используемая в системах семейства UNIX для побайтовой работы с данными), предназначенным для работы в компьютерной криминалистике. Одной из решаемых этим расширением задач является обнаружение изменений данных, содержащихся на каком-либо носителе. При этом используется низкоуровневый подход: изменения фиксируются на уровне организации данных ниже файловой системы, то есть на уровне носителя.

Так, пространство жёсткого диска разбивается на участки фиксированного размера (размер участков указывается пользователем). Каждый по-

лученный участок хэшируется при помощи одного из доступных алгоритмов (поддерживаются md5, sha1, sha256, sha384 и sha512). Данная операция может быть повторена через некоторое время. Хэши, полученные в первом случае, сравниваются с хэшами, полученными во втором случае. Несовпадение хэшей означает изменение соответствующего участка памяти.

Этот подход является эффективным для задачи обнаружения изменений в большом объёме данных, так как позволяет не хранить его полностью (что сильно сокращает объём данных, необходимых для хранения), при этом остаётся также эффективным с точки зрения скорости работы. Длина хэша является пропорциональной размеру файла и зависит от длины блока.

Утилита md5bloom

Данная утилита разработана в 2006 году командой исследователей из Новорлеанского университета. В оригинальной статье указано два основных направления использования:

1. установление связи между несколькими целями расследования, заключающееся в поиске среди множества изображений наиболее похожего (или непо похожего) на некоторое целевое;

2. обнаружение версионирования объекта, заключающееся в обнаружении файла несмотря на то, что он был изменён

(например, обнаружение исполняемых файлов некоторого программного обеспечения не смотря на обновления).

Входными данными для утилиты, помимо потока байт для хэширования, являются следующие значения:

- k – количество частей, на которые будет разделён каждый хэш;
- l – число, определяющее размер фильтров Блума;
- r – максимальное количество хранимых элементов для одного фильтра Блума;
- размер блоков, на которые делится входной поток.

Механизм работы хэша во многом схож с defltd. Так, входной поток разделяется на блоки фиксированного размера, от каждого блока вычисляется хэш MD5. Однако, вместо того, чтобы сохранять этот хэш целиком, md5bloom разделяет его на k подхэшей, каждый из которых добавляется в фильтр Блума размера $2l$ бит. Если количество занесённых в фильтр Блума значений достигает r , он конкатенируется к текущему значению хэша, после чего новые значения добавляются в новый фильтр Блума. Сравнение производится путём побитового сопоставления фильтров Блума.

Контекстно-побуждаемое кусочное хэширование

Исторически первым типом алгоритмов, по-настоящему отнесённых к классу нечётких

хэшей, является контекстно-побуждаемое кусочное хэширование (Contex-Triggered Piecewise Hashing, СТРН).

Алгоритмы этого класса обладают следующими свойствами:

1. результирующий хэш является последовательной конкатенацией хэшей «кусков», то есть участков входных данных;
2. разделение файла на «куски» зависит от его содержимого.

Таким образом, данный класс нечёткого хэширования образуется от кусочного хэширования, однако расширяет эту концепцию при помощи разделения файла на куски на основе его содержимого.

Это связано с тем, что кусочное хэширование имеет один серьёзный недостаток: при изменении входных данных не путём изменения значения определённых байтов, но путём добавления или удаления каких-либо новых участков, из-за сдвига изменятся все кусочные хэши, входящие в состав результирующего. Чтобы устранить эту проблему, была выдвинута идея изменить способ разделения данных на хэшируемые участки. СТРН в качестве такого решения предлагает некоторым образом анализировать содержимое и проводить границу определённого участка при появлении определённого «триггера», то есть срабатывании некоторого условия, зависящего от данных.

Разделение входных данных

на участки в зависимости от содержимого даёт дополнительную гибкость и устойчивость результирующего хэша к изменениям входных данных.

Алгоритм ssdeep

Является не только первым алгоритмом указанного типа, но и традиционно считается первым нечётким хэшем. Одновременно с этим данный алгоритм является первым алгоритмом нечёткого хэширования, получившим широкое распространение при решении задач информационной безопасности, помимо обнаружения спам-сообщений.

Алгоритм ssdeep разработан Джесси Корнблумом [6] с целью использования в компьютерной криминалистике. Основан на алгоритме spamsum за авторством Эндрю Триджелла [7]. Изначально разработанный для обнаружения спама, алгоритм был адаптирован для использования против файлов любого типа.

Алгоритм использует скользящее окно байт для вычисления кольцевого хэша. Такой тип хэша был выбран с целью обеспечения большей производительности, так как он позволяет быстро получить хэш следующего окна, если известен хэш предыдущего. Байты, через которые проходит скользящее окно, добавляются в некоторый буфер, представляющий очередной «кусок». Далее, когда очередное значе-

ние кольцевого хэша удовлетворяет условию, срабатывает триггер к хэшированию текущего буфера. Буфер хэшируется при помощи некриптографического хэша FNV [8]. Младшие 6 бит получившегося хэша переводятся в кодировку base64 и добавляются к результирующему хэшу.

Одним из важных ограничений ssdeer является то, что сравнивать хэши от двух разных файлов можно только в том случае, если размеры скользящего окна, используемого при их построении, совпадают. Для того, чтобы расширить возможности сравнения файлов, происходит расчёт не только для скользящего окна размером N , но и размером $2N$. Таким образом, результирующий хэш является конкатенацией двух хэшей с разным размером окон, отличающимся в 2 раза.

Размер скользящего окна подбирается таким образом, чтобы размер результирующего хэша не превышал 80 символов. Таким образом, хэш может быть пересчитан несколько раз с разным размером окна.

Сравнение двух хэшей происходит путём измерения расстояния Дамерау-Левенштейна между ними, причём веса для операций имеют следующие значения:

- удаление или вставка – 1;
- изменение байта – 3;
- обмен двух байтов местами – 5.

Данный хэш является достаточно распространённым. Это подтверждается тем, ресурс антивирусной проверки файлов Virustotal рассчитывает ssdeer для файлов, присылаемых на проверку.

Тем не менее, ssdeer обладает рядом недостатков, таких как низкая производительность, невозможность выявления частей файла и ограничение на сравнение файлов, связанное с размером окна. В связи с этим на сегодняшний день имеется множество нечётких хэшей, призванных устранить эти недостатки.

Так, алгоритм FKsum [9] является прямым развитием алгоритма ssdeer и призван решить проблему размерности скользящего окна в ssdeer. Для решения этой задачи FKsum использует дополнительное окно четырехкратной длины при расчёте хэша.

Использование статистически маловероятных особенностей

Следующим исторически появившимся после СТРН подходом является использование статистически маловероятных особенностей (Statistically Improvable Features, SIP). Данный подход основан на идее отпечатка Рабина [4]. Наиболее известным его представителем является алгоритм sdhash.

Алгоритм sdhash

Этот алгоритм создан Василем Руссевым. Хэш, используемый в данном алгоритме, основан на следующей идее: хэш строится не на файле в целом, но на его наиболее характерных особенностях. Так, используется скользящее окно, рассчитывающее для каждого участка значение энтропии. Дальше по полученным значениям проходит другое скользящее окно, которое выбирает среди своих элементов наиболее характерные. Эти элементы сохраняются в хэш, но не целиком. Вместо этого для их сохранения используется набор фильтров Блума, которые в дальнейшем и представляют собой результирующий хэш.

Этот нечёткий хэш позволил решить множество проблем, связанных с ssdeer, и является вторым по частоте использования нечётким хэшем.

Алгоритмы блочного перестроения

Третий тип нечётких хэшей имеет три наиболее ярких представителя: mrsh, его продолжение mrsh-v2 и bbhash.

Алгоритмы mrsh и mrsh-v2

Алгоритм mrsh [10] был создан как попытка совместить в себе ssdeer и sdhash, сохра-

нив преимущества обоих и устранив их недостатки. Так же, как и в ssdeer, кусочные хэши вычисляются при срабатывании определённого условия, однако результат не конкатенируется к общему результирующему хэшу, а заносится в блум-фильтры с фиксированным количеством элементов.

Другим изменением по сравнению с оригинальным ssdeer является замена хэшей, используемых в ssdeer, на более криптостойкие [5].

Детали работы mrsh:

1. Скользящее окно (длина по умолчанию – 7) проходит по файлу. Для каждого состояния скользящего окна вычисляется хэш djb2.

2. Очередной хэш участка вычисляется в том случае, если все 7 младших битов хэша скользящего окна имеют значение «1».

3. В качестве хэша для участков используется MD5.

4. Полученный MD5 делится на 4 куска по 11 бит каждый, которые затем заносятся в фильтры Блума.

5. Когда количество элементов в блум-фильтре достигает максимума (256 элементов), создаётся новый.

Алгоритм mrsh-v2 [11] является развитием mrsh. В частности, mrsh не оправдал идею использования криптографически стойких хэшей, в связи с чем в mrsh-v2 используется кольцевое хэширование и FNV, как и в ssdeer.

Алгоритм **bbhash**

Для работы алгоритма **bbhash** [12] используется некоторое предварительно заданное инициализирующее множество блоков. Цель алгоритма – обнаружить признаки того, что в анализируемых файлах содержатся данные, которые не являются широко используемыми, однако являются общими для анализируемого множества.

Работа алгоритма заключается в поблочной обработке файла. Каждый очередной блок сравнивается со всеми блоками из инициализационного множества. Сравнение происходит посредством измерения расстояния Хэмминга. Выбирается минимальное значение из всех. При этом значение добавляется в результирующий хэш только в случае, если оно меньше некоторого порогового значения.

Таким образом, в работе данного алгоритма прослеживается идея поиска маловероятных особенностей.

Множество блоков инициализации может быть выбрано случайно, однако для корректного сравнения двух файлов множества блоков, используемых при расчёте их хэшей, должны быть одинаковы. В связи с этим рекомендуется использовать блоки, приведённые в оригинальной статье.

Для сравнения блоков может использоваться как механизм сравнения, используемый в **sdhash**, так и механизм сравнения из **ssdeep**.

Алгоритм **mvhash-b**

Алгоритм вычисления нечёткого хэша **mvhash-b** [13] состоит из трёх этапов:

1. Преобразование всех байт входных данных по методу мажоритарного голосования.

2. Применение к полученной последовательности байт алгоритма кодирования длин серий (Run Length Encoding – RLE).

3. Разбиение результата на оптимальные для добавления в фильтр Блума группы.

Мажоритарное голосование заключается в том, что для каждого байта входных данных определяется количество единиц и нулей в его двоичном представлении. Если в байте количество единиц больше, чем нулей, он заменяется на **0xFF** (все единицы). В противном случае он заменяется на **0x00** (все нули).

Кодирование длин серий заключается в том, что последовательности повторяющихся элементов (нулей или единиц) заменяются на последовательность вида **NW**, где **N** – количество повторений символа **W**.

Для добавления группы в фильтр Блума используется специальный хэш. Так, каждый элемент группы заменяется на его остаток от деления на два. Полученная последовательность из **И** бит делится на две части, где первые 8 позиций указывают номер байта блум-фильтра, а оставшиеся 3 – номер бита в байте. Таким образом, длина группы – **И** элементов. Группы

перекрываются, и каждая группа смещена относительно другой на 2 элемента. Для сравнения хэшей, как и в `sdhash`, используется расчёт расстояния Хэмминга между блум-фильтрами.

Статистический отпечаток

Одним из новых направлений в развитии нечётких хэшей является вычисление статистического отпечатка. Основным представителем такого подхода является алгоритм `tlsh`.

Алгоритм `tlsh`

Одним из наиболее современных фаззи-хэшей, используемых для решения задач информационной безопасности, является `tlsh` [14], разработанный компанией TrendMicro. Данный хэш основан на алгоритме `Nilsimsa` [15], который, так же, как и алгоритм `sprmsum`, был использован для идентификации почтового спама.

Алгоритм заключается в обработке данных при помощи скользящего окна длиной 5 байт. Из каждого окна выбираются тройки, которые хэшируются и по значению хэша заполняют гистограмму частоты появления. Полученная гистограмма нормируется таким образом, чтобы каждое значение занимало два байта, то есть каждое значение заменяется номером четверти, в которую данное значение попало относительно максимального значения в ги-

стограмме. Например, если максимальный элемент равен 16, то элемент «3» будет заменён на «1», элемент «6» на «2», элемент 10 на «3», а сам максимальный элемент на «4». Результирующий хэш представлен конкатенацией всех элементов полученной гистограммы.

Это позволяет хэшу, с одной стороны, быть устойчивым к изменению входных данных, а с другой – использовать для вычисления всё пространство входных данных.

Контекстно-специфичные алгоритмы

Одной из современных тенденций в сфере нечёткого хэширования является создание фаззи-хэшей для конкретных типов данных, в отличие от созданных ранее алгоритмов для данных общего вида. Мотивацией к созданию такого класса алгоритмов является то, что одни и те же данные могут быть преобразованы в разные бинарные представления, несмотря на то, что имеют идентичную структуру.

Этот подход может быть полезным для тех ситуаций, когда необходимо обрабатывать большие объёмы данных конкретного вида. В качестве примера можно привести задачу поиска схожих изображений в большом массиве данных. При этом изображения могут иметь разный формат, способы сжатия и т.д. В таком случае использование традиционного побайтового нечёткого хэширования будет

являться малоэффективным, так как для схожих изображений нечёткие хэши могут сильно отличаться за счёт разного представления на уровне двоичного кода. В то же время, алгоритмы нечёткого хэширования, анализирующие не двоичный код, но само изображение, могли бы оказаться полезными для решения такой задачи.

Алгоритм Machoke

Представителем данного класса нечётких хэшей является Machoke. Данный алгоритм был впервые представлен на конференции r2con в 2017 году и предназначен для создания нечёткого хэша для исполняемых файлов. Для этого он хэширует не просто бинарное представление, а граф потока исполнения программы. Для каждой полученной функции строится граф потока выполнения. Узлы этого графа нумеруются, после чего граф записывается в строковом представлении. При этом записываются переходы между графами, а также тип перехода, если это вызов функции. Эти строки хэшируются при помощи некриптографического алгоритма murmurhash2, после чего результаты хэширования для всех функций конкатенируются для получения результата.

Данный подход призван улучшить использование нечёткого хэширования в за-

дачах автоматизации обнаружения вредоносных исполняемых файлов и их классификации.

Дальнейшие работы

На данный момент в области нечёткого хэширования существует множество перспективных направлений развития. Одним из них является использование нечёткого хэширования в анализе вредоносного ПО.

В современном мире угрозы, связанные с распространением вредоносного программного обеспечения, являются одними из ключевых в сфере информационной безопасности. Антивирусными компаниями обнаруживается всё больше образцов вредоносных программ. Вирусные эпидемии представляют серьёзную угрозу как для рядовых пользователей, так и для коммерческих компаний и даже государственных служб. В качестве примеров крупных вирусных атак можно привести Mirai и WannaCry. Из этого следует, что современные способы борьбы с вредоносным ПО требуют постоянной модификации с целью повышения её эффективности. При этом под эффективностью, могут пониматься: скорость обнаружения вредоносного ПО, процент ошибок первого и второго рода, время реагирования на новую угрозу и т.п.

Как было сказано во введении, многие антивирусы используют для обнаружения вредоносного ПО т.н. «сигнатуры», позволяющие обнаружить уже известные вирусы по некоторому характерному признаку. В качестве такого признака может выступать не только определённая последовательность байт, но и какое-либо более сложное правило, связывающее ряд последовательностей. Ключевой особенностью данного метода является тот факт, что для выявления отдельных сигнатур и их последовательностей используются значения хэш-функций от соответствующих участков кода вредоносных программ. Соответственно, эффективность этого метода обосновывается высокой скоростью обнаружения вредоносного ПО после того, как его образец попадает в руки антивирусных аналитиков.

Таким образом, современная индустрия разработки вредоносного ПО представляет собой попытки «установить сигнатуру» на вирус со стороны антивирусной компании и попытки «убрать сигнатуру» со стороны вирусописателей. Однако необходимость сокращения числа ошибок второго рода приводит к тому, что сигнатуры, особенно те из них, которые получают аналитиками в первые дни распространения угрозы (наиболее эффективное «окно возможностей» для злоумышленни-

ков), являются достаточно короткими, так как описывают наиболее вероятный признак, без детального анализа структуры самой программы вредоносного ПО. Это ведёт к тому, что вредоносный файл часто получает незначительные изменения, сделанные с целью убрать сигнатуру, и распространяется снова. Наиболее универсальным подходом при этом является использование автоматизированных средств обфускации программ. Так, обфускация даёт способ генерировать семантически эквивалентные программы, зачастую кардинально отличающиеся на уровне двоичного кода.

В этой области очень перспективным является использование нечёткого хэширования. Так, незначительно изменённый файл может быть легко сопоставлен со своей оригинальной модификацией и обнаружен даже в том случае, если сигнатура его обнаружения была убрана. Более того, нечёткие хэши так же, как и обычные хэш-функции, являются достаточно быстрыми в вычислении и могут использоваться для быстрого сопоставления значения, полученного от подозрительного файла, с базой уже имеющихся хэшей.

Существующие виды обфускации вредоносных программ подчас снижают эффективность использования нечёткого хэширования в анализе вредоносного ПО. Это связано с тем, что применение обфуска-

ции не приводит к равномерному изменению кода (часть секций остается без изменений, а часть может быть изменена достаточно сильно), что, в свою очередь, не находит пропорционального отражения в результирующих значениях нечётких хэш-функций широкого профиля, т.к. они рассчитаны на однородные данные и их изменения.

Несмотря на то, что для изображений задача определения схожести уже является во многом решённой [16], для других типов данных эта область может всё ещё иметь открытые проблемы. Одной из таких областей являются исполняемые программные файлы (несмотря на то, что существуют алгоритмы их сравнения, например, BinDiff [17]).

Так, является открытой задача создания нечёткого хэша, позволяющего идентифицировать семантически схожие вредоносные программы. В то время как проблема установления эквивалентности программ с точки зрения семантики является NP-трудной, вероятно, могут существовать способы определения схожих программ. Так, например, для различных видов программного обеспечения могут использоваться различные, наиболее подходящие для конкретного вида, способы определения схожести. Эти способы будут основаны на ключевых особенностях программ, характерных для того или иного вида. Воз-

можно, в то время как в одних программах преобладают операции математических вычислений, для других будет более характерным наличие большого числа вызовов функций API операционной системы для операций ввода-вывода и т.д.

Кроме того, для идентификации могут быть использованы особенности стиля программирования, характерные для авторов программного обеспечения.

Таким образом, развитие исследований в области нечётких хэш-функций уже сейчас позволяет решать множество задач в сфере информационной безопасности. Однако большинство таких задач эффективно решаются лишь специфичными хэш-функциями, зависящими как от контекста задачи, так и от ряда её параметров (таких как объём анализируемых данных). В том числе, задачи обнаружения вредоносного программного обеспечения, скрываемого с использованием автоматизированных методов обфускации, могут решаться с использованием контекстно-специфичных алгоритмов вычисления нечётких хэш-функций, использующих для построения хэш-значения внутреннюю структуру программ.

Литература:

1. Alfred J. Menezes Paul C. van Oorschot and Scott A. Vanstone Handbook of Applied Cryptography.

Boca Raton, Florida, США: CRC Press, 2001, 810 стр.

2. Jaccard P. Distribution de la flore alpine dans le Bassin des Dranses et dans quelques regions voisines // Bull. Soc. Vaudoise sci. Natur. 1901. V. 37. Bd. 140. S. 241-272.

3. Rabin M. Fingerprinting by random polynomials, technical report TR1581, center for research in computing technology. Cambridge, Massachusetts: Harvard University; 1981.

4. ddcfld [Электронный ресурс] Режим доступа: <http://dcfld.sourceforge.net/>. Дата обращения: 10.09.2018 г.

5. Vassil Roussev, Yixin Chen, Timothy Bourg, Golden G. Richard III. md5bloom: Forensic filesystem hashing revisited // Digital Investigation. Volume 3, Supplement, September 2006, Pages 82-90

6. Jesse Kornblum. Identifying almost identical files Using context triggered piecewise hashing // Digital Investigation. Volume 3, Supplement, September 2006, Pages 91-97

7. Spamsum readme. [Электронный ресурс] Режим доступа: <http://www.samba.org/ftp/unpacked/junkcode/spamsum/README> Дата обращения: 10.09.2018 г.

8. The FNV Non-Cryptographic Hash Algorithm [Электронный ресурс] Режим доступа: <https://tools.ietf.org/html/draft-eastlake-fnv-03> Дата обращения: 10.09.2018 г.

9. Roussev, V., Building a Better Similarity Trap with Statistically Improbable Features // In Proceedings of the 42nd Hawaii International Conference on System Sciences, IEEE, Jan 2009.

10. Vassil Roussev, Golden G. Richard III, Lodovico Marziale. Multi-

resolution similarity hashing // Digital Investigation. Volume 4, Supplement, September 2007, Pages 105-113

11. Similarity Preserving Hashing: Eligible Properties and a New Algorithm MRSH-v2 // Lecture Notes of the Institute for Computer Sciences, Social Informatics and Telecommunications Engineering book series (LNICST, volume 114)

12. Frank Breiting, Harald Baier. A Fuzzy Hashing Approach Based on Random Sequences and Hamming Distance // Annual ADFSL Conference on Digital Forensics, Security and Law 2012

13. Frank Breiting, Knut Petter Astebøl, Harald Baier, Christoph Busch. mvHash-B - a new approach for similarity preserving hashing // Seventh international conference on IT security incident management and IT forensics, IMF 2013, nuremberg, germany, march 12-14, 2013 (pp. 33-44)

14. TLSH - A Locality Sensitive Hash Jonathan Oliver, Chun Cheng, Yanggui Chen 2013

15. E. Damiani, S. De Vimercati, S. Paraboschi, P. Samarati. An Open Digest-based Technique for Spam Detection // Proceedings of the ISCA 17th International Conference on Parallel and Distributed Computing Systems, September 15-17, 2004, The Canterbury Hotel, San Francisco, California, USA

16. Исследование перцептивных хеш-функций изображений // Наука и Образование. МГТУ им. Н.Э. Баумана. Электрон. журн. 2015. № 08. С. 269-280

17. BinDiff [Электронный ресурс] Режим доступа: <https://www.zynamics.com/bindiff.html> Дата обращения: 10.09.2018 г.

Молодёжь как социально-демографическая группа, наиболее подверженная влиянию экстремизма и терроризма в сети Интернет

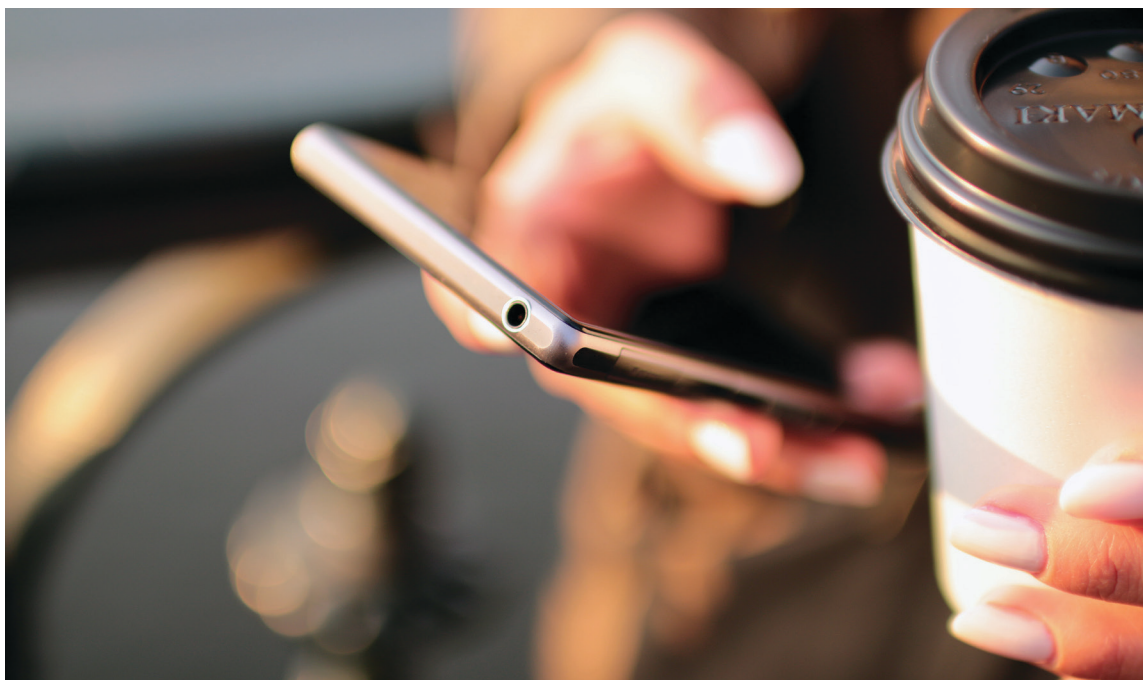
Дёшина Екатерина Игоревна — бакалавр Южного федерального университета, г. Ростов-на-Дону

Меркулова Анастасия Николаевна — бакалавр Южного федерального университета, г. Ростов-на-Дону

Развитие и массовое использование международной информационно-коммуникационной сети Интернет – общемировая тенденция, получившая особое распространение в последнее время. Деятельное участие большого числа как рядовых пользователей, так и крупных организаций в виртуальном пространстве определяет необходимость выработки актуальных технологий обеспечения национальной информационной безопасности, которые были бы адекватны текущим тенденциям, могли бы противостоять популяризации идей экстремизма и терроризма.

Используя в своих целях процессы глобализации, организаторы и участники экстремистских групп принимают на вооружение новейшие информационные технологии, средства коммуникации, которые делают их менее уязвимыми для правоохранительных органов. Возникает всё больше террористических организаций, построенных на принципах сетевой структуры. Все они объединены рядом характерных признаков, в их числе:

- наличие единых центров и информационно-коммуникативных каналов;
- автономность существования отдельных преступных



группировок, входящих в сообщество, свободно взаимодействующих как с центром, так и между собой.

Статистика последних лет неутешительна: борьба с экстремизмом всё активнее выходит за границы реального мира, проникая в виртуальные сферы. С каждым годом растёт и количество интернет-порталов, числящихся в Федеральном списке экстремистских материалов. Всё это выводит проблему виртуального экстремизма и терроризма на уровень общегосударственной, требующей повышенного внимания со стороны государственной власти и правоохранительных органов. Подтверждением этому могут служить

официальные заявления Президента Российской Федерации В.В. Путина, представителей МВД и ФСБ России.

При этом особую актуальность и практическую значимость приобретают проблемы экстремизма и терроризма среди молодёжи. Поскольку именно она является основным двигателем прогресса и интеллектуальным ресурсом государства. Поэтому для дальнейшего изучения проблемы необходимо определить, что мы понимаем под терминами «молодёжь», «экстремизм», «терроризм» и «информационный экстремизм».

Молодёжью в Российской Федерации принято считать население от 14 до 30 лет (рас-

поряжение правительства РФ от 18.12.2006 №1760-р). Данную возрастную категорию можно разделить ещё на 3 группы: школьники (14-18 лет), студенческая молодёжь (18-25 лет), работающая молодёжь (25-30 лет). Молодёжь – категория населения, наиболее уязвимая к влиянию различного рода идеологий, в том числе, экстремизма и терроризма, в силу присущих ей различных особенностей: социально-психологических, физиологических, демографических и других. В связи с этим существует острая необходимость исследования данного феномена. В таком возрастном диапазоне люди являются наиболее активными пользователями интернета, что подвергает их еще большей опасности угодить «в сети» запрещённой деятельности.

Экстремизм – это приверженность к радикальным взглядам и действиям, кардинально отрицающим существующие в обществе нормы и правила. Терроризм же является составной частью экстремизма и проявляется в применении силового воздействия (насилия), создании опасности, нанесении вреда индивиду, группе лиц или государству для достижения своих целей и др.

В последнее десятилетие возник такой феномен, как информационный экстремизм в сети Интернет, которому свойственны антисоциальность, аморальность,

радикальность в действиях и убеждениях, противоправность (зачастую действия информационного экстремизма соответствуют закону, но используют возможности в противоположных целях), анонимность и безличный характер. Информационный экстремизм – деятельность, направленная на социально-психическое деструктивное воздействие граждан через использование информационных технологий для достижения противоправных целей [3].

К проявлениям экстремизма и терроризма в сети можно отнести:

- публичное оправдание и поддержку террористической деятельности;
 - рекламу деятельности и идеологии террористических и экстремистских организаций;
 - открытое демонстрирование и пропаганду нацистской атрибутики или символики экстремистских и террористических организаций;
 - массовое изготовление, хранение и распространение экстремистских материалов, публичные призывы к осуществлению указанных действий;
 - призывы к насильственному изменению конституционного строя РФ;
 - призывы к нарушению целостности Российской Федерации;
 - разжигание национальной, социальной, расовой, религиозной розни и т.д. [1].
-

Правовая основа борьбы с экстремизмом и терроризмом представлена в законодательстве РФ. Регулирование контента в сети Интернет также предусмотрено законодательством Российской Федерации и осуществляется в соответствии со следующими федеральными законами: «О связи», «О СМИ», «Об информации, информатизации и защите информации». В свою очередь такие социальные сети, как «ВКонтакте», «Одноклассники» и другие платформы для размещения информации в целях борьбы с экстремизмом безоговорочно следуют закону об организаторах распространения информации, который обязывает к передаче соответствующих данных в правоохранительные органы.

В настоящее время интернет является универсальным средством общения, получения и обмена информацией между людьми, которые находятся в разных точках планеты. Невзирая на многие положительные аспекты использования мировой сети, она так же привлекает к себе внимание со стороны запрещённых организаций, в том числе экстремистского и террористического характера. За последние десять лет всё сильнее проявляется угрожающая тенденция ухода идеологов так называемого «чистого» ислама и других в глобальную сеть. В настоящее время проблема экстремизма и терроризма в сети актуальна, но мало изучена. Интернет-пространство за счет своего повсеместного распро-

странения, стихийного развития и доступности практически не поддается контролю. Сегодня интернет является универсальным, самым популярным и наиболее используемым источником получения информации для молодёжи и в то же время представляет для неё серьезную угрозу – попасть под влияние террористической и экстремистской идеологии. Таким образом, идеологи и организаторы данных запрещённых течений направляют свои усилия на пополнение круга сторонников и единомышленников именно из числа молодых людей.

При посещении подобных сайтов молодой человек с сформировавшейся и неустойчивой психикой достаточно быстро воспринимает пропагандируемые идеи и взгляды, перенося их на своё повседневное поведение и жизнь в целом. Процесс посредственного общения в интернет-пространстве между людьми с поверхностными, беглыми интерпсихическими отношениями усиливается за счет современных сетевых технологий. Таким образом, возникающие в глобальной сети связи носят неполноценный, искусственный характер. Как следствие, сокращается влияние на индивида его ближайшего окружения, тем самым снижается социальный контроль и нарушаются механизмы определения позитивного поведения. Допустимость анонимности в сетевом общении зачастую создает ощущение вседозволенности

и безнаказанности за какие-либо действия и проявления в сети Интернет.

Индивиды, относящиеся к возрастной категории молодёжи, находятся в особой группе риска. Это обусловлено такими факторами, как их только развивающееся самосознание, пребывание в состоянии «поиска себя» и предстоящего самоопределения. Нередко у молодого человека возникает чувство непохожести на других, обособленности и одиночества, и в поиске поддержки и общения в сети он может попасть под отрицательное влияние. Во время процесса осознания конечности существования и невозвратности времени возникает необходимость серьезного осмысления жизни и перспектив, определения целей и расстановки приоритетов.

Находясь на данном этапе развития и попав под влияние экстремистских идеологий, индивид подвергает себя реальной опасности. Проведенный РАН экспертный опрос в ходе проекта «Реакция российского общества на терроризм» позволяет проследить следующую тенденцию – в первую очередь пропаганда идей экстремизма и терроризма направлена на такие социальные группы, как молодёжь – 60%, в том числе безработная молодёжь – 12%, и молодёжь, вовлечённая в религиозные и националистические движения – 5% [9,10].

К факторам молодёжного экстремизма можно отнести влияние радикально настроенных родителей и друзей, а также поддерживающих экстремистские взгляды сверстников и иных авторитетных лиц из ближайшего окружения индивида, дезинтеграция в обществе посредством стрессовых ситуаций и нестабильного психического состояния, личные моральные убеждения и представления. Одной из самых благоприятных ситуаций для внушения идей экстремизма является духовно-нравственный кризис личности.

По словам председателя Верховного суда Вячеслава Лебедева, которые приводит РИА «Новости», с каждым годом в Российской Федерации возрастает количество уголовных дел об экстремизме, в том числе и тех, которые возбуждаются из-за постов в социальных сетях. По данным, представленным Судебным департаментом, в 2017 году только по части 1 статьи 282 УК РФ было осуждено 572 человека, всего осуждено в 2017 году – 786 человек, в 2016 году было осуждено 662 человека, 502 человека по части 1 статьи 282 УК РФ, а в 2015 – 369 человек.

Так, например, в 2016 году в Краснодаре было заведено уголовное дело в отношении 19-летнего студента, подозревавшегося в публичных призывах к осуществлению террористической деятельности (ч.2 ст.205.2 УК РФ) и возбуждении

ненависти и вражды по национальному признаку (ч.1 ст.282 УК РФ). В том же 2016 году к двум годам и трем месяцам колонии-поселения за публичные призывы к осуществлению деятельности, направленной на нарушение территориальной целостности России (ч.2 ст.280.1), был приговорён молодой человек из Твери.

В октябре 2018 года на сайте Судебного департамента Верховного суда РФ были опубликованы статистические данные о деятельности российских судов и состоянии судимости за первую половину текущего года. По интересующим нас статьям было осуждено 337 человек. Если для сравнения с показателями 2017 года увеличить это число вдвое, то можно получить следующие данные: 674 человека против 785 осуждённых в 2017 году. Это позволяет предположить, что итоговые цифры за 2018 год окажутся ниже. При этом большая часть приговоров за пропаганду была вынесена по ст. 282 УК (возбуждение ненависти).

Для современного российского общества характерно неравномерное и неодновременное распространение идей терроризма: в одних социальных группах – быстрее и активнее, в других – медленнее и с меньшим размахом. Принимая во внимание этот факт, считаем необходимым сделать акцент на «целевые группы». Основные очаги экстремизма

отмечаются на Северном Кавказе. Это, конечно, не означает, что экстремистская идеология не получает распространения в других регионах.

В 2012 году Российская академия наук провела экспертный опрос в рамках проекта «Реакция российского общества на терроризм», который позволил выделить следующие целевые группы, подверженные пропаганде экстремизма:

- молодёжь – 60% (особенно в Республике Дагестан – 82%);
- в том числе, безработная молодёжь – 12% (Республика Дагестан – 21%);
- в том числе, молодёжь, вовлечённая в религиозные и националистические движения – 5% (Республика Дагестан – 8%).

Большинство экспертов в качестве наиболее проблемных социальных групп рассматривают безработную молодёжь (46%), студентов (29%) и школьников (20%).

Проведённый экспертный опрос позволил выявить невысокую эффективность идеологического противодействия экстремистским настроениям в полиэтнических регионах (по десятибалльной шкале):

- в Республике Дагестан средний балл составил 3,73;
- Республике Татарстан – 4,1;
- Республике Башкортостан – 4,97.

По наблюдениям экспертов, особенно сложно идеологическое противодействие экстремизму складывается в Республике Дагестан – все

проводимые мероприятия оказываются малоэффективными, а силовые решения запускают непрекращающийся цикл, который заключается в воспроизводстве бандформирований среди молодёжи.

Что касается более свежих исследований, в 2015 году в социальных сетях был проведен анонимный интернет-опрос, целью которого стало криминологическое изучение экстремистских проявлений [12]. Выборка составила 900 пользователей, проводилась по профилям в социальной сети «ВКонтакте» в соответствии с соотношением пола, возраста и места проживания.

Проанализировав содержание личной страницы потенциального респондента, сотрудник, проводивший опрос, обращался к нему, разъясняя суть исследования и предлагая пройти анкетирование. Сама анкета размещалась на сервере virtualexs.ru.

Анкета состояла из двух блоков вопросов: первый – о некоторых характеристиках респондентов и количестве времени, которое они проводят в социальных сетях; второй – о различных проявлениях экстремизма в виртуальном пространстве.

На основе полученных эмпирических данных удалось сделать ряд общих выводов:

- вероятность обнаружения материалов экстремистского характера прямо

пропорциональна времени, проводимому в социальных сетях: чем дольше пользователь находится в виртуальном пространстве, тем выше шанс натолкнуться на опасный контент;

- частота обнаружения экстремистских материалов определяет частоту встреч виртуальных объединений людей, разделяющих идеологию экстремизма;

- самый распространенный контент экстремистского характера связан с информацией, унижающей и оскорбляющей людей по признаку социальной, расовой, национальной, религиозной или языковой принадлежности, отношения к религии.

Также отметим, что наибольшее число экстремистских проявлений приходится на социальную сеть VK. При этом информация чаще предстаёт в графическом виде.

Подводя итоги, отметим, что информационный экстремизм в социальных сетях представляет собой многоуровневое понятие, включающее в себя манипуляцию сознанием, разжигание межнациональной и межконфессиональной вражды, распространение искусственно созданных слухов в бескрайнем пространстве интернета. Всё это может рассматриваться как реальная угроза стабильному существованию социума, информационной безопасности госу-

дарства в целом. Особенно подвержена влиянию данного феномена такая социальная группа, как молодёжь. Олицетворяющая будущее страны, определяющая ее развитие, она довольно уязвима, поддается внешним воздействиям. Именно поэтому для борьбы с экстремистскими проявлениями в виртуальном пространстве необходимо формирование эффективной государственной политики, которая была бы адекватной современным условиям.

Противостояние экстремистской идеологии в сети Интернет, выработка действенных мер по профилактике информационного терроризма являются важными государственными задачами. В этих условиях особую значимость приобретает формирование осознанного поведения молодых людей, а также активная гражданская позиция каждого представителя молодёжного сообщества. Кроме того, процессы глобализации требуют учета опыта других стран, а также международного сотрудничества, в частности в вопросах, касающихся профилактики экстремизма.

Литература:

1. Федеральный закон от 25 июля 2002 г. N 114-ФЗ «О противодействии экстремистской деятельности» (с изменениями и дополнениями).
2. <http://fb.ru/article/293286/profilaktika-ekstremizma-v-molodejnoj-srede-cto-takoe-ekstremizm-statya-uk-rf>
3. <https://pravo.team/uk-i-koap/gosudarstvennaya-bezopasnost/ekstremizm/v-seti.html>
4. <https://cyberleninka.ru/article/n/ispolzovanie-seti-internet-terroristicheskimi-i-ekstremistskimi-organizatsiyami>
5. <https://zona.media/number/2018/09/25/repost>
6. <https://www.rbc.ru/newspaper/2016/05/10/572ca7d09a794742dedc645c>
7. <http://scienceport.ru/files/method2013.pdf>
8. http://ojkum.ru/images/articles/2016-3/_2016_3_0038-06.pdf
9. Маркин В.В., Роговая А.В. Противодействие распространению идеологии экстремизма и терроризма в молодёжной среде: 1-я часть // Власть. 2012. № 11. С. 142–146.
10. Маркин В.В., Роговая А.В. Противодействие распространению идеологии экстремизма и терроризма в молодёжной среде: 2-я часть // Власть. 2012. № 12. С. 114–118.
11. Рудик М.В., Волков Д.В. Социальные сети как средство распространения экстремизма // Вестник КРУ МВД России, 2017. №2 (36).
12. Соловьев В.С. Криминологическое исследование экстремистских проявлений в социальных сетях Интернета (по материалам интернет-опроса пользователей) // ЮП, 2016. №5 (78).
13. Самошин А.В., Горовой В.В. Особенности предупреждения распространения экстремистских материалов в молодёжной среде по глобальной сети Интернет // Труды Академии управления МВД России, 2016. №3 (39).

Проблемы противодействия религиозному экстремизму в России

Кудрявцев Никита Александрович — бакалавр Южного федерального университета, г. Ростов-на-Дону

Хасеинов Эмин Яхьяевич — бакалавр Южного федерального университета, г. Ростов-на-Дону

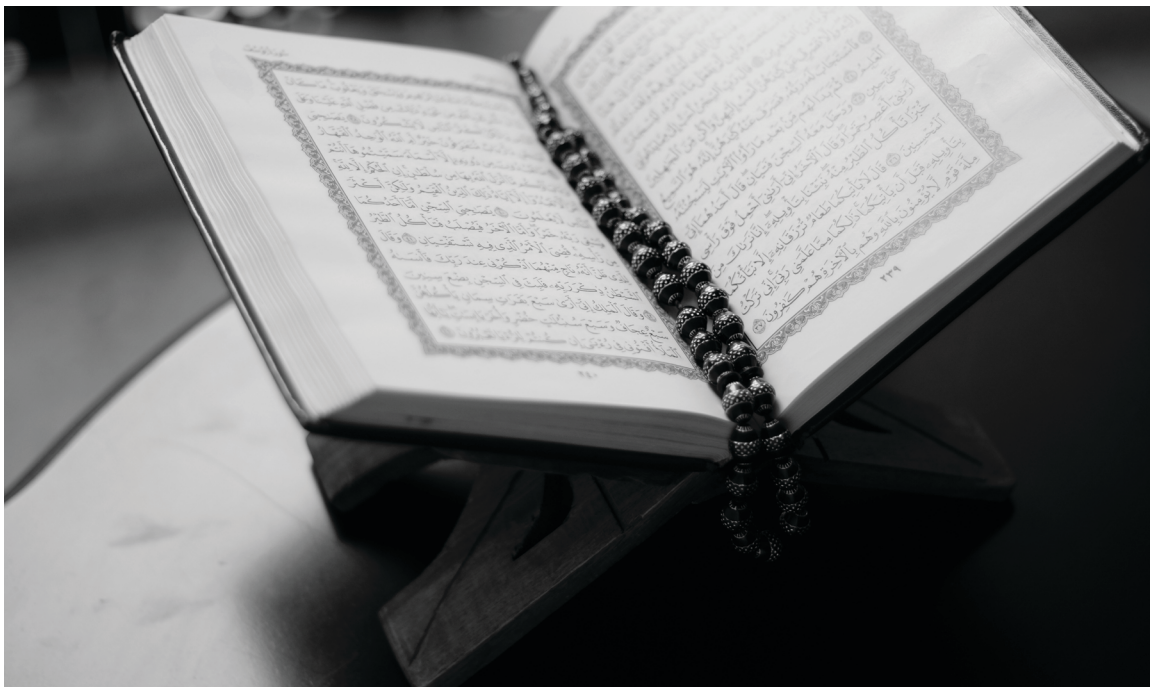
Одна из наиболее острых проблем, стоящих перед современным миром – религиозный экстремизм. Эта беда, к сожалению, не обошла стороной и нашу страну. Более того, именно Россия стала одной из первых жертв религиозного экстремизма. Большинство ученых, занимающихся изучением вопросов борьбы с экстремизмом, называют конкретный год и даже день его появления в России.

Это случилось 4 апреля 1864 года, когда Дмитрий Каракозов осуществил покушение на Александра II. Попытка покушения оказалась неудачной, и Дмитрий Каракозов был прилюдно повешен, но данный исторический факт считают началом эпохи экстремизма в России. Экстремистской является также попытка насильственной смены власти 25 декабря 1825 года. В дальнейшем

эсеры, народовольцы, коммунисты очень часто прибегали к подобному способу решения проблем. Г.И. Телегин [8] выделяет четыре этапа распространения экстремизма в России: дореволюционный, советский, переходный и новейший, охватывающий период с 2000 года и по настоящее время.

В новейшее время две чеченские кампании стали толчком для зарождения террористических организаций и появления новой модели поведения, такой как религиозно-экстремистская деятельность. Именно в 90-е годы произошли крупные террористические акты на территории России, их количество только увеличивалось в последующие несколько лет [1].

Поскольку довольно большая часть террористических актов совершается от имени мусульманских организаций,



то говоря о религиозном экстремизме, чаще всего подразумевают именно исламский экстремизм. По данным ЦРУ, в 2004 году из 80 международных террористических организаций 72 представляли воинствующий ислам. В том же году они совершили 651 теракт, погибло 1907 человек [2]. В данной статье авторы тоже под религиозным экстремизмом понимают исламский радикализм.

Этот феномен имеет различные обозначения в современной литературе – исламский терроризм, исламский экстремизм, исламский радикализм или просто исламизм и т.д. Ряд ученых и общественных деятелей, особенно мусульман, счи-

тают недопустимым использование в наименовании этого явления слова «исламский», поскольку полагают, что в исламе нет места терроризму, экстремизму и всякого рода насилию [3]. Согласно их мнению, подобные названия в лучшем случае некорректны или же ненаучны, противоречат исламу и крайне вредны для общества. Ислам отделен от политики, является религией мира и добра.

Другая часть исламских богословов и самих мусульман воспринимает ислам как политическую идеологию, что существенно затрудняет отделение экстремизма от самого ислама: «До сих пор некоторые люди утверждают, что религию и политику не следу-

ет смешивать. Религия – личное дело, и поэтому её не надо навязывать обществу. <...> То, чего часто не понимают, как мусульмане, так и немусульмане, – это факт, что политике нельзя отделить от Ислама, она является частью его идеологии, поскольку призвана решать те проблемы, с которыми сталкиваются мусульмане. Бухари цитирует слова Ибн Умара: «Пророк (да благословит его Аллах и приветствует) сказал: «Имам несет ответственность за своих граждан». Следовательно, в Исламе нет разделения на духовное и светское, нет отделения религии от экономики, внутренней и внешней политики. Одно и то же общество не может руководствоваться одновременно Исламом и другими идеологиями, такими как капитализм или коммунизм.» [4]

При таком подходе террористические акты понимаются как методы ведения войны двух противоборствующих политических сил, где слабая сторона (в данном случае исламские силы), за неимением авиации и других видов оружия массового уничтожения, устраивает взрывы в тылу врага. Сторонники такого подхода, квалифицируя акты насилия, разделяют их на диверсионные и террористические акты. Диверсионные акты рассматриваются как вполне нормальные методы ведения войны, которые соответствуют военным нормам ислама. Их

отличительным признаком является направленность только на военнослужащих как на «воинов вражеской стороны» и ненасильственное отношение к мирному населению. При подобной трактовке, например, события в Будённовске лета 1995 года, к которым был причастен Шамиль Басаев, квалифицируются именно как диверсия, поскольку нападение было на милицейскую часть, а роддом являлся лишь укрытием при отступлении.

Террористический акт, напротив, направлен на мирное население с целью манипуляции вражеским государством (предъявление требований, запугивание и т.д.). Теракт является преступлением с точки зрения ислама (в отличие от диверсии) и даже существует конкретный богословский термин, обозначающий это отклонившееся от ислама течение – хариджиты (от араб. – выступившие (в том числе против власти), покинувшие) [5]. В данном случае, не важно отношение террористов (хариджитов) к мирному населению – считают они их «виновными», т.е. составной частью вражеской системы, «поддерживающей его налогами или молчанием» или же рассматривают просто как средство для достижения политических целей. И в том, и в другом случае это теракт. Например, события в Беслане, которые были организованы всё тем же Басаевым, уже являются терактом,

поскольку они ориентированы на захват мирных жителей с целью предъявления политических условий (в данном случае – прекращения войны в Чечне и признания независимости и государственного статуса Чеченской Республики Ичкерия).

В силу того, что маркером террористического акта в данном случае не является насильственное действие как таковое (как в случае с первой точкой зрения), а субъективный смысл и направленность террористов на определенную социальную группу, данный подход существенно усложняет регистрацию террористических актов и сильно политизирует этот процесс. Более того, подобное понимание не укладывается в юридические рамки большинства стран, включая Россию, и, соответственно, не позволяет проводить адекватную политику противодействия экстремизму и терроризму.

В связи с вышесказанным, в данной работе мы будем определять религиозный экстремизм как приверженность к любым крайним взглядам, насильственным методам, обосновываемым религиозными учениями. Исламский радикализм как разновидность религиозного экстремизма понимается нами как тактика насильственных расправ с оппонентами (оппозицией), находящая себе идеологическое обоснование и

оправдание в трактовках вероучения и направленная на защиту исламского мира от влияния или агрессии немусульманских стран и идеологий, в особенности, западного мира.

Проблема религиозного экстремизма часто обсуждается в СМИ. В общественных местах можно заметить таблички с рекомендациями, призывающими граждан быть бдительными; чтобы пресечь террористические акты, проводятся воспитательные беседы в школах, различные акции в молодёжных организациях и т.д.

Одним словом, со стороны государственных служб заметна деятельность, направленная на профилактику, предупреждение и противодействие экстремизму. Меры противодействия и профилактики экстремизма особенно усилились в начале 2000-х годов, после ряда крупных терактов, прокатившихся по всей стране.

Действительно, статистика свидетельствует, что число терактов с середины 2000-х начало снижаться и значительно сократилось за последние несколько лет, также сократилось и число жертв террористических актов [6]. Так, если в период с 1994 по 2004 гг. в результате террористических актов погибло более 1800 человек, то число жертв с 2005 по 2015 годы не превышало 350. Исходя из этого, можно предположить, что профилактика и борьба с экстремизмом

ведутся достаточно успешно и проблем в этой сфере стало меньше. Однако при более пристальном изучении проблемы можно обнаружить довольно тревожные симптомы сбоя в механизме противодействия экстремизму, которые могут оказаться миной замедленного действия.

Так, по мнению А.А. Найдды, отсутствие четких критериев квалификации экстремистской деятельности или публичной информации как экстремистской позволяет правоприменителям находить всё новые признаки экстремизма, увеличивая количество возбужденных и рассмотренных дел, из-за которых искусственно завышается статистика, создавая иллюзию повышения уровня борьбы с экстремизмом в стране [7].

Основным стержневым актом, вокруг которого сформирован весь массив российского антиэкстремистского законодательства, является Федеральный закон от 25.07.2002 № 114-ФЗ «О противодействии экстремистской деятельности». Как механизм защиты и профилактики, регулирования и пресечения экстремизма закон имеет определенные недостатки: введя понятие «экстремизм», уравнивает его с понятием «экстремистская деятельность», не выделяет характерные признаки экстремизма, не раскрывает сущность данного социального

явления, а лишь перечисляет его формы [8].

Экстремистская деятельность не отграничена от схожих с ней проявлений иной общественно-политической активности в виде полемики, дискуссии и т.д., которые не преследуются по закону, а составляют фактически часть демократии и свободы слова, свободы выбора убеждений и вероисповедания [8].

Не определены и не отграничены в Законе также и другие ключевые понятия: «экстремистская деятельность», «экстремистская организация», «экстремистские материалы», «атрибутика или символика, сходные с нацистской атрибутикой или символикой до степени смешения», «вражда», «пропаганда», «социальная группа» и т.д. [8].

Подобные упущения приводят к слишком широкой трактовке экстремизма, что недопустимо, иначе противодействие экстремизму превратится в подавление инакомыслия, будь то в политической, религиозной или любой другой сфере человеческой жизни.

Другая проблема, вытекающая из неразработанности на законодательном уровне понятия «экстремизм» – это фактическое делегирование судьями полномочий по осуществлению правосудия экспертам. Экспертизы рассматриваются судами как единственно возможное и

единственно правильное доказательство, предreshающее исход всего дела.

Подобная практика доводит судопроизводство до абсурда, превращая экспертов в инструмент вынесения обвинительных приговоров, значительно расширяя поле манипуляций и разночтений. Судьи непосредственно не изучают материалы дела, и если эксперты нашли (или не нашли) признаки экстремизма в расследуемом деле, то с вероятностью чуть ли не в 100 процентов решение суда будет совпадать с экспертным мнением. Порой это приводит к тому, что экспертами изобретаются новые конфессии, как, например, «иудаисты» в деле о признании книг «Славяно-Арийские Веды» (9) экстремистскими и их запрете; или такой национальности, как «мигранты» - в деле Александра Салагаева, доктора социологических наук и президента Общества русской культуры Татарстана.

Однако чаще и сильнее всего эта практика сказывается на подозреваемых в религиозном экстремизме, в частности, исламском. При рассмотрении дела, касающегося исламского радикализма, к противоречивой и неразработанной юридической терминологии закона об экстремизме добавляется столь же неразработанное и противоречивое понятие «ваххабизм».

Несмотря на попытки некоторых ученых методологически обосновать концепцию существования ваххабизма как исламского течения и тем самым легализовать употребление этого термина не только в СМИ, но и в науке, данный термин остается крайне неоднозначным и спорным. В частности, в работе И.И. Нурутдинова «Методологические проблемы концептуализации понятия «ваххабизм»» [10] предпринята попытка осветить основные подходы и методологические проблемы, затрудняющие концептуализацию понятия «ваххабизм», и предложить возможные решения указанной проблемы с точки зрения автора. Однако, как сам освещенный в работе дискурс, так и предложенные автором решения крутятся вокруг одного - признаков и характеристик ваххабизма и самих так называемых «ваххабитов».

Указывая на то, что «последователи ваххабизма сами ваххабитами себя не называют» и что данное понятие довольно обширно и может включать в себя довольно большое количество мусульманских течений (в том числе и официально признанных и легально существующих в Саудовской Аравии), автор делает попытку предложить свой список признаков, благодаря которым можно отличить «ваххабита» от умеренного мусульманина [11]. Как уже указывалось

выше, во всех этих случаях говорится лишь о признаках и не артикулируются две ключевые проблемы, которые, на наш взгляд, препятствуют научно-методологическому обоснованию концепции «ваххабизм» в рамках исламского радикализма. Это, во-первых, выделение единого, отличительного маркера, поддающегося регистрации, который был бы характерен для всех «ваххабитов», а во-вторых, установление этимологической связи выделенного маркера с самим словом «ваххабизм». Игнорирование этой проблемы ставит под сомнение вообще целесообразность использования данного термина в науке и работе по противодействию экстремизму, а исследования в данной области превращаются в «масло масляное».

Таким образом, подводя итоги, мы можем указать на две основные и взаимосвязанные проблемы, которые препятствуют проведению грамотной и эффективной работы по противодействию религиозному экстремизму: 1) терминологическая путаница и неразработанность терминов в юридических актах и науке; 2) кризис в процедуре экспертизы в судопроизводстве, которая при наличии высококлассных экспертов могла бы компенсировать неполноту юридических актов, однако за неимением таковых лишь усугубляет ситуацию.

Решение этих проблем особенно важно для нашей многонациональной и многоконфессиональной страны, поскольку за мнимой статистикой увеличения количества предотвращённых терактов и снижения террористических актов могут скрываться необоснованные репрессивные меры по отношению к определённым слоям населения. Последствия таких мер могут оказаться самыми разными: от повышения социального напряжения в притесняемых слоях населения, роста недовольства и непредвиденных акций протеста до появления сепаратистских настроений и резкого увеличения террористических актов и т.д. Всё это может оказаться полной неожиданностью для должностных лиц, оценивающих ситуацию в стране лишь по отчетам силовых структур, что не позволит им адекватно среагировать на подобные события, в случае развития такого сценария.

Более того, подобные меры борьбы с экстремизмом вызывают у граждан недоверие к российской правоохранительной структуре и власти в целом, особенно у представителей ислама. Мусульмане России, особенно молодёжь, чувствуют себя притесняемой группой в своей стране, что в свою очередь способствует сегментации российского народа, препятствуя формированию единой российской нации.

По мнению авторов, лишь тесное сотрудничество с популярными в мусульманской среде российскими исламскими деятелями позволит приблизиться к решению указанных проблем. Привлечение последних в органы государственного управления, законотворчества, в экспертную группу, проведение совместных круглых столов и т.д. могут способствовать налаживанию контактов с «лидерами мнений» российских мусульман для совместной работы по противодействию религиозному экстремизму в нашей стране.

Литература:

1. Террористическая опасность в РФ сохраняется // РИА Новости, 12 февраля 2008 // <https://ria.ru/20080212/99008486.html> (19.01.2019)
2. 90% международных террористических организаций – исламистского толка, считают в ЦРУ // Интерфакс-Религия, 29.04.2005 г. <http://www.interfax-religion.ru/?act=interview&div=438> (14.01.2019)
3. Вице-спикер Совета Федерации А. Торшин: Исламский терроризм меня не волнует. Его нет Архивная копия от 18 октября 2009 на Wayback Machine // Ислам.ру <http://islam.ru/pressclub/vslux/torwinsal/> (16.01.2019)
4. Правильная политическая активность мусульман на Западе // Ислам.ру <http://islam.ru/content/analitics/542> (16.01.2019)
5. Али-заде, А. А. Хариджиты: [арх. 1 октября 2011] // Исламский энциклопедический словарь. – М.: Ансар, 2007.
6. Крупнейшие теракты в России в 2010-2013 годах. РИА Новости (29 декабря 2013). <https://ria.ru/20131229/987132908.html> (17.01.2019)
7. Найда А.А. Практические аспекты применения закона о противодействии экстремистской деятельности. Религиозный экстремизм // Практика применения закона о противодействии экстремистской деятельности: сб. матер. науч.-практ. конф. – М., 2016. – С.6–13.
8. Андреева Е.А. Теоретико-методологические основы экстремизма в контексте научного знания // Актуальные проблемы современной науки. – Алушта: НОУ ВПО «Сев-КавГТИ», 2015. – С. 118-122.
9. Центральный районный суд г. Омска, федеральный судья И.И. Соснин, дело № 2-561/2015 по заявлению прокурора Омской области о признании книг «Славяно-Арийские Веды» издательства ООО «Родович» экстремистскими материалами, включении их в список экстремистской литературы.
10. Нурутдинов И.И. Методологические проблемы концептуализации понятия «Ваххабизм» // ВЭПС. 2015. №3. URL: <https://cyberleninka.ru/article/n/metodologicheskie-problemy-kontseptualizatsii-ponyatiya-vahhabizm> (дата обращения: 23.01.2019).
11. Довгяло В.К. Профилактика экстремизма в молодёжной среде // Вестник ПГГПУ. Серия № 3. Гуманитарные и общественные науки. 2018. №1. URL: <https://cyberleninka.ru/article/n/profilaktika-ekstremizma-v-molodezhnoy-srede-1> (дата обращения: 22.01.2019).

Игра-квест «Антитеррор» как положительный опыт профилактики терроризма и экстремизма в молодёжной среде

Малышева Ирина Сергеевна — педагог-психолог высшей категории, ГОБУ МО ЦППМС-помощи, г. Мурманск

Шихова Марина Валерьевна — инспектор по особым поручениям штаба Забайкальского ЛУ МВД России на транспорте, г. Чита

Впервые игра-квест для молодёжи «Антитеррор» прошла в Мурманске в октябре 2016 года, инициаторами ее проведения стали сотрудники отдела информации и общественных связей и Центра противодействия экстремизму УМВД России по Мурманской области совместно с отделом по делам молодёжи министерства по внутренней политике и массовым коммуникациям Мурманской области. Консультационную помощь при подготовке игры оказали представители УФСБ России по Мурманской области.

Участники игры-квеста – молодёжь в возрасте от 18 до 26 лет, студенты и представители общественных объединений Мурманской области. В игре принимали участие 5-6 команд, общее количество участников – не более 30 человек.

В 2017 году в Мурманске прошли две игры для молодё-

жи «Антитеррор-2017». Сначала игра проводилась в один этап в Мурманске. Позже, когда комплект материалов (положение об игре-квесту, рекомендации для организаторов, рекомендации для участников) был разослан по муниципальным образованиям Мурманской области, состоялись муниципальные этапы, победители которых приняли участие в областном этапе.

В мае 2018 года в Мурманске прошел областной этап игры «Антитеррор-2018». Цель игры «Антитеррор» – обучение молодых людей правильным действиям в случаях угрозы террористического акта, а также противодействие экстремистской пропаганде с помощью смоделированных ситуаций, носящих условный характер.

Задачи игры:

– обучение молодых людей оптимальным действиям при угрозе совершения террористи-



ческих актов, действиям по их предотвращению;

- профилактика негативного воздействия экстремистских и террористических организаций на молодых людей, в том числе так называемой вербовки по национальному и расовому признакам;

- пропаганда в молодёжной среде толерантности и мирного сосуществования в пределах нашей страны граждан разной национальности и вероисповедания;

- формирование общественного мнения о проблеме терроризма и экстремизма в молодёжной среде.

В ходе игры командам необходимо пройти пять этапов, на каждом из которых выполняются определённые задания, некоторые – в форме квеста. Оцениваются правильные действия молодых людей, в том числе, порядок оповещения правоохранительных органов в случае обнаружения подозрительных предметов или людей.

После завершения игры для ее участников, как правило, проводятся специальные меропр-

ятия, подготовленные сотрудниками правоохранительных органов, например, условный «захват заложников». В роли «заложников» и «террористов» выступают сотрудники полиции. Молодые люди в это время наблюдают за правильными действиями «условных заложников», после этого им объясняют, как грамотно вести себя в подобных ситуациях.

Перед началом игры для её участников проводится инструктаж, который включает методические рекомендации (рассылаются заранее, за день до игры) и устные рекомендации от организаторов, в том числе о порядке прохождения игры, технике безопасности при прохождении ее этапов. Ход игры контролируют кураторы (как правило, сотрудники полиции). Они наблюдают за прохождением этапа, начисляют баллы за правильное решение ситуации либо снимают их за нарушение техники безопасности.

Игра проводится в два этапа: на районном уровне – первый этап (отборочный) проходит в первом полугодии. Команды-

победители районного этапа участвуют в региональном этапе, который проводится в Мурманске во втором полугодии, дата назначается организаторами по согласованию.

Для участия в игре организаторам предоставляется заявка от команды из пяти человек по определённой форме и согласие каждого члена команды на обработку персональных данных. Основанием для регистрации участников является предоставление полного пакета документов. По желанию команды могут заранее выбрать себе название и командира. Заявки, не соответствующие требованиям, не принимаются.

В 2017 году на муниципальном уровне в рамках игры были реализованы следующие виды заданий:

– «Подземка» - имитация метро или подземного перехода. На данном этапе участники игры, двигаясь по коридору, среди нескольких различных надписей должны найти изображения или граффити, которые, возможно, содержат экстремистские лозунги либо картинки, запрещённые в России. Прохождение этапа оценивается при обнаружении всех подозрительных изображений, а также при правильных действиях команды при их обнаружении (согласно методическим рекомендациям).

– «Студенческая аудитория» - имитация класса или аудитории, в которой, возможно, находится взрывное устройство в

оставленном кем-то пакете или другом подобном предмете. Прохождение этапа оценивается при обнаружении подозрительного предмета и правильных действиях при его обнаружении (согласно методическим рекомендациям).

– «Библиотека» - имитация зала студенческой библиотеки, в которой среди нескольких кратких (не более одной страницы формата А4) текстов, возможно, находятся экстремистские высказывания. Прохождение этапа оценивается после обнаружения всех текстов и совершения правильных действий при их обнаружении (согласно методическим рекомендациям).

– «Интернет» - имитация социальных сетей. На страницах нескольких пользователей, возможно, находятся экстремистские файлы или материалы. Прохождение этапа оценивается при обнаружении всех подозрительных файлов или материалов и правильных действиях при их обнаружении (согласно методическим рекомендациям).

– «ЖД-вокзал» - имитация зала ожидания на железнодорожном вокзале. Среди людей, находящихся в зале ожидания, возможно, находится террорист-смертник. Как правило, организаторы игры на эту роль определяют человека славянской внешности (в то же время, среди людей могут находиться представители других национальностей), для того, чтобы молодые люди поняли, что терро-

ризм не имеет национальности. Прохождение этапа оценивается при обнаружении подозрительного человека и правильных действиях при его обнаружении (согласно методическим рекомендациям).

Команды начинают прохождение этапов игры одновременно. На прохождение каждого этапа отводится до 10 минут. Для игры необходимы пять аудиторий или классов, в которых команды будут по очереди проходить смоделированные ситуации.

За прохождение этапа начисляются баллы – от одного до трех. Максимальное количество баллов начисляется, если команда выполнила все задания правильно. Минимальное количество баллов начисляется, если команда при прохождении этапа не смогла обнаружить подозрительные материалы или предметы, однако не совершила грубых ошибок, например, при обнаружении взрывного устройства не касалась подозрительного предмета (то есть не «взорвалась»). При совершении грубых ошибок баллы не начисляются.

Команда, набравшая максимальное количество баллов, становится победителем игры, получает кубок и диплом победителя. В случае, если две команды или больше набирают одинаковое количество очков, победитель выбирается путем ответа на вопросы организаторов игры.


Во время подсчета баллов участники игры просматривают ролики, посвященные профилак-

тике экстремизма и терроризма, подготовленные НАК России, либо (на областном уровне) смотрят показательные выступления спецназа полиции или Росгвардии (по согласованию), кинологической службы (по поиску взрывчатых веществ).

Награждение победителей проходит после подсчета баллов. Победитель игры на региональном этапе получает кубок, остальные участники получают поощрительные призы. За месяц до проведения мероприятия в региональных СМИ размещается информация о порядке приема заявок на участие в игре-квесте.

Опыт проведения игры показал, что она интересна как форма профилактики. Более того, многие студенты, представители молодежных объединений после участия в игре в 2016 году подавали заявки на участие в аналогичных мероприятиях в 2017 и 2018 годах. Поэтому организаторы квеста приняли решение о том, что участвовать в играх «Антитеррор» могут только те молодые люди, которые ранее не являлись их участниками. Это позволит охватить как можно больше молодых людей данной формой профилактической работы.

Одним из позитивных результатов игры стало то, что ее участники, получив знания и навыки в организации профилактической работы в области антитеррора и противодействия экстремизму, стали проводить подобные мероприятия самостоятельно, ретранслируя тем самым опыт игры на более широкую аудиторию.



Положение о конкурсе научных и творческих работ среди молодых ученых, специалистов в сфере противодействия идеологии терроризма и экстремизма и сотрудников образовательных организаций Юга России

СОВРЕМЕННЫЕ МЕТОДЫ ПРОФИЛАКТИКИ РАСПРОСТРАНЕНИЯ ЭКСТРЕМИЗМА В МОЛОДЕЖНОЙ СРЕДЕ И ОБРАЗОВАТЕЛЬНОЙ СФЕРЕ


1. ОБЩИЕ ПОЛОЖЕНИЯ

1.1. Настоящее Положение определяет порядок проведения Конкурса, условия участия в нем, требования к заявкам, сроки и порядок рассмотрения работ, определения и награждения победителей.

1.2. Цели и задачи Конкурса.

1.2.1. Конкурс проводится в целях активизации деятельности профессионального сообщества России в сфере профилактики и идеологического противодействия экстремизму и терроризму.

1.2.2. Задачи Конкурса:

- повышение роли молодых ученых в сфере профилактики распространения террористической идеологии;
 - привлечение научной общественности к вопросам противодействия идеологии терроризма;
 - содействие формированию у граждан Российской Федерации неприятия терроризма и экстремизма и их идеологии, способности противостоять террористическим угрозам;
 - информационное противодействие пропаганде терроризма и экстремизма с использованием новых информационных технологий.
- 

2. ПРЕДМЕТ И УЧАСТНИКИ КОНКУРСА

2.1. На Конкурс выдвигаются материалы, посвященные антитеррористической проблематике, вопросам противодействия терроризму, его идеологии и современным методам их решения.

2.2. На Конкурс могут быть представлены только оригинальные публикации студентов, преподавателей, ученых, специалистов сферы противодействия терроризму и экстремизму (в том числе в соавторстве – не более 5 соавторов).

2.3. К участию в конкурсе допускаются текстовые публикации. Не принимаются и не рассматриваются работы, не соответствующие цели, задачам и номинациям Конкурса (например, о технических средствах антитеррора и др.), а также представляющие собой рецензии, отзывы, размышления и т.п. на опубликованные ранее книги, статьи, вышедшие в прокат кино- и телефильмы, театральные постановки.

2.4. Жанр публикации и ее конкретную тему автор определяет по своему усмотрению, исходя из цели, задач и номинаций Конкурса.

2.5. Заявки на участие в Конкурсе в любой номинации принимаются от авторов – физических лиц (далее – Участник), пишущих на темы антитеррористической направленности.

3. ОРГАНИЗАТОРЫ, УЧРЕДИТЕЛИ И ПАРТНЕРЫ

3.1. Национальный центр информационного противодействия терроризму и экстремизму в образовательной среде и сети Интернет совместно с региональным общественным движением Ростовской области «Интернет без угроз».

3.2. Оператор конкурса - Национальный центр информационного противодействия терроризму и экстремизму в образовательной среде и сети Интернет.

3.3. Учредителями Конкурса выступают: Национальный центр информационного противодействия терроризму и экстремизму в образовательной среде и сети Интернет, региональное общественное движение Ростовской области «Интернет без угроз».

3.4. Оператор конкурса осуществляет оперативную деятельность по организации Конкурса:

- формирование жюри Конкурса (далее – Жюри);
- прием заявок Участников посредством электронной почты (info@ncpti.ru);
- предоставление заявок на рассмотрение Жюри;
- проведение награждения победителей;
- решение иных задач, связанных с проведением Конкурса.

3.5. Контактные данные Оператора Конкурса:

344011 г. Ростов-на-Дону, ул. Города Волос, 6, оф. 1314.

Сайт конкурса - [НЦПТИ.рф](http://ncpti.ru)

Электронная почта секретаря Жюри: info@ncpti.ru



4. НАГРАДЫ КОНКУРСА

4.1. Жюри Конкурса определяет три заявки, победившие в конкурсе.

4.2. Победители Конкурса награждаются дипломами об участии в конкурсе и памятными сувенирами.

4.3. Работы победителей и лучших конкурсантов будут опубликованы в журнале «ОБЗОР.НЦПТИ».

5. ПОРЯДОК И СРОКИ ПРЕДОСТАВЛЕНИЯ ЗАЯВОК

Участник предоставляет на Конкурс до 31 июля 2019 года:

5.1. Заявку на участие с указанием:

- Ф.И.О. участника и его научного руководителя (если имеется), ученой степени и ученого звания (если имеются), места работы (учёбы), должности,
- названия представленной на конкурс работы (у опубликованных ранее книг и статей указываются полные выходные данные);
- контактных данных участника (телефона, электронной почты, места проживания).

5.2. Конкурсную работу в цифровом формате (выполненную в текстовом редакторе Word, шрифт Times New Roman – 14), список литературы располагается в конце текста. В начале работы указывается ее название, инициалы и фамилия автора (научного руководителя), наименование организации или учебного заведения.

5.3. Принимаются материалы только на русском языке. Минимальный объем работы – 7000 знаков с пробелами, максимальный – 30000 знаков с пробелами.

5.4. Присланные на Конкурс материалы рецензированию, возврату и оплате не подлежат.

5.5. Оператор Конкурса проводит проверку работ на наличие недобросовестных заимствований и премодерацию заявок на соответствие целям, задачам конкурса, техническим требованиям. Одобренные заявки передаются Жюри.

6. ЖЮРИ КОНКУРСА

6.1. Жюри Конкурса формируется из представителей научного сообщества (кандидатов наук, докторов наук), представителей министерств, общественных организаций и ведомств субъектов Юга России.

6.2. Члены Жюри работают на добровольной основе.

6.3. Жюри осуществляет следующие функции:

- проведение экспертизы конкурсных материалов (по критериям);
- определение победителей Конкурса в каждой номинации по сумме набранных баллов;
- Результаты Конкурса оформляются протоколом, который подписывается председателем Жюри. Решения Жюри являются окончательными и не подлежат обжалованию.

7. ПОРЯДОК ПРОВЕДЕНИЯ КОНКУРСА

7.1. Конкурс проводится в следующем порядке:

- сбор и определение заслуживающих внимания заявок;
- оценка работ;
- утверждение списка победителей Конкурса;
- объявление результатов Конкурса и награждение победителей.

7.2. Критерии оценки работ и определения победителей Конкурса:

- Соответствие требованиям оформления и предоставления заявки – от 0 до 5 баллов.
- Соответствие работы задачам конкурса – от 0 до 5 баллов.
- Актуальность заявленной темы и полнота ее раскрытия – от 0 до 5 баллов.
- Научная новизна – от 0 до 5 баллов.
- Научность (научно-понятийный аппарат, обоснованность утверждений, аргументированность выводов) – от 0 до 10 баллов.
- Качество используемого фактического материала – от 0 до 5 баллов.

7.3. Материалы рассматриваются только в электронном виде и оцениваются членами Жюри в заочном порядке.

7.4. Оценка конкурсных работ осуществляется каждым членом Жюри через электронную систему методом выставления экспертной оценки, соответствующей балльной шкале по каждому критерию.

7.5. Итоговая оценка каждого Участника в номинации формируется путем суммирования его баллов по каждому из указанных выше критериев.

7.6. На очном заседании Жюри путем открытого голосования утверждает общий протокол и баллы участников.

7.7. Победители и лауреаты Конкурса (первые три места) определяются исходя из общего числа набранных баллов.

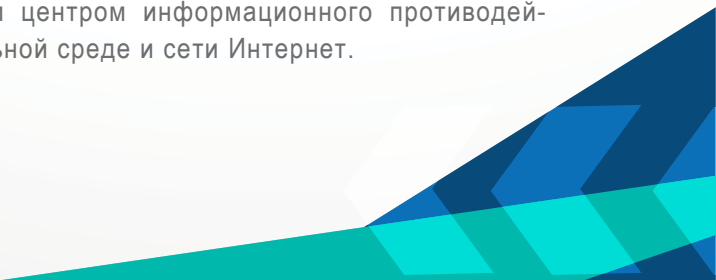
8. ПОДВЕДЕНИЕ ИТОГОВ И НАГРАЖДЕНИЕ ПОБЕДИТЕЛЕЙ

8.1. Итоги Конкурса будут подведены и объявлены не позднее 10 сентября 2019 года.

8.2. Информация об итогах конкурса размещается на сайте конкурса не позднее 30 сентября 2019 года.

9. ЗАКЛЮЧИТЕЛЬНЫЕ ПОЛОЖЕНИЯ

9.1. По согласованию с авторами, материалы могут быть опубликованы в научном журнале «ОБЗОР.НЦПТИ», выпускаемом Национальным центром информационного противодействия терроризму и экстремизму в образовательной среде и сети Интернет.



ОСНОВНЫЕ НАПРАВЛЕНИЯ ДЕЯТЕЛЬНОСТИ



Организация подготовки к лицензированию предприятий, учреждений и организаций на осуществление работ, связанных с использованием сведений, составляющих государственную тайну



Аттестация автоматизированных систем и выделенных помещений на соответствие требованиям безопасности информации



Проектирование и внедрение систем защиты информации, обрабатываемой в информационных системах ПДн, ГИС и информационных (автоматизированных) системах, используемых для обработки иной конфиденциальной информации



Защита персональных данных в соответствии с требованиями Федерального закона от 27.07.2006 № 152-ФЗ



Подключение к государственным информационным системам: ЕГИСМ, ФИС ЕГЭ, ФИС ФРДО, ГИС «Контингент» и др.



Реализация программ дополнительного профессионального образования в области информационной безопасности



НЦПТИ

ОБЗОР.НЦПТИ
СБОРНИК ИНФОРМАЦИОННЫХ
МАТЕРИАЛОВ

Национальный центр информационного противодействия терроризму и экстремизму в образовательной среде и сети Интернет
