

# ОБЗОР.НЦПТИ

Выпуск № 1 (24)

Март 2021



## Кибердобровольцы в образовательных организациях высшего образования Российской Федерации

### Кулягин И. В.

Об организации и кадровом обеспечении деятельности по противодействию идеологии терроризма в образовательной среде

### Жученко В. С.

Информационная справка по кибердобровольчеству. Кто такие кибердобровольцы?

### Куценко М. В.

Интервью с М. Наместниковой: Тренды развития киберугроз в информационном пространстве России и способы противодействия

18+



# ОБЗОР.НЦПТИ

Выпуск № 4 (23)

Декабрь 2020



Рецензия на научно-практическое пособие «Организация контрпропаганды в области борьбы с терроризмом и экстремизмом»

**Кученко М.В.**

Восприятие экстремизма и других информационных угроз в образовательной среде Приволжского и Уральского федеральных округов: анализ результатов эмпирического исследования

**Шапошников А.А.**

Социальная сеть TikTok как инструмент распространения идеологии терроризма и экстремизма

**Вавилов А.В.**

Противоправный контент в российском сегменте сети Интернет: динамика изменений за период с 2015 по 2020 гг.

18+



Обзор.НЦПТИ № 1 (24), 20.03.2021

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»).  
Издатель: Национальный центр информационного противодействия терроризму и экстремизму в образовательной среде и сети Интернет.  
При поддержке: Минобрнауки России.

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;  
Лобода Виталий Викторович, кандидат юридических наук;  
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;  
Яковлев Максим Николаевич, кандидат политических наук.

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 редколлегии может не совпадать с мнением авторов.

Адрес учредителя: 344002, г. Ростов-на-Дону,  
пер. Газетный, 51, тел. +7 (863) 201-28-17

Адрес издателя и редакции:

344011, г. Ростов-на-Дону,

ул. Города Волос, 6, тел.: (863) 201-28-22.

Адрес типографии: 344064, г. Ростов-на-Дону,

ул. Вавилова, д. 55, ООО «Альтаир»,  
тел.: (863) 219-84-25, 8 (958) 544-59-27.

Тираж: 250 экз.

Заказ № 1001.

Подписано в печать

По графику: 25.03.2021

Фактически: 25.03.2021

## 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



В середине декабря прошлого года в онлайн-формате, ставшем характерной приметой жизни в условиях пандемии, прошел V Всероссийский научно-практический форум «Безопасность в науке и образовании».

Впервые в рамках этого форума была организована площадка «Киберволон-

терство как форпост информационной безопасности в интернете», в работе которой приняли участие почти 250 человек, среди которых представители федеральных и региональных органов исполнительной власти, а также сотрудники из 110 образовательных организаций высшего образования, находящихся в 56 субъектах Российской Федерации.

Нынешний выпуск составлен из публикаций участников форума, что нас радует, а читателям дает возможность ознакомиться с точкой зрения специалистов на ситуацию в такой тонкой сфере, как защита от кражи персональных данных, кибербуллинга, а еще поможет узнать о способах обеспечения технической и информационной безопасности неискушенных владельцев смартфонов и прочих умных средств связи, особенно школьного или пенсионного возраста. Не секрет, что подключенный к интернету гаджет зачастую обрекает его хозяина на возможные провокации, травлю или давление мошенников, действующих в соцсетях, грозит гражданину дискриминацией по самым различным признакам. И тому, как должна действовать потенциальная жертва, чтобы не стать заложником злоумышленников, призваны обучать в том числе наши добровольные помощники в рамках мастер-классов, вебинаров.

Не могу удержаться от лингвистического укора в связи с новообразованным

понятием «киберволонтер». Снова наступаем мы на грабли словозамещения, иноязычевания родной русской речи и, поддавшись магии престижного западного словечка «волонтер», отказываем исконному – «доброволец». Споры нет, немало появилось понятий и терминов, к которым трудно или даже бессмысленно

подбирать равнозначные русские слова в силу сложившихся социально-политических, технологических и экономических процессов. Но в данном случае очевидно, что «доброволец» вполне имеет право на существование, пусть и в сочетании с оправданным англицизмом «кибер».

.....

# Онлайн-курс «Интернет без угроз. Практикум для родителей»

.....

Где записаться?

[интернетбезугроз.нцпти.рф](http://интернетбезугроз.нцпти.рф)

Для кого?

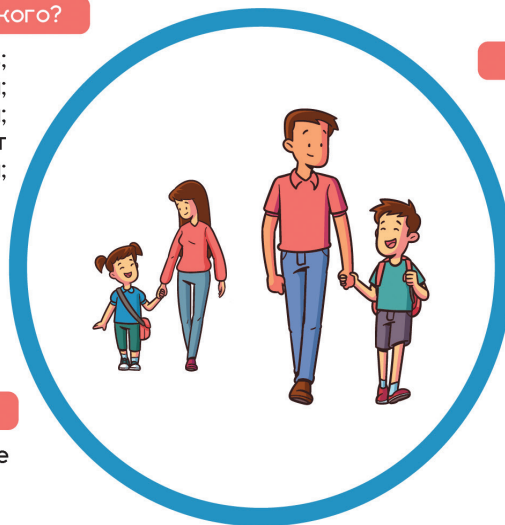
Родители школьников;  
Классные руководители;  
Детские психологи;  
Все, кто работает  
с несовершеннолетними;

Цена?

2000 рублей

Где?

Платформа Moodle



Когда?

Курс индивидуальный,  
в любое удобное для вас  
время в течение месяца  
после оплаты

Объем

15 видеолекций  
12 инфографик  
9 инструкций

.....

Остались вопросы?

[ano@ncpti.ru](mailto:ano@ncpti.ru)  
8 (863) 310-53-83

Что вы узнаете?

с какими угрозами в сети  
может столкнуться ребенок

какие признаки свидетельствуют,  
что ребенок попал под влияние  
деструктивной идеологии

какие действия в сети являются  
противоправными и могут  
повлечь правовую ответственность  
несовершеннолетних

как не поддаваться фейковой  
информации, распространяемой  
через интернет-каналы





# ПРИЁМ ЗАЯВОК ДО 15 АВГУСТА 2021 ГОДА



ВСЕРОССИЙСКИЙ  
ОНЛАЙН-ФЕСТИВАЛЬ  
СОЦИАЛЬНОГО  
МЕДИАКОНТЕНТА

**Я ПРОТИВ  
ЭКСТРЕМИЗМА  
И ТЕРРОРИЗМА**

**ГЕОГРАФИЯ: РФ И СТРАНЫ СНГ**



МИНИСТЕРСТВО НАУКИ  
И ВЫСШЕГО ОБРАЗОВАНИЯ  
РОССИЙСКОЙ ФЕДЕРАЦИИ



НЦПТИ



PM



CENTER FOR  
STUDYING  
REGIONAL  
THREATS



АЗИЯ  
ГРУПП

**VIDEOFEST.NCERTI.RU**

# Содержание

---

**10**

---

**ЖУЧЕНКО ВИКТОРИЯ СЕРГЕЕВНА**

Информационная справка по кибердобровольчеству.  
Кто такие кибердобровольцы?

**13**

---

**КУЦЕНКО МАКСИМ ВИКТОРОВИЧ**

Интервью с М. Наместниковой: Тренды развития киберугроз в информационном пространстве России и способы противодействия

**17**

---

**КУЛЯГИН ИГОРЬ ВАЛЕРЬЕВИЧ**

Об организации и кадровом обеспечении деятельности по противодействию идеологии терроризма в образовательной среде

**25**

---

**НЕПЕЙВОДА КИРА МИХАЙЛОВНА**

Киберволонтерство в условиях кризиса

**30**

---

**ВЕНЦЕЛЬ СЕРГЕЙ ВЛАДИМИРОВИЧ**

Особенности мониторинга противоправного контента в интернете в рамках киберволонтерской деятельности

**38**

---

**САЕНКО АЛЕКСАНДР ВЛАДИМИРОВИЧ**

Проект онлайн-фестиваля как комплексный метод вовлечения молодежи в создание антитеррористического контента

**45**

---

**ГЛЯНЦЕВ НИКИТА СЕРГЕЕВИЧ**

Лидеры мнений как инструмент противодействия идеологиям терроризма и экстремизма

**52**

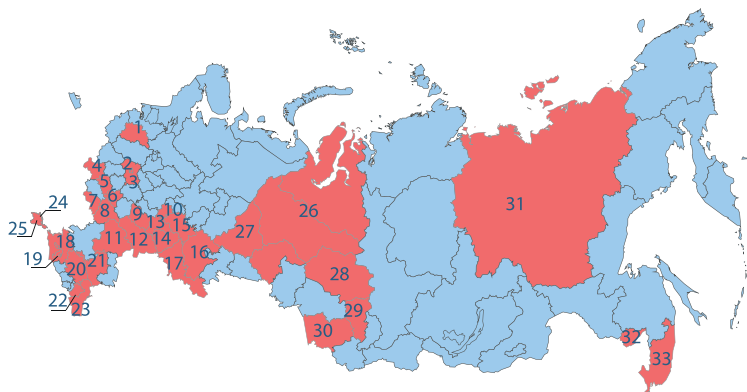
---

**ВСПОМНИМ**

Воронцов Сергей Алексеевич



## Кибердобровольцы в структуре образовательных организаций высшего образования

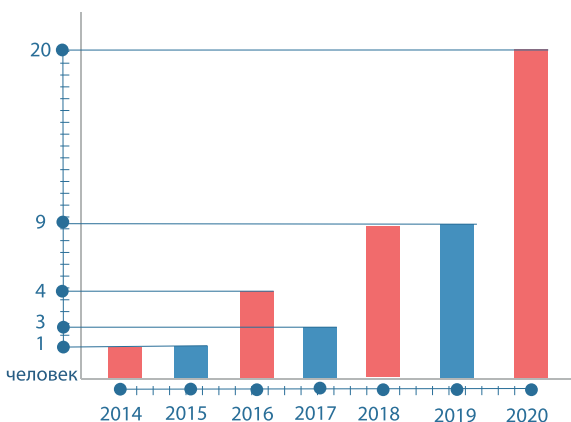


- 1 Новгородская область
- 2 Москва
- 3 Московская область
- 4 Брянская область
- 5 Орловская область
- 6 Липецкая область
- 7 Белгородская область
- 8 Воронежская область
- 9 Пензенская область
- 10 Чувашия

- 11 Волгоградская область
- 12 Саратовская область
- 13 Ульяновская область
- 14 Самарская область
- 15 Республика Татарстан
- 16 Республика Башкортостан
- 17 Оренбургская область
- 18 Краснодарский край
- 19 Республика Адыгея
- 20 Ставропольский край

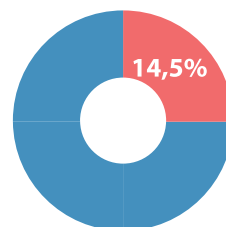
- 21 Республика Калмыкия
- 22 Республика Чечня
- 23 Республика Дагестан
- 24 Республика Крым
- 25 Севастополь
- 26 Ханты-Мансийский автономный округ
- 27 Свердловская область
- 28 Томская область
- 29 Кемеровская область – Кузбасс
- 30 Алтайский край
- 31 Республика Якутия
- 32 Еврейская автономная область
- 33 Приморский край

### Статистика роста кибердобровольческих организаций



**14,5%**

ведут информационное сопровождение своей деятельности







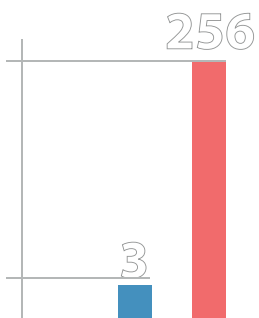
## Кибердобровольцы в структуре образовательных организаций высшего образования

**1270**  кибердобровольцев


**48**  образовательных организаций высшего образования

**33**  региона присутствия

Численный состав кибердобровольческих организаций:



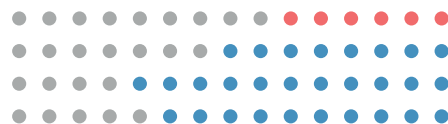
**3**  чел. - самая маленькая

**256**  чел. - самая большая

» **10-15** 

### ЧЕЛОВЕК

среднее число кибердобровольцев в организации



# Информационная справка по кибердобровольчеству. Кто такие кибердобровольцы?

*Кибердобровольчество – организация деятельности работы добровольцев, нацеленная на качественное улучшение функционирования онлайн-пространства и безопасное пребывание пользователей самых различных возрастов в интернете.*

Сейчас кибердобровольчество развито преимущественно в сфере информационного противодействия идеологии терроризма, экстремизму и другим негативным явлениям в сети (онлайн-мошенничество, кибербуллинг, утечка персональных данных и т. д.).

Сразу оговоримся, что мы рассматриваем термин «кибердоброволец» исключительно в рамках проблематики информационной безопасности и медиаграмотности. В то же самое время понятия «кибердоброволец», «киберволонтер» и «кибердружинник» подразумеваются как синонимичные. Выбор того или иного термина зависит исключительно от индивидуальных предпочтений.

В России данная деятельность начала развиваться с 2011 года (появление Лиги безопасного Интернета), а популярность набрала в 2017 году, объявленном Годом добровольца.

## **Что может сделать кибердоброволец?**

Можно выделить три ключевых направления работы ки-

бердобровольцев: выявление противоправного контента, реализация просветительских проектов и создание позитивного медиаконтента.

Важно осознавать, что мониторинг информационного пространства на предмет выявления угроз – только часть того, что может делать кибердоброволец. Высокую социальную значимость приобретают социальная реклама, видеоролики, памятки, методички, инфографика, буклеты и другие материалы, направленные на формирование культуры поведения в интернете, основ медиабезопасности, продвижения позитивных ценностей.

## **Есть ли ограничения и нюансы?**

Да, их несколько. Во-первых, целенаправленно искать противоправный контент могут только совершеннолетние граждане. Это связано с психовозрастными особенностями несовершеннолетних и с тем, что противоправный контент зачастую содержит информацию, которая подпадает под действие Федерального закона от 29.12.2010 № 436-ФЗ (ред. от 31.07.2020) «О защите детей от информации, причиняющей вред их здоровью и развитию».

Во-вторых, кибердобровольцы не подменяют своей активностью работу правоох-

ранительных органов. Они не борются с запрещенными материалами, злоумышленниками и мошенниками, а только выявляют факты нарушения закона и передают эту информацию в соответствующие инстанции.

В-третьих, является ли контент противоправным или нет решает не кибердоброволец. В российском законодательстве четко прописывается, какие именно материалы являются противоправными. На блокировку отправляется только тот контент, который действительно попадает под нормы антиэкстремистского или антитеррористического законодательства, а не просто не нравится кибердобровольцу.

### **Как регламентируется деятельность кибердобровольцев?**

Отдельного закона о работе кибердобровольцев на начало 2021 года еще нет, однако разрабатывается законопроект.

Можно выделить три ключевые формы организации деятельности киберволонтеров:

- движение при образовательной организации;
- движение при органах исполнительной власти;
- некоммерческая организация (НКО).

Почему лучше работать в составе кибердобровольческой организации, а не в одиночку? Причин несколько: обучение кибердобровольцев, психологическая поддержка и партнерские отношения с правоохранительными органами, которые могут курировать работу волонтеров.

### **Что уже сделано?**

26 ноября 2020 года в рамках V Всероссийского научно-практического форума «Безопасность в науке и образовании» была впервые организована работа онлайн-секции «Киберволонтерство как форпост информационной безопасности в интернете».

Участниками онлайн-секции на платформе Zoom стали 108 человек из 41 субъекта Российской Федерации, представлены все федеральные округа. Средний возраст участников – 26 лет (самому младшему – 17 лет, старшему – 68 лет), 74 % участников – кибердобровольцы, 26 % – руководители кибердобровольческих организаций.

Участники обратили внимание на следующие проблемы, которые предстоит решать кибердобровольцам для организации эффективной работы:

- отсутствие специализированных программ и курсов повышения квалификации, направленных на подготовку кибердобровольцев, как системного решения вопроса подготовки;
- сложности в психологическом сопровождении деятельности кибердобровольцев;
- отсутствие налаженной коммуникации между кибердобровольцами и курирующими их структурами;
- непонимание понятия «позитивный контент» в сфере противодействия идеологии терроризма и экстремизму;
- проблемы с получением обратной связи по выявленному потенциально противоправному контенту в сети.

После обсуждения наиболее актуальных проблем были внесены следующие предложения в резолюцию:

1. Создать общий канал коммуникации (telegram-канал) для обмена информацией и поиска партнеров.

Канал кибердобровольцев России: <https://t.me/joinchat/VexQVg8G08jReJ4nM9afuw>.

2. Разработать методические рекомендации по организации работы киберволонтеров на базе образовательных организаций высшего образования.

Предоставление методических рекомендаций осуществляется через официальный запрос на почту [info@ncpti.ru](mailto:info@ncpti.ru).

3. Разработать обучающие материалы (курсы повышения квалификации) для кибердобровольцев.

В 2021 году разрабатывается онлайн-курс. Свои предложения по содержанию курса можно направлять на почту [info@ncpti.ru](mailto:info@ncpti.ru).

4. Привлекать различные общественные объединения (национальные, религиозные и др.) к поиску эффективных моделей и форматов проведения профилактической работы.

Участники площадки отметили, что организация секции «Киберволонтерство как форпост информационной безопасности в интернете» – первый в России опыт объединения на одной площадке кибердобровольцев. Участники высказали желание проводить данную секцию ежегодно в рамках работы Всероссийского научно-практического форума «Безопасность в науке и образовании», проходящего под эгидой Минобрнауки России.



*Логотип движения «Интернет без угроз»*

*Интервью:*

## **Тренды развития киберугроз в информационном пространстве России и способы противодействия**

Гость рубрики «интервью» – **Мария Наместникова**, руководитель российского исследовательского центра Лаборатории Касперского, г. Москва

Интервью подготовил **Куценко Максим Викторович** – аналитик Национального центра информационного противодействия терроризму и экстремизму в образовательной среде и сети Интернет, г. Ростов-на-Дону

Мария – выпускница Московского педагогического государственного университета. Еще на пятом курсе, в 2008 году, пришла работать в «Лабораторию Касперского» спам-аналитиком. Уже тогда интересовалась проблемами информационной безопасности детей, принимала участие в целом ряде образовательных инициатив. Мария – автор более десятка статей, в том числе «Дети в Интернете», а также учебного пособия «Информационная безопасность, или На расстоянии одного вируса».

В настоящее время является частью команды GReAT (Глобального центра исследований и анализа угроз), которая занимается изучением киберугроз и способов противодействия им.

**– Прошедший год преподнёс немало сюрпризов, резонанс,**

**вызванный мировой пандемией, навсегда изменил прежнюю форму мира, взаимодействий между людьми. Всё больше стали говорить о цифровизации жизни. Скажите, в свете этого как изменятся подходы к кибербезопасности в ближайшее время?**

– На самом деле цифровизация всех сфер нашей жизни идет уже давно, пандемия лишь ускорила и подчеркнула необходимость этого процесса. Вопросы цифровой безопасности в результате становятся более актуальными, чем когда-либо, и важными для всего большего количества людей и сфер экономики. Думаю, что пандемия вряд ли принесла революцию в сферу ИТ-безопасности именно с точки зрения подходов, опыт нашей индустрии наработан годами и развитие ее происходит

вместе с развитием технологий. Тем не менее с точки зрения общественного восприятия защита цифровых пространств стала значительно понятнее людям, осознание ее необходимости возросло: чего в этом смысле стоят только атаки на медицинские учреждения, в том числе занимающиеся лечением коронавирусных больных, чьи жизни в результате действий злоумышленников оказались под угрозой. Или первый подтвержденный случай смерти пациента, которого не удалось вовремя доставить в больницу в результате атаки шифровальщика. Мы надеемся, что пандемия и ускорившаяся цифровизация заставят большее количество организаций задуматься о защите своей ИТ-инфраструктуры.

– **Дистанционный формат образования в 2020 году продемонстрировал низкий уровень информационной грамотности многих специалистов из сферы образования.**

**На Ваш взгляд, как эта ситуация будет меняться в 2021 году и есть ли уже конкретные меры со стороны государственных и частных структур, предпринимаемые для повышения уровня медиаграмотности?**

– Многие исследования еще несколько лет назад показывали в целом низкий уровень информационной грамотности в нашей стране. Ситуация, конечно, постепенно меняется, но не так быстро, как хотелось бы. Разумеется, сейчас многих специалистов в сфере образования обучили использованию отдельных

приложений, для проведения дистанционных уроков. Тем не менее даже когда речь идет об использовании этих конкретных приложений большинство учителей зачастую не до конца понимает их функциональность. Я не думаю, что в 2021 году ситуация кардинально переменится. Преподавателям не нужны будут инструктажи по использованию программ для проведения конференций, но те из них, кто далек от технологий, вероятно, вряд ли значительно продвинулся в их изучении. Это значит, что им по-прежнему нужна будет помощь в освоении технологий, необходимо расширение знаний не только по работе с конкретными приложениями, но и по цифровой среде в целом.

– **Одной из главных информационных угроз сегодня уверенно можно назвать распространение fake news. Как можно защитить себя от фейков и почему это важно?**

– Единственный путь защиты от фейков – проверять любую информацию в нескольких доверенных источниках. Под доверенными источниками подразумеваются, например, крупные новостные агентства и СМИ, в том числе заграничные. При этом надо помнить, что из-за безумного ритма работы репортеров, даже крупные и доверенные агентства в последнее время допускают публикацию непроверенной информации. Поэтому лучше спустя какое-то время перепроверить, не убрали ли эти издания «новость» или не выпустили ли они опровержения.

– **И всё-таки, говоря о мерах по обеспечению собственной безопасности в цифровом пространстве, расскажите, какие меры можно предпринять. Какие бы советы Вы могли бы дать нашим читателям?**

Основных советов несколько, и они относятся как к сфере собственного поведения людей, так и к программной части:

1. Установите защитное решение на все устройства, которыми пользуетесь. Многие сейчас устанавливают антивирус только на компьютер, не защищая свой смартфон. Злоумышленники знают об этом и вредоносное ПО для смартфонов активно распространяется.

2. Используйте сложные пароли и не храните их в браузере. Чтобы не забыть пароли используйте специальные программы – менеджеры паролей. Это так же удобно, как хранить пароли в браузере, но намного безопаснее. К тому же такие программы позволяют создавать по-настоящему надежные пароли.

3. Используйте на всех сайтах (и в приложениях), где это возможно, двухфакторную аутентификацию – проверку входа с помощью номера телефона или одного из ваших устройств или аккаунтов.

4. Не публикуйте в открытом доступе никакой информации, которая компрометирует вас и/или подвергает вас или ваших детей опасности: ответы на секретные вопросы, информация о доходах семьи, номер школы, где учится ваш ребенок, неприличные фотографии (их лучше вообще не делать).



5. Никогда не общайтесь по телефону, если вам звонят и представляются службой безопасности банка, просят предоставить данные о своем счете или карточке, установить какую-либо программу по ссылке в эсэмэс. Положите трубку и, если у вас есть сомнения, найдите в интернете или на обратной стороне своей карты номер телефона банка и уточните, пыталась ли с вами связаться служба безопасности. Ответ почти наверняка будет «нет».

– **Всё популярнее среди родителей несовершеннолетних детей становятся различные приложения и программы родительского контроля. Каким образом они работают?**

– Приложения, обеспечивающие безопасность ребенка в интернете, обладают разным функционалом. Они устанавливаются на устройство родителя (с него происходит настройка приложения) и ребенка (здесь приложение непосредственно выполняет свою задачу). Чаще всего такие

приложения выполняют следующие функции:

- ограничение доступа к интернет ресурсам (как к определенным, так и к целым категориям сайтов – порнографическим, сайтах о насилии и т. д.);
- контроль времени работы устройства в целом (в какие часы можно использовать, сколько времени можно использовать);
- ограничение доступа к определенным программам (как к конкретным, так и к целым подвидам, например, к любым приложениям соцсетей или только к определенным);
- контроль времени работы с определенными приложениями (можно ограничить время в играх или в интернете);

- ограничение доступа к контенту (фильмам, музыке, книгам) по возрастному рейтингу;

- знание о местоположении ребенка в реальном мире (это удобно, если ребенок, например, сам возвращается из школы домой).

– **Противоправного контента, в частности в социальных сетях, за последний год стало разительно больше. Помимо усиления технических мер по борьбе с ним, в деятельность по блокировке таких данных включились и кибердобровольцы – волонтеры, которые помогают защитить детей и подростков от небезопасной информации.**

**Возвращаясь к центральной теме нового выпуска Обзора. НЦПТИ, какие советы Вы могли бы дать киберволонтерам? Как повысить свои компетенции в этой сфере?**

- Сегодня есть большое количество различных сайтов, рассказывающих о тенденциях в мире информационной безопасности. Для тех, кто заинтересован в повышении своей цифровой грамотности, а не в глубоком изучении вопроса и технических деталях, я бы порекомендовала [blog.kaspersky.ru](http://blog.kaspersky.ru) – наш ресурс, где собраны истории из области ИТ-безопасности, написанные доступным языком. Если хочется углубиться в технические детали – читайте [securelist.ru](http://securelist.ru), на этом ресурсе мы публикуем статистические и технические исследования, интересные специалистам по информационной безопасности.

## Свежее



### Шифровальщики в виртуальной среде

Несколько групп злоумышленников используют уязвимости в VMware ESXi для заражения шифровальщиками.

26 марта 2021



### Развод криптотрейдеров в Discord: мекка мошенников

Рассказываем об очередной мошеннической схеме, нацеленной на участников криптовалютных серверов в Discord.

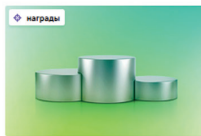
25 марта 2021



### Год красного локдауна — как COVID-19 повлиял на кибербезопасность

Смотрим на год, прошедший с начала локдауна, через призму угроз IT и рассказываем, какой след оставила пандемия в этой сфере.

24 марта 2021



### Тесты и награды независимых экспертов и решения «Лаборатории Касперского»

Рассказываем, кто и как оценивает защитные решения, и отчитываемся о тестах и наградах за прошедший год.



### Stalkerware в 2020 году: проблема все еще актуальна

Активность stalkerware уменьшилась во время пандемии, чтобы затем снова набрать обороты. Рассказываем об угрозе и о том, как с ней бороться.



### Ваш шанс выиграть PlayStation 5 (на самом деле нет)

Мошенники придумали, как нажиться на дефиците PlayStation 5. Рассказываем, как не попасться на их уловку.



# Об организации и кадровом обеспечении деятельности по противодействию идеологии терроризма в образовательной среде

**Кулягин Игорь Валерьевич** – первый заместитель руководителя аппарата Национального антитеррористического комитета, вице-адмирал, г. Москва

Благодаря последовательной, системной и скоординированной работе всех субъектов противодействия терроризму в России уже не первый год сохраняется тенденция сокращения количества преступлений террористической направленности.

Данная тенденция является результатом функционирования в стране общегосударственной системы противодействия терроризму. Ключевую роль в этой системе играет Национальный антитеррористический комитет, который организует взаимодействие субъектов противодействия терроризму, осуществляет планирование применения сил и средств федеральных органов исполнительной власти и их территориальных органов по борьбе с терроризмом, а также управление контртеррористическими операциями.

Вместе с тем эмиссары международных террористических организаций не прекращают попыток вербовать новых сторонников, в первую очередь из числа молодёжи. При этом в период ограничений, вызванных рас-

пространением новой коронавирусной инфекции, они активизировали пропагандистскую и вербовочную деятельность в социальных сетях и мессенджерах.

Это требует сосредоточения усилий в настоящее время на реализации мер профилактики.

Национальным антитеррористическим комитетом был разработан и в 2018 году утвержден Президентом России Комплексный план противодействия идеологии терроризма в Российской Федерации на 2019–2023 годы, реализуемый как на федеральном, так и на региональном и муниципальном уровнях, приоритетными задачами которого являются:

- повышение эффективности профилактической работы с лицами, подверженными воздействию идеологии терроризма, а также подпадавшими под ее влияние;

- реализация мер по формированию у населения Российской Федерации антитеррористического сознания;

- совершенствование мер информационно-пропагандистского характера и защиты ин-

формационного пространства Российской Федерации от идеологии терроризма;

– развитие организационных и иных мер, направленных на повышение результативности деятельности субъектов противодействия терроризму.

На федеральном уровне при координации Национального антитеррористического комитета федеральными министерствами осуществляется выработка организационных мер, подготовка методик профилактики, разработка программ подготовки специалистов в сфере профилактики терроризма.

Основная работа по исполнению мероприятий Комплексного плана осуществляется на региональном уровне территориальными органами ведомств во взаимодействии с органами власти субъектов

Российской Федерации при координирующей роли региональных антитеррористических комиссий.

В профилактическую деятельность активно включены представители общественных и религиозных организаций, а также лидеры общественного мнения (журналисты, спортсмены, политики, блогеры и т. д.).

Важную роль в этой работе играют образовательные организации, которым для выстраивания системной работы по противодействию идеологии терроризма необходимо обеспечивать реализацию профилактических мер в рамках образовательной деятельности, массовой работы, индивидуальной воспитательной работы с группой риска.

Так, целесообразно актуализировать содержание реализуемых в вузах образовательных программ на предмет включения в образовательный процесс вопросов, позволяющих формировать у обучающихся негативное отношение к идеологии терроризма.

Организаторы массовой работы должны стремиться к максимальному охвату культурными, спортивными, форумными и иными массовыми мероприятиями обучающихся для обеспечения их полной занятости в свободное от учебы время.

Образовательным организациям необходимо осуществлять мониторинг социального самочувствия обучающихся (анкетирование, наблюдение, беседы) и выявление групп риска в целях проведения адресной работы с привлечением опытных психологов, педагогов, представителей правоохранительных органов и духовенства. Индивидуальная работа должна осуществляться с учетом современных реалий жизни, интересов молодых людей, не быть навязчивой. Прикрепляя к обучающемуся педагога-психолога либо преподавателя для проведения индивидуальной работы нужно, конечно же, учитывать наличие у них межличностного контакта и доверительных отношений.

Работая с группами риска, важно определить наиболее эффективные формы для снижения уровня радикализации молодых людей и недопущения их вовлечения в террористическую деятельность. Преподаватели, психологи, административ-

ный состав должны не только четко понимать, как выявлять таких лиц, но и обладать твердыми знаниями как действовать в таких ситуациях.

При формировании подходов к организации профилактической работы усилия должны быть нацелены на активное задействование индивидуального подхода к каждому профилактируемому, исключение шаблонного планирования мероприятий и их формального выполнения.

С этих же позиций следует формировать подходы к созданию антитеррористического контента, который должен стать более адресным, наглядным и понятным для молодежи. Для этого целесообразно обстоятельно изучать современные тенденции и учитывать существующие практики федеральных органов власти и институтов гражданского общества при разработке таких материалов. Немаловажным также остается выбор каналов их распространения, как, например, социальные сети с максимально возможным охватом целевой аудитории, а при необходимости и целенаправленное формирование групп в социальных сетях с привлечением к работе в них молодежных лидеров и авторитетных в молодежной среде людей. Все эти мероприятия должны проводиться в сочетании с мероприятиями, которые в регионах проводят АТК.

Эффективность осуществляемой профилактической работы во многом зависит от компетенции соответствующих должностных лиц.

Помимо государственных гражданских и муниципальных служащих требуется также специальная подготовка работников образования, участвующих в противодействии распространению идеологии терроризма, а также самих педагогов, задействованных в обучении указанных категорий специалистов. На сегодняшний день уровень квалификации и профессионализма должностных лиц, занятых в этой сфере, остается недостаточным.

Совместные усилия федеральных и региональных органов власти на основе решений НАК позволили создать основу системы дополнительного образования соответствующих должностных лиц.

В рамках реализации решения Комитета от 10 апреля 2018 года Минтруд России дополнил Справочник квалификационных требований, необходимых для замещения должностей гражданской службы, новым видом деятельности – «Регулирование в сфере противодействия терроризму» и сформировал единые квалификационные требования к сотрудникам, осуществляющим такую деятельность.

В федеральных и региональных органах исполнительной власти проведена работа по дополнению должностных регламентов гражданских служащих требованиями к знаниям и умениям в области профилактики терроризма.

В настоящее время уже реализуется государственный заказ на переподготовку и повышение квалификации соответствующих

щих специалистов. Таким образом, в стране сформирована потребность в профессионалах, занимающихся противодействием терроризму, и в настоящее время осуществляется реализация мер, направленных на организацию их специальной подготовки в указанном направлении. Вместе с тем этой работе предстоит придать необходимую системность на федеральном, региональном, муниципальном уровнях и в самих образовательных организациях.

На наш взгляд, необходимо разработать обоснованную компетентностную модель специалиста в сфере противодействия терроризму и, соответственно, элементы профессионального стандарта таких специалистов, в том числе описания должностных функций сотрудников образовательных организаций, реализующих в студенческой среде мероприятия по противодействию идеологии терроризма, воспитанию у молодежи традиционных российских духовно-нравственных ценностей.

Типовой должностной регламент и квалификационные требования при объявлении конкурсов к соискателям на соответствующие должности, содержат стандартный набор требований, предъявляемых к лицам, поступающим на государственную службу. Вместе с тем конкретизированные квалификационные требования, на наш взгляд, должны содержать более подробную регламентацию в зависимости от характера исполняемых должностных обязанностей. Такие требования должны определять

все дальнейшие направления и содержание подготовки, переподготовки и повышения квалификации как государственных гражданских и муниципальных служащих, так и работников образования, участвующих в противодействии распространению идеологии терроризма.

При этом потребуются сопряжение усилий ученых и практиков для составления возможного перечня должностей, оценки основных задач в рамках антитеррористической деятельности, в решении которых принимают участие специалисты, выделения необходимых знаний, умений и навыков, необходимых указанным сотрудникам.

Это позволит сформировать механизмы оценки качества образовательных услуг, конкретизировать действующие программы переподготовки и повышения квалификации указанных должностных лиц, разработать дополнительные специализированные модули и курсы, а также более четко понять критерии оценки подготовленности специалиста.

Для решения проблемы формирования модели специалиста в сфере профилактики необходимо более активное включение в этот процесс научно-образовательного сообщества.

Для сближения теории и практики в системе антитеррористического профессионального образования особенно важно привлекать к проведению занятий экспертов – ученых и специалистов-практиков. Для этого целесообразно организовать формирование в субъектах Российской Федерации так называ-

емых пулов экспертов, которые могут быть привлечены к созданию и оценке образовательных программ и проведению занятий. При этом необходимо определить требования к ним.

Необходимо расширять взаимодействие преподавателей с группами специалистов, экспертными советами и институтами гражданского общества, а также их практическое участие в организации и проведении мероприятий по противодействию распространению терроризма на территории субъектов Российской Федерации, используя для этого возможности антитеррористических комиссий.

Решение этой задачи требует не одного дня и, действительно, нуждается в предварительном глубоком анализе. Мы ожидаем межведомственного, межвузовского обсуждения, возможно, на страницах периодических изданий НАК, чтобы сформулировать цель профессионального образования в данной сфере, определить какого же специалиста нам необходимо получить в результате.

Важным элементом системы профилактической работы в сфере антитеррора является уровень кадрового потенциала самих образовательных организаций, работающих на этом направлении.

Анализ ряда образовательных программ региональных вузов, реализуемых по линии подготовки кадров в области противодействия терроризму, свидетельствует о недостаточной подготовленности их разработчиков, слабой осведом-

ленности преподавателей о практической стороне деятельности должностных лиц, участвующих в противодействии терроризму. Как следствие, отмечается значительный дисбаланс между избыточной теорией и слабой практической составляющей подготовки. Необходимо понимать, что государственные органы, направляя своих специалистов для повышения квалификации, ожидают преимущественно практикоориентированного профессионального образования, а не формирования базовых понятий и расширения кругозора по предметам курса.

В интересах повышения информированности о проблемах противодействия терроризму в стране, а также о возможных мерах по их решению, некоторыми региональным антитеррористическими комиссиями организована разработка и направление, в том числе в образовательные организации, специализированных методических рекомендаций.

Также в рамках реализации решений Комитета сформированы учебно-методические центры, к числу задач которых относится обеспечение научно-методической и консультационной поддержкой образовательных организаций, осуществляющих подготовку должностных лиц, принимающих участие в деятельности по профилактике терроризма на региональном и муниципальном уровнях.

Под председательством министра науки и высшего образования Российской Федерации Валерия Николаевича Фалькова проведено заседание Коор-

динационного совета по вопросам формирования у молодежи активной гражданской позиции, предупреждения межнациональных и межконфессиональных конфликтов, противодействия идеологии терроризма и профилактики экстремизма.

На заседании утверждена концепция создания сети координационных центров, из которых семь являются основными, осуществляющими работу на федеральном уровне, а также 23 центра в субъектах Российской Федерации, которые планируется сформировать на базе образовательных организаций высшего образования.

Одной из рабочих групп, входящих в состав Совета, будут решаться задачи по противодействию идеологии терроризма. Руководителем этой группы назначен Чурилов Сергей Анатольевич – директор Национального центра информационного противодействия терроризму и экстремизму в образовательной среде и сети Интернет ФГАНУ «Научно-исследовательский институт «Специализированные вычислительные устройства защиты и автоматика».

Для обеспечения деятельности Совета и координационных центров как на федеральном уровне, так и в регионах на базе вузов, необходимо решить ряд задач, направленных на организацию системной деятельности по противодействию идеологии терроризма в сфере образования и в молодежной среде.

В качестве первоочередной задачи мы видим необходимость организации подготовки преподавателей

центров, разработки учебно-методических материалов, которые позволили бы обеспечить обучение достаточного количества специалистов как региональных и муниципальных органов власти, так и образовательных организаций для реализации Комплексного плана противодействия идеологии терроризма и мероприятий по другим направлениям деятельности координационных центров.

Во взаимодействии с антитеррористическими комиссиями и органами исполнительной власти субъектов требуется своевременно проработать вопросы финансирования обучения данных специалистов, а также получения по итогам соответствующих свидетельств и удостоверений.

В настоящее время довольно остро стоит вопрос о научном обеспечении деятельности по профилактике терроризма. Отмечаем наличие многих нерешенных научных проблем, в том числе ведомственную разобщенность в подходах к понятийно-терминологическому аппарату, отсутствие разработанных инструментов прогнозирования террористической активности, комплексного обоснования модели радикализации молодежи.

Оценить сегодня уровень и состояние указанного научно-го потенциала мы можем лишь в общем виде, от более точных и ответственных характеристик приходится воздержаться, потому что проблема эта практически не изучалась.

Дальнейшего развития и качественной проработки требует вопрос координации научных исследований по антитеррорис-

тической проблематике. На наш взгляд, это позволит обеспечить более активное развитие и более эффективное использование научного потенциала, сфокусированного на вопросах противодействия терроризму. Полагаем, что к этой работе следует более активно привлекать самих студентов, обеспечивая при необходимости грантовую поддержку, возможность стажировок и прохождения практики в органах власти и аппаратах АТК.

Планирование научных исследований следует приблизить к проблемам практики, чтобы разрабатывались в первую очередь назревшие проблемы. Ведь задача науки не только в том, чтобы быть одним из средств определения целей и задач противодействия терроризму, но и в том, чтобы быть средством достижения этих целей с помощью научно обоснованных рекомендаций, т. е. не только описывать и объяснять явления обстановки, но и активно участвовать в целенаправленном ее изменении, в доведении результатов научных исследований до стадии реализации.

Аппарат Комитета, антитеррористические комиссии, специалисты на местах ждут от исследователей практических рекомендаций, позволяющих эффективно решать задачи, стоящие перед субъектами противодействия терроризму (практических наставлений, аналитических записок, вскрывающих появляющиеся негативные тенденции, не всегда заметные в повседневной деятельности; информационных материалов, меняющих устояв-

шиеся представления и позволяющих по-новому подойти к решению стоящих задач).

Необходимы рекомендации для непосредственного использования в работе по всем направлениям профилактики терроризма. Нужны практикоориентированные учебники, учебные пособия, учебно-методические материалы для вузов, проводящих переподготовку и повышение квалификации сотрудников, участвующих в противодействии терроризму, а также для педагогов, осуществляющих реализацию учебных программ по направлению противодействия терроризму.

В вопросе развития научного обеспечения деятельности по профилактике терроризма, главной, на наш взгляд, является необходимость отталкиваться от запросов практики, а не от диссертационных интересов, вести научно-исследовательские работы по болевым точкам и слабым местам, а не по принципу свободного поиска проблемы и получения знания по принципу «когда-нибудь кому-нибудь пригодится», растрачивая ресурсы и научный потенциал. Аппарат Комитета, со своей стороны, готов участвовать в организации апробации, в экспертной оценке полученных научных результатов.

Как было отмечено в начале, одним из важных факторов эффективного противодействия терроризму является наличие системы подготовки профессионально компетентных специалистов, способных решать сложнейшие задачи в указанной сфере.

## НАЦИОНАЛЬНЫЙ АНТИТЕРРОРИСТИЧЕСКИЙ КОМИТЕТ

Переподготовка и повышение квалификации государственных и муниципальных служащих – это лишь часть антитеррористического образования. Пока остались без глубокого анализа программы высшего профессионального образования, затрагивающие указанную тематику.

Программы обучения в вузах должны содержать требования по формированию у обучающихся установок антитеррористического сознания, толерантного поведения и противодействия идеологии терроризма.

Будущие преподаватели, психологи, теологи, врачи, журналисты, строители, специалисты государственного и муниципаль-

ного управления, информационной безопасности, по окончании обучения должны обладать способностью организовывать и поддерживать выполнение комплекса мер по противодействию терроризму с учетом решаемых ими задач в профессиональной сфере.

В заключение полагаю необходимым отметить, что успешное решение обозначенных задач позволит обеспечить эффективность и качество реализуемых профилактических мероприятий и оказывать тем самым самое позитивное воздействие на обстановку в образовательной сфере и снизить уровень радикализации молодежи.

The screenshot displays the website nac.gov.ru with a navigation bar at the top containing links for: ГЛАВНАЯ, НАК, ЗАКОНОДАТЕЛЬСТВО, ПУБЛИКАЦИИ, МЕЖДУНАРОДНОЕ СОТРУДНИЧЕСТВО, and КОНТАКТЫ. The main content area features a grid of video thumbnails from various meetings and conferences. On the right side, there is a 'В ЦЕНТРЕ ВНИМАНИЯ' (In the Spotlight) section with news items dated 24.02.2021, 10.03.2021, and 09.02.2021. Below this is a 'НОВОСТИ' (News) section with items dated 09.02.2021, 20.01.2021, and 26.12.2020. At the bottom, there is a blue navigation bar with buttons for: Конференции и круглые столы, Хроника событий, НАК принимает решения, Контртеррористические операции, Пресс-конференции и брифинги, Терроризму—нет!, АТК в регионах, and Антитеррористические учения.



# Киберволонтерство в условиях кризиса

**Непейвода Кира Михайловна** — кандидат филологических наук, научный сотрудник Национального центра информационного противодействия терроризму и экстремизму в образовательной среде и сети Интернет по аналитической работе, г. Ростов-на-Дону

Пандемия коронавируса обострила проблему распространения не только информации, которая нарушает законодательство Российской Федерации, но и информации, которая не соответствует действительности.

Два Федеральных закона от 18 марта 2019 года: № 27-ФЗ «О внесении изменений в Кодекс Российской Федерации об административных правонарушениях», а также ФЗ № 31-ФЗ «О внесении изменений в статью 15-3 Федерального закона «Об информации, информационных технологиях и о защите информации» — СМИ окрестили антифейковым законодательством.

Оба закона запрещают распространять в интернете информацию, которая создает «угрозу причинения вреда жизни или здоровью граждан, имуществу, угрозу массового нарушения порядка и общественной безопасности, угрозу создания помех функционирования или прекращения функционирования объектов жизнеобеспечения, транспортной или социальной инфраструктуры, кредитных

организаций, объектов энергетики, промышленности или связи».

Очевидно, что бесконтрольно распространяемая непроверенная информация может провоцировать панические настроения в обществе. И изменения, вводимые законодательством, — это попытка сдержать поток подобной информации.

Параллельно мессенджеры начали вводить ограничения на пересылку сообщений. Так, в условиях пандемии коронавируса WhatsApp ограничил пересылку чужих сообщений до одного раза [1].

И государственные, и коммерческие структуры отметили рост количества фейковой информации в сети [2–4]. Ученые создали Энциклопедию коронавирусных слухов и фейков [5].

Одна из ключевых задач киберволонтерства — мониторинг интернет-пространства с целью выявления информации, нарушающей законодательство Российской Федерации.

Очевидно, что в условиях пандемии возрастает роль киберволонтерства как ресурса, который

позволяет уменьшить количество недостоверной информации в интернет-пространстве. Для этого киберволонтеру нужно не просто знать алгоритм поиска и ключевые слова, но и уметь воспринимать информацию критически.

Безусловно, это умение играет важную роль во все времена и для всего человечества. И неважно, какие процессы происходят в социуме. Но сейчас умение отделить зерна от плевел (информацию, соответствующую действительности, от фейка, слуха, манипуляции) становится жизненно важным.

Мышление – способность человека мыслить, рассуждать, делать умозаключения [6].

Критическое мышление – «система суждений, которая используется для анализа вещей и событий с формулированием обоснованных выводов и позволяет выносить обоснованные оценки, интерпретации, а также корректно применять полученные результаты к ситуациям и проблемам» («Критическое мышление: отчёт об экспертном консенсусе в отношении образовательного оценивания и обучения» [7].

Разница между критическим и докритическим мышлением упрощенно представлена на схеме 1.

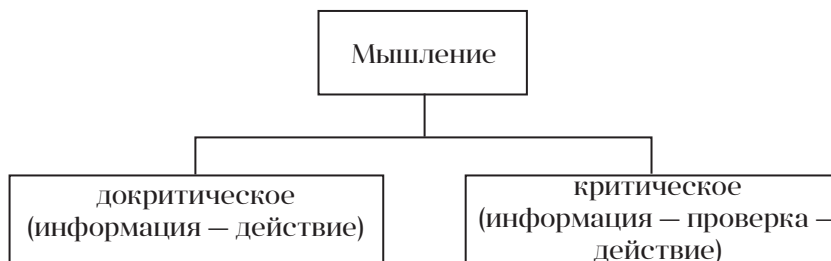


Схема 1.

*Соотношение докритического и критического мышления*

Важным элементом критического мышления является проверка информации. Именно этот этап позволяет человеку выявлять фейки, не поддаваться на уловки мошенников и сохранять спокойствие в непростые времена.

Критическому мышлению противостоит докритическое. С его помощью человек воспринимает информацию, например, в детстве, до определенного возраста не подвергая сомнению

то, что говорят ему старшие: родители, учителя и т. д. Однако нельзя утверждать, что, становясь взрослым, человек автоматически начинает пользоваться критическим мышлением. Иногда люди просто не умеют анализировать информацию и верят всем на слово, иногда (чаще всего под воздействием эмоций) забывают о том, что получаемые сведения стоит перепроверять.

В эпоху так называемой пост-правды, когда огромное количество

тво фейков наполняет интернет, умение критически оценивать и перепроверять информацию, находить источники, которые заслуживают доверия, становится жизненно необходимым.

Задача киберволонтера – ставить под сомнение получаемую информацию и проверять ее. Алгоритм проверки информации может быть следующим:

1. Обращать внимание на источник информации.

Насколько он авторитетный, заслуживает ли доверия. При этом важно помнить, что от ошибок никто не застрахован.

2. Искать первоисточник информации.

«Дядя работает в полиции и рассказал...», «знакомый из администрации» – источники, которым не стоит доверять. Проверять необходимо и время публикации. Это касается любого формата: текста, фотографий, иллюстраций, видеороликов, аудиосообщений. Известны случаи, когда один и тот же фейк с незначительными модификациями появляется снова спустя какое-то время.

3. Сопоставлять данные из нескольких независимых источников.

Будьте предельно внимательны. Есть проекты, которые создают псевдоновости (например, проекты «Панорама» и Onion).

4. Обращать внимание на эмоциональный фон.

Многочисленные восклицательные знаки, капслок, глаголы в форме повелительного наклонения и т. д. – повод насторожиться.

5. Фиксировать ошибки.

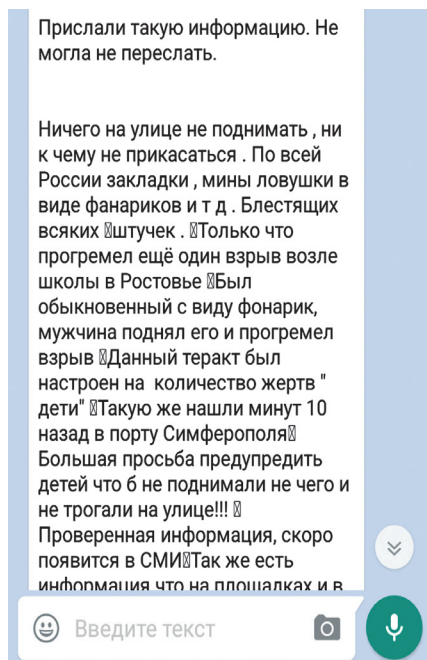
Ошибки могут быть орфографическими, грамматическими, логическими. В фейковых сообщениях обычно их чрезмерно много.

Стоит отметить, что ошибки сами по себе, конечно, не указывают на то, что перед нами сообщение, которому не стоит доверять.

Основными причинами создания фейков считаются трафик и троллинг. Иногда фейки создаются ради развлечения, иногда – чтобы отомстить.

Если речь идет о рассылках в мессенджерах, то чаще всего в их основе лежит эмоциональный компонент. Так, в подавляющем большинстве случаев сообщения, которые распространяются через родительские чаты – это предупреждения о потенциальной опасности для детей. И это логично: под влиянием сильных эмоций мы перестаем мыслить рационально. А именно это и требуется в подобных ситуациях, чтобы спокойно проанализировать поступившую информацию и понять, надо ли бить тревогу или можно просто не реагировать.

Например, в апреле 2017 года в Ростове-на-Дону взорвался предмет, похожий на фонарик [8]. При взрыве пострадал один человек. Событие произошло рядом с одной из школ города. Официальная информация появилась только к концу дня, что спровоцировало рост слухов. Впоследствии было несколько волн информационной атаки в мессенджерах не только в городе, но и далеко за его пределами (см. рисунок 1).



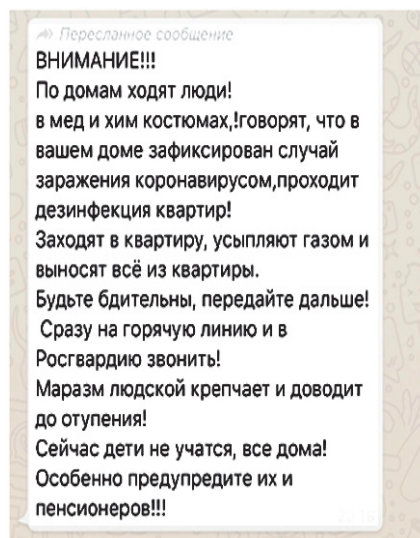
*Рисунок 1. Скриншот  
фейкового сообщения о  
возможном теракте*

Подобную реакцию можно было наблюдать во время пандемии во время появления слуха о грабителях в защитных костюмах (см. рис. 2).

В основе распространения подобных фейков лежит страх за жизнь и здоровье близких. Именно это заставляет даже здравомыслящих людей усомниться в ложности подобной информации и распространить ее дальше.

В связи с этим в процессе выстраивания работы киберволонтерских отрядов важно не только обучить непосредственно киберволонтеров выявлению недостоверной информации, но и проводить обучающие мероприятия для широких слоев населения, чтобы люди могли самостоятельно анализировать поступающую

к ним информацию и понимать, как следует на нее реагировать. Кроме того, важно донести мысль о том, что распространяя информацию, человек как бы узаконивает ее. Информация, повторенная неоднократно, начинает восприниматься как общее место. Безусловно, не всегда можно убедить того, кто переслал фейк, что он/а вводит читателей в заблуждение, однако это не означает, что не надо пытаться. И перед киберволонтерскими организациями стоит задача не только по выявлению недостоверной или потенциально опасной информации, информации, которая нарушает законодательство Российской Федерации, но и по информированию и обучению граждан Российской Федерации о том, как вычислять фейки, как проверять и что предпринимать в том случае, если человек с подобной информацией столкнулся.



*Рисунок 2. Скриншот  
фейкового сообщения о  
грабителях*

### Литература и ссылки

1. WhatsApp ввел новые ограничения на пересылку сообщений [Электронный ресурс] // URL: <https://tass.ru/obschestvo/8180289> (публикация от 7.04.2020) (дата обращения 19.02.2020).

2. Количество фейков в интернете выросло в 10 раз за время пандемии [Электронный ресурс] // URL: <https://tass.ru/obschestvo/8673695> (публикация от 8.06.2020) (дата обращения 19.02.2020).

3. Group-IB заявила об обнаружении фейковых сообщений о коронавирусе [Электронный ресурс] // URL: <https://www.kommersant.ru/doc/4275407> (публикация от 2.03.2020) (дата обращения 19.02.2020).

4. Эксперты расследуют вброс фейковых новостей о коронавирусе в Москве [Электронный ресурс] // URL: <https://ria.ru/20200410/1569836770.html>

(публикация от 10.04.2020) (дата обращения 19.02.2020).

5. Энциклопедия коронавирусных слухов и фейков [Электронный ресурс] // URL: <https://nplus1.ru/material/2020/04/08/coronarumors> (дата обращения 19.02.2020).

6. Словарь русского языка: В 4-х т. / РАН, Ин-т лингвистич. исследований; Под ред. А. П. Евгеньевой. – 4-е изд., стер. – М.: Рус. яз.; Полиграфресурсы, 1999.

7. Critical Thinking: A Statement of Expert Consensus for Purposes of Educational Assessment and Instruction. Executive Summary // Dr. Peter A. Facione (Dean of the College of Arts and Sciences, Santa Clara University), перевод Е. Н. Волкова.

8. Следователи ищут причастного к взрыву возле школы в Ростове-на-Дону [Электронный ресурс] // URL: <https://tass.ru/proisshestviya/4160355> (публикация от 6.04.2017) (дата обращения 19.02.2020).



# Особенности мониторинга противоправного контента в интернете в рамках киберволонтерской деятельности

**Венцель Сергей Владимирович** — аналитик Национального центра информационного противодействия терроризму и экстремизму в образовательной среде и сети Интернет, г. Ростов-на-Дону

Проблема проникновения и распространения в интернете идей деструктивных течений по-прежнему сохраняет свою актуальность. Эффективное противостояние таким угрозам, как пропаганда идеологии терроризма, радикальных нарративов экстремистских течений, влияние так называемых «групп смерти» и т. д. требует более активного вовлечения самих пользователей интернета в общую систему информационного противодействия и профилактики. Такая потребность стала катализатором возникновения киберволонтерства как разновидности волонтерской деятельности, осуществляемой дистанционно с помощью интернет-технологий. В сферу противодействия идеологии терроризма и экстремизма, а также различным информационным угрозам и другим негативным явлениям в интернете киберволонтерство проникло значительно

позже появления самого феномена киберволонтерства. Именно этим можно объяснить, что само понятие до сих пор не нашло закрепления в современном российском законодательстве федерального уровня. Поэтому киберволонтеры в своей деятельности опираются в первую очередь на Федеральный закон от 11.08.1995 № 135-ФЗ «О благотворительной деятельности и добровольчестве (волонтерстве)», а также на ряд других нормативно-правовых актов.

Киберволонтерские организации концентрируются на выполнении следующих задач: мониторинг и выявление противоправного контента в интернете; создание и распространение позитивного профилактического контента, организация и проведение адресных профилактических мероприятий среди целевых групп, наиболее подверженных влиянию деструк-

тивных течений. В данной научно-исследовательской работе следует сосредоточиться на анализе поиска и выявления противоправного контента как информации, содержание которой нарушает действующее законодательство Российской Федерации. Качественный мониторинг противоправного контента предполагает наличие у киберволонтера определенного набора знаний и умений, включая знание действующего российского законодательства и владение инструментами и механизмами поиска и выявления противоправного контента.

При мониторинге противоправного контента киберволонтеру следует опираться на трактовку деструктивных явлений в актуальных нормативно-правовых актах. Опора на законодательную базу позволит избежать возможных неточностей и неопределенностей смыслов (особенно это касается экстремистского и террористического контента), свойственных различных гуманитарным направлениям, включая философию и политологию. В своей работе киберволонтер сталкивается с такими формами противоправного контента, как экстремистский, террористический, наркотический и суицидальный. Следует проанализировать каждый из них.

Понимание сущности экстремистского контента основывается на той информации, которая содержится в Федеральном законе от 25.07.2002 г. № 114-ФЗ «О противодействии экстремистской деятельности» и Стратегии противодействия экстремизму в

Российской Федерации до 2025 г. (утв. Президентом РФ 28.11.2014 № Пр-2753), а также подробно прописанных в них определенных таким понятиям, как «экстремизм / экстремистская деятельность», «экстремистская организация», «экстремистские материалы», «экстремистская идеология» и «экстремистские проявления».

Термин «экстремизм / экстремистская деятельность» имеет 13 характеристик: насильственное изменение основ конституционного строя и (или) нарушение территориальной целостности РФ; публичное оправдание терроризма и иная террористическая деятельность; возбуждение социальной, расовой, национальной или религиозной розни; нарушение прав, свобод и законных интересов человека и гражданина в зависимости от его социальной, расовой, национальной, религиозной и языковой принадлежности или отношения к религии и т. д.

Экстремистской организацией является то общественное или религиозное объединение, в отношении которого судом принято решение о ликвидации или запрете в связи с осуществлением экстремистской деятельности.

Экстремистскими признаются те материалы, которые призывают к осуществлению экстремистской деятельности либо обосновывающие или оправдывающие необходимость осуществления такой деятельности. Здесь следует использовать Федеральный список экстремистских материалов, составляемый Министерством юстиции

#	Материал	Дата
1	Музыкальный альбом "Музыка белых", автор - Музыкальная группа Order, решение вынесено Первомайским районным судом г. Омска от 23.11.2006;	
2	Книга "Книга единобожия", автор - Мухаммад ибн Сулейман ат-Тамими, источник публикации - Некоммерческое партнерство "Издательский дом "Бадр", решение вынесено Савеловским районным судом г. Москвы от 02.04.2004;	
3	Письма Рады земли Кубанской духовно-родовой державы Русь, авторы - Н.М. Лозинский, В.М. Герасев, решение вынесено Первомайским районным судом г. Краснодара от 20.03.2006;	
4	Печатные материалы в газете "Для русских людей" N 1(1), июнь 2002 г.; N 2 (2), август 2002 г.; N 3, октябрь 2002 г.; N 4, ноябрь 2002 г.; N 5, декабрь 2002 г.; 2003 г. N 6, 7, решение вынесено Тихвинским городским судом Ленинградской области от 25.05.2004;	
5	Кинофильм "Вечный жид", решение вынесено Тихвинским городским судом Ленинградской области от 25.05.2004;	
6	Брошюра "Мать-земля: чудо-чудное, диво-дивное. Введение в геобиологию", автор - А.А. Добровольский, источник публикации - КОГУП "Котельничская типография", решение вынесено Котельничским районным судом Кировской области от 09.03.2005;	
7	Брошюра "Язычество как волшебство", автор - А.А. Добровольский, источник публикации - КОГУП "Котельничская типография", решение вынесено Котельничским районным судом Кировской области от 09.03.2005;	

*Рисунок 1. Федеральный список экстремистских материалов*

Российской Федерации на основе судебных решений о признании материалов противоречащими закон [3].

В Стратегии экстремистская идеология определяется как «совокупность взглядов и идей, представляющих насильственные и иные противоправные действия как основное средство разрешения конфликтов», а экстремистские проявления — как особого рода противоправные действия [6].

Экстремистский контент в форме публикаций, репостов и комментариев в социальных будет обладать следующими признаками:

- содержание публичного оправдания и поддержки деятельности как террористических и экстремистских организаций, так и отдельных личностей, ответственные за террористические и экстремистские действия;
- наличие призывов к социальной, расовой, национальной

или религиозной розни, совершению насилия на основании таких признаков;

- пропаганда идей исключительности человека или определенной социальной группы на основании определенных признаков (национальный, религиозный, социальный, языковой или расовый);
- публичная демонстрация нацистской символики, атрибутики экстремистских сообществ и организаций.

Ключевыми законодательными актами для понимания сущности террористического контента является Федеральный закон от 06.03.2006 г. № 35-ФЗ «О противодействии терроризму» и Концепция противодействия терроризму в Российской Федерации (утверждена Президентом РФ 5.10.2009 г.). Согласно упомянутому закону, терроризм представляет собой «идеологию насилия и практику воздействия на принятие решений органами



государственной власти, органами местного самоуправления или международными организациями, связанными с устрашением насилия и иными формами противоправных насильственных действий» [4]. Обозначенная Концепция подробно раскрывает тенденции и факторы развития терроризма. Важным для понимания явления термином является «террористическая деятельность», содержащая шесть характеристик. Они коррелируются с типами террористического контента в интернете, а именно:

- оправдание и пропаганда террористической деятельности;
- публичные призывы к осуществлению террористической деятельности;
- финансирование терроризма путем организации сбора средств, своеобразных «пожертвований»;
- вербовка и вовлечение в террористическую деятельность.

Террористический контент в интернете обладает следующими особенностями:

- распространение символики террористических организаций. Наиболее «популярной» среди адептов террористических течений в интернете является символика (флаг и печать) ИГИЛ (террористическая организация, запрещена на территории РФ);
- публикация фотографий и положительной информации об известных террористах: от организатора терактов 22.07.2011 года в Осло Андерса Брейвика до экслидера международной исламистской террористической организации «Аль-Каида»;

– выдержки из священных религиозных книг с радикальной интерпретацией. Несмотря на то, что цитаты из Корана не могут попадать под противоправный контент, вольная интерпретация смыслов, к которой часто прибегают радикально настроенные пользователи, может нарушать действующее законодательство в части пропаганды идеологии терроризма и экстремистских идей;

- инструкции по изготовлению взрывчатых веществ и огнестрельного оружия из подручных материалов;
- методы ведения партизанской войны в различных условиях и т.д.

Понимание сущности наркотического контента обеспечивается за счет изучения Федерального закона от 08.01.1998 г. № 3-ФЗ «О наркотических средствах и психотропных веществах» и Стратегия государственной антинаркотической политики Российской Федерации на период до 2030 года (утверждена Указом № 733 Президента РФ от 23.11.2020 г.) Наркотиками, согласно законодательству, признаются «наркотические средства и психотропные вещества, включенные в Перечень наркотических средств, психотропных веществ и их прекурсоров, подлежащих контролю в Российской Федерации, аналоги наркотических средств и психотропных веществ, новые потенциально опасные психоактивные вещества, а также растения, содержащие наркотические средства или психотропные вещества либо их прекурсоры, включен-

ные в Перечень растений, содержащих наркотические средства или психотропные вещества либо их прекурсоры и подлежащих контролю в Российской Федерации» [2]. Наркотический контент в социальных сетях, на видеохостингах и в мессенджерах имеет следующие формы: реклама наркотиков; пропаганда наркотического образа жизни; каналы продажи наркотиков; вербовка в так называемые закладчики и наркокурьеры.

И еще один вид противоправного контента, с которым регулярно сталкиваются киберволонтеры – суицидальный. В данном случае киберволонтеру следует знать о Федеральном законе от 29 декабря 2010 г. N 436-ФЗ «О защите детей от информации, причиняющей вред их здоровью и развитию», причиняющей вред их здоровью и развитию». Такой контент, распространяемый преимущественно в тематических сообществах в социальных сетях, обладает следующими опознавательными признаками: описание способов самоубийства; шок-контент (публикации порезов, сцен смерти и т. д.), героизация совершивших суицид подростков, побуждения к совершению самоубийства.

Процедура мониторинга противоправного контента в интернете имеет одну важную особенность: к данной деятельности категорически нельзя привлекать несовершеннолетних, так как это нарушение законодательства. В частности 436-ФЗ, прописывающий виды информации, причиняющие вред здоровью и развитию детей: от по-

буждающей детей к совершению действий, представляющих угрозу их жизни и жизни окружающих до обосновывающей или оправдывающей жестокость и насилие к отношению людей и целых социальных групп [1]. Также стоит отметить нежелательность привлечения и взрослых к киберволонтерской деятельности в том случае, если они не прошли специальное обучение и не обладают психологической устойчивостью. Поскольку контент, выявляемый киберволонтерами, может иметь крайне негативные моменты, способные разрушить психику человека.

Помимо знания законодательных основ по противодействию противоправному контенту, киберволонтер должен обладать навыками поиска информации. Такой поиск осуществляется либо в ручном режиме с использованием специального перечня ключевых слов, либо с помощью специальных автоматизированных поисковых систем, собирающих сведения также на основе заданных слов или выражений. Киберволонтеру следует использовать оба метода поиска в силу их взаимодополняемости и нивелирования недостатков каждого метода по отдельности при одновременном использовании. Автоматизированная поисковая система создает и предоставляет киберволонтеру условное поле, обнаружить противоправный контент, в котором можно лишь с помощью ручного поиска и детализированной работы со смыслами. Именно работа с смысловыми единицами позволяет киберволонтеру определить

для себя, действительно ли обнаружен контент, имеющий признаки противоправного.

Заключительным аспектом мониторинга является систематизация и передача найденного контента в правоохранительные органы для последующего реагирования. Если киберволонтер действует в рамках определенной киберволонтерской организации, то проблема правильно передать обнаруженный материал для него не является актуальной. Поскольку при создании киберволонтерской организации ее руководство должно наладить сотрудничество с правоохранительными органами и всеми заинтересованными сторонами. Позитивным примером является история создания Регионального общественного движения Ростовской области «Интернет без угроз», в Координационный совет вошли представители от [5]:

- Управления ФСБ России по Ростовской области;
- Главное Управление МВД России по Ростовской области;
- Следственное управление Следственного комитета России по Ростовской области;
- аппарат антитеррористической комиссии Ростовской области;
- Комитет по молодежной политике Ростовской области;
- Управления Роскомнадзора по Ростовской области;
- Министерство общего и профессионального образования Ростовской области;
- Национальный центр информационного противодействия терроризму и экстремизму в образовательной среде и сети Интернет.



Рисунок 2. Волонтеры наших проектов

Четко выстроенная структура партнерства позволяет оперативно передавать найденную информацию в правоохранительные органы для последующего реагирования. Однако в том случае, если киберволонтер действует самостоятельно, у него есть два способа передать обнаруженную информацию: либо напрямую в правоохранительные органы; либо через зарекомендовавшие себя киберволонтерские организации.

В первом случае киберволонтеру следует знать о том, какой противоправный контент в какой орган следует направлять. В Прокуратуру Российской Федерации следует направлять экстремистский контент, инструкции по изготовлению взрывчатых веществ, информацию о незаконном обороте оружия, суицидальный контент и т. д. В случае нахождения наркотического контента, пропаганды суицида, порнографии с участием несовершеннолетних, экстремистского контента и некоторых других видов незаконной информации следует обращаться в Главное Управле-

ние МВД Российской Федерации. Террористический контент следует отправлять в Управление ФСБ Российской Федерации. Важно отметить, что блокировкой противоправного контента занимается Роскомнадзор. Возможны два варианта блокировки: досудебная; и по решению суда. Досудебная блокировка осуществляется по требованию прокуратуры в следующих случаях: ресурсы с детской порнографией; пропаганда суицида; пропаганда наркотиков; ресурсы с призывами к экстремизму и массовым беспорядкам.

Во втором случае киберволонтеры могут передавать найденную информацию в имеющие хорошую репутацию киберволонтерские организации или специальные центры по сбору таких данных. Позитивной практикой является дифференцированный сбор сведений о противоправном контенте, практикуемый в НЦПТИ. Ссылки на противоправный контент может присылать как специально созданный на сайте сервис «Сообщить о противоправном контенте», так и через сообщества в социальной сети «ВКонтакте». Отдельным показательным моментом в деятельности НЦПТИ являются регулярно проводимые тематические онлайн-акции по поиску противоправного контента. В период с января по декабрь 2020 года специалистами НЦПТИ совместно с представителями регионального общественного движения «Интернет без угроз» и киберволонтерами со всей России было проведено четыре акции по поиску нарко-

тического контента, фейковой информации о коронавирусной инфекции, террористического контента, а также информации, содержащей разжигание межнациональной и межрелигиозной вражды и ненависти. В общей сложности за время проведения онлайн-акций было найдено свыше 700 гиперссылок на противоправный контент. По итогам анализа специалистами НЦПТИ из присланных материалов отобрано 195 ссылок на материалы, пропагандирующие идеологию терроризма и экстремизма, 32 ссылки на фейковую информацию о коронавирусной инфекции и 25 – по незаконному распространению наркотических средств. Участниками онлайн-акций стали киберволонтеры из более чем 20 субъектов Российской Федерации, включая Ростовскую область, Краснодарский край, Москву, Мурманскую область, Челябинскую область, Республику Калмыкия, Оренбургскую область и др.

Таким образом, эффективный мониторинг противоправного контента, осуществляемый киберволонтерами как обязательный элемент деятельности, складывается из нескольких составляющих. Во-первых, расширение знаний действующего российского законодательства в области противодействия информационным угрозам. Во-вторых, совершенствование навыков поиска и выявления противоправного контента, в том числе работы со смыслами. И, в-третьих, установление постоянных каналов коммуникации с правоохранительными органами



Рисунок 3. Результаты онлайн-акции по поиску противоправного контента

с целью передачи найденного материала для блокировки.

### Литература и ссылки

1. О защите детей от информации, причиняющей вред их здоровью и развитию: Федеральный закон от 29.12.2010 г. № 436-ФЗ (принят Государственной Думой 21.12.2010 г.; одобрен Советом Федерации 24.12.2010 г.) [Электронный ресурс]. URL: <https://rg.ru/2010/12/31/deti-inform-dok.html> (дата обращения: 07.02.2021 г.)

2. О наркотических средствах и психотропных веществах: Федеральный закон от 08.01.1998 г.

№ 3-ФЗ (принят Государственной Думой 10.12.1997 г.; одобрен Советом Федерации 24.12.1997 г.) [Электронный ресурс]. URL: [http://www.consultant.ru/document/cons\\_doc\\_LAW\\_17437/](http://www.consultant.ru/document/cons_doc_LAW_17437/) (дата обращения: 07.02.2021 г.)

3. О противодействии экстремистской деятельности: Федеральный закон № 14-ФЗ (принят Государственной Думой 27.06.2002 г.; одобрен Советом Федерации 10.07.2002 г.) [Электронный ресурс]. URL: <https://rg.ru/2002/07/30/extremizm-dok.html> (дата обращения: 07.02.2021 г.)

4. О противодействии терроризму: Федеральный закон от 06.03.2006 г. № 35-ФЗ (принят Государственной Думой 26.02.2006 г.; одобрен Советом Федерации 01.03.2006 г.) [Электронный ресурс]. URL: <https://rg.ru/2006/03/10/borba-terrorizm.html> (дата обращения: 07.02.2021 г.)

5. Положение о региональном общественном движении «Интернет без угроз» (утвержден на заседании антитеррористической комиссии Ростовской области 21.12.2017 г.) [Электронный ресурс]. URL: <https://ncpti.su/upload/polozhenie-IWT.pdf> (дата обращения: 07.02.2021 г.)

6. Указ Президента Российской Федерации от 29.05.2020 г. № 344 «Об утверждении Стратегии противодействия экстремизму в Российской Федерации до 2025 года». [Электронный ресурс]. URL: <http://kremlin.ru/acts/bank/45555> (дата обращения: 07.02.2021 г.).

# Проект онлайн-фестиваля как комплексный метод вовлечения молодежи в создание антитеррористического контента

**Саенко Александр Владимирович** — аналитик Национального центра информационного противодействия терроризму и экстремизму в социальных сетях и сети Интернет, г. Ростов-на-Дону

Задача профилактики терроризма и экстремизма, заложенная в Комплексном плане противодействия идеологии терроризма в Российской Федерации на 2019–2023 годы (утвержден Президентом Российской Федерации 28 декабря 2018 года № Пр-2665), продолжает оставаться актуальной все последние годы [1, 2, 3]. Практика показала преимущество нестандартных форм профилактики, вовлекающих целевую аудиторию в творческий созидательный процесс.

В отличие от распространенного формата лекций, конкурсы и фестивали способствуют более активному вовлечению целевой аудитории в профилактический процесс. Одно из мероприятий, реализующих данное направление, — фестиваль социального медиаконтента «Я против терроризма и экстремизма», который проводит Национальный центр информационного противодействия терроризму

и экстремизму в образовательной среде и сети Интернет под эгидой Министерства науки и высшего образования Российской Федерации. Фестиваль проходит в рамках исполнения мероприятий по пункту 2.2.1 Комплексного плана и представляет собой интернет-конкурс медиаматериалов и интернет-ресурсов, посвященных профилактике распространения экстремизма и идеологии терроризма в молодежной среде.

Неизменными целями Фестиваля (пункт 1.4. текущего Положения) является вовлечение молодежи в общественно значимую деятельность по профилактике терроризма и экстремизма, в том числе посредством сети Интернет.

Задачами Фестиваля (пункт 1.5. текущего Положения) являются:

– содействие формированию у молодежи неприятия экстремизма и терроризма и их идеологии;

– содействие способности противостоять информационным угрозам;

– повышение роли молодежных сообществ и студенческих организаций образовательных организаций высшего образования в профилактике экстремистской и террористической идеологии;

– создание базы материалов и перечня интернет-ресурсов, направленных на информационное противодействие пропаганде терроризма и экстремизма с использованием новых технологий, для их дальнейшего распространения в сети Интернет и молодежной среде.

Первый фестиваль социального контента «Я против терроризма и экстремизма» был проведен в 2017 году. Именно тогда были созданы фирменный стиль фестиваля, название, лендинг (одностраничный сайт), а также определена процедура проведения. На тот момент к участию в фестивале принимались только видеоматериалы.

Фестиваль 2017 года привлек 140 человек (138 заявок) из 40 регионов Российской Федерации. Из них проверку на технические требования прошли 63 видеоматериала – 37 созданных авторскими коллективами и 26 – одиночными авторами. Остальные не соответствовали техническим или содержательным требованиям, из-за чего были отклонены. Более 2000 человек принимали участие в финальном голосовании.

В отборочной кампании Фестиваля 2019 года приняли участие 80 человек. Техническую

проверку прошли 46 материалов. Данный фестиваль характерен возросшей диверсификацией прошедшего материала – 23 изображения, 12 социальных роликов, 9 текстов, а также по одному подкасту и флешмобу.

В 2020 году численные показатели Фестиваля составили более 60 заявок, из них 53 были допущены к основному конкурсу. Наибольшее количество работ было подано участниками из Центрального федерального округа (25 % от общего числа заявок), Южного федерального округа (19 %) и Уральского федерального округа (15 %). В форматах преобладали изображения (23 заявки) и видеоролики (20 заявок), однако были и тексты (пять заявок), аудиоподкасты (три), сайт, группа «ВКонтакте» и одна видеигра.

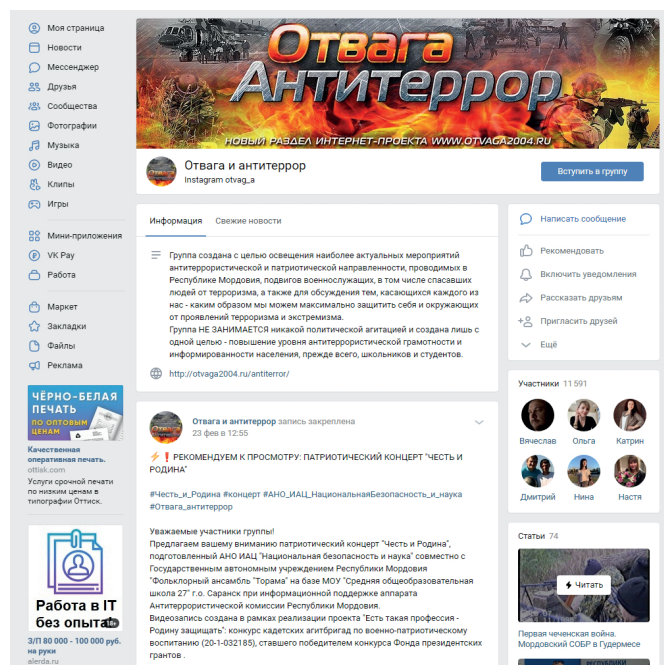


Рисунок 1.

Проект-победитель Фестиваля 2020 года

Обязательные критерии отбора в целом оставались неизменными в течение всего периода проведения Фестивалей. Первым из них являлся возраст автора или, по крайней мере, одного из участников коллектива – от 18 до 30 лет. Не допускались работы, не соответствующие задачам и целям Фестиваля. Кроме того, отклонялись произведения, содержащие символику запрещённых организаций, фрагменты и цитирования материалов, включённых в Единый реестр запрещённых материалов или же прямо пропагандирующие межнациональную, межрасовую или иную рознь. По морально-этическим соображениям отклонялись работы, содержащие элементы или сцены насилия.

Большую часть отклонённых за 2017–2020 годы материалов составляют не соответствующие вышеуказанным критериям, оставшаяся – не соответствующие техническим. Таким образом, несмотря на некоторую нестабильность в числе поданных заявок, соотношение отобранных участников к заявкам неуклонно возрастает, что позволяет говорить о качественном росте участников. Кроме того, остаётся стабильным количество голосующих в финальной части Фестиваля.

Традиционно высокую долю материалов с 2019 года составляют изображения: фотоакции, рисунки, агитационные плакаты. Доля и количество текстов, наоборот, упали к 2020 году. Наблюдается некоторая тенденция к росту числа подкастов (0 в 2017, 1 в 2019 и 3 в 2020 годах).

Иные формы медиаконтента (сайт, группа в социальной сети, видеоигра, флешмоб) остаются эпизодическими, о каком-то стабильном интересе участвующих можно будет говорить только при их неоднократном появлении в будущих Фестивалях.

За годы проведения Фестиваля партнёрами НЦПТИ, кроме Министерства образования и науки Российской Федерации, выступали Антитеррористический центр государств-участников Содружества Независимых Государств, ГБОУ ВО «МИРЭА – Российским технологический университет», Центр профилактики религиозного и этнического экстремизма в образовательных организациях Российской Федерации, а Федеральное агентство по делам молодежи (Росмолодежь) и Центр изучения региональных угроз (г. Ташкент, Республика Узбекистан).

В целом можно говорить о сложившейся целевой аудиторией, а также о состоятельности идеи дистанционного фестиваля, позволяющего при минимальных затратах создать и провести эффективное профилактическое мероприятие. Контент-анализ тематики и содержания полученных заявок представляется перспективной темой, нуждающейся в отдельном исследовании, поэтому производиться в рамках данной статьи не будет.

В 2020 году Фестиваль проходил с 30 апреля по 31 октября, заявки поступили из всех восьми федеральных округов и 29 субъектов Российской Федерации. К участию принимались работы, созданные с 1 января 2019 по 20



сентября 2020 года, на русском языке. Важным отличием от предыдущих лет являлось участие авторов из СНГ, что позволяет говорить о выходе Фестиваля на международный уровень.

Первое место по итогам голосования интернет-пользователей заняла тематическая группа «ВКонтакте» «Отвага и антитеррор» (А. И. Комиссарова). Проект является своеобразным ответвлением сайта «Отвага» (существует с 2002 года) – одного из старейших военно-патриотических проектов российского сегмента Интернета. По состоянию на начало 2021 года число подписчиков данной группы превысило 11 тысяч человек, при этом достигаются высокие показатели как публикационной, так и пользовательской активности.

Второе место принадлежит проекту творческого коллектива Института социологии и регионоведения Южного Федерального Университета «TikTok против экстремизма». В серии коротких роликов, выполненных в формате и стиле актуальной социальной сети, учащиеся с юмором представили актуальные идеи о недопустимости радикальных идей.

Третье место занял видеоролик «Старый друг» Д. С. Серикова. Короткий социальный ролик в нестандартной форме показывает взаимодействие двух старых друзей, один из которых увлекся радикальными идеями.

Отдельно можно выделить прошедшую вне конкурса игру FRIENDLY INTERNET, созданную студенткой АНОО ВО Воронежский институт высоких техноло-



гий Екатериной Миляковой. Игра представляет собой текстовый квест с различными вопросами по ежедневной безопасности в сети Интернет. Используя распространённый игровой формат Ren'Py и узнаваемую стилистику, автору удалось создать редкий сплав интерактивного теста с интерактивным художественным произведением. Подобное направление можно считать перспективным, поскольку позволяет геймифицировать вопро-

сы как цифровой гигиены, так и профилактики терроризма/экстремизма. Кроме того, с учётом популярности субкультуры аниме среди подростков и молодежи, представляется важной аккуратная работа в данном поле [4].

Все работы, поданные на конкурс в 2017–2020 годах и прошедшие в финальную его часть, были размещены на одностороннем сайте Фестиваля, в соответствующем году разделе [5].

Одной из причин, почему Фестиваль можно назвать примером удачной социальной акции, является разноплановость поданных работ. Для привлечения авторов используются варьирующиеся механизмы вовлечения в творческую деятельность, в зависимости от типа личности. Условно их можно разделить на методы подхода, стимулы вовлечения и вознаграждение.

К методам подхода относятся [6] творческая работа (реализовано творческой сущностью конкурса), работа малой группой (реализовано ориентацией на творческие коллективы) и задачи открытого типа. Последнее также лежит в основе Фестиваля – поставленная задача создания актуального позитивного контента предполагает множество направлений действия, без ограничения способов её достижения или форме/характеру.

К стимулам вовлечения [6], частично проистекающим как из стратегии, так и из методов подхода, относятся материальные (ожидаемые участниками призы, реклама, возможная награда от университета) и нематериальные (также ожидаемые сертификаты,

возможность получения практики и опыта по интересующим направлениям деятельности).

Как стратегия, так и стимулы вовлечения влияют на характер выбираемого организаторами вознаграждения. К нему относятся наличие (и выбор) призов/грамот/практики, предоставление площадки для рекламы творческих групп. Обеспечиваемое методологией саморазвитие является важным нематериальным вознаграждением.

Выбранная стратегия вовлечения тесно взаимосвязана с социальной стороной проекта. Для неё характерно объединение в себе воедино как методов подхода, так и стимулов вовлечения вместе с вознаграждениями.

С одной стороны, она диктует общественный, творческий формат работы участников Фестиваля. С другой – является своеобразным стимулом вовлечения. С третьей – обеспечивает чувство социальной значимости, являющееся ещё одним вознаграждением.

При безусловно важных общественной и социальной целях Фестиваля, не менее важна практическая сторона, более заметная для участников. Несмотря на свою нематериальность, она затрагивает всех его акторов.

Участники при создании конкурсных материалов нарабатывают определенный опыт в создании мультимедийного контента, что поможет им в дальнейшем саморазвитии. Кроме того, творческий процесс побуждает искать нестандартные подходы и взгляды на сущность и происхождение проблем терроризма

и экстремизма. Примером тому могут служить участники 2020 года. Серия роликов «TikTok против экстремизма» и игра Friendly Internet – это непривычные форматы социальной рекламы. Однако актуальность социальной сети и распространенность компьютерных игр вместе с субкультурой аниме делают их крайне востребованными в текущих реалиях.

С другой стороны, профилактические структуры получают обратную связь от собственно объекта профилактики, а также получают наглядный пример актуального антитеррористического и антиэкстремистского контента, созданного в тесном взаимодействии с целевой аудиторией. Подобный опыт может

помочь как в проведении аналогичных мероприятий и создании позитивного контента, так и в совершенствовании тактики построения профилактических мер.

Таким образом, Фестиваль социального контента «Я против терроризма и экстремизма» по ряду причин представляется удачным комплексным методом вовлечения молодежи в создание антитеррористического контента по следующим причинам:

– используемая организаторами стратегия вовлечения (сочетание нескольких методик и механизмов вовлечения), позволяет привлечь широкий пласт творческой молодежи, что ведёт к качественному развитию социального контента.



## Я ПРОТИВ ЭКСТРЕМИЗМА И ТЕРРОРИЗМА

*Логотип «Фестиваля социального медиаконтента»*

– методики и механизмы вовлечения обеспечивают возможность для поиска новых форматов социальной рекламы, что в перспективе благотворно повлияет на разнообразие представленных площадок.

– падающее соотношение поданных материалов к допущенным до финального голосования на фоне возрастания общего роста числа поданных заявок свидетельствует о общем качественном росте.

– международный масштаб мероприятия свидетельствует о качественном развитии, что представляется крайне важным в контексте современных интеграционных теорий [7].

#### Литература и ссылки

1. Беляева Т. Н., Борисов С. В. Противодействие экстремизму (терроризму): приоритетное направление правоохранительной деятельности в аспекте обеспечения национальной безопасности // Труды Академии управления МВД России. 2020. №4 (56). С. 105–116. URL: <https://cyberleninka.ru/article/n/protivodeystvie-ekstremizmu-terrorizmu-prioritetnoe-napravlenie-pravoohranitelnoy-deyatelnosti-v-aspekte-obespecheniya-natsionalnoy> (дата обращения: 20.02.2021).

2. Гаджигасанова Н. С. Особенности межэтнических представлений и социальных практик учащейся молодежи в контексте вузовского образования (на примере обучающихся ЯрГУ им. П. Г. Демидова) // Противодействие идеологии терроризма в

образовательной сфере и молодежной среде: сборник статей / составитель В. В. Каберник. Московский государственный институт международных отношений (университет) Министерства иностранных дел Российской Федерации. Москва: МГИМО–Университет, 2019. С. 59–72.

3. Профилактика терроризма и экстремизма в молодежной среде / под ред. А. П. Новикова. СПб.: ООО «Издательство «Русь», 2018. 96 с.

4. Страница в социальной сети «ВКонтакте» с публикацией игры FRIENDLY INTERNET. URL: [https://vk.com/wall-112267450\\_5354](https://vk.com/wall-112267450_5354).

5. Страница онлайн-фестиваля «Я против терроризма и экстремизма». URL: <https://videofest.npfti.ru/>.

6. Журавская Н. Т. Активизация самостоятельной работы студентов как фактор формирования их инновационного мышления // Вестник ТГПУ. 2010. №4. URL: <https://cyberleninka.ru/article/n/aktivizatsiya-samostoyatelnoy-raboty-studentov-kak-faktor-formirovaniya-ih-innovatsionnogo-myshleniya> (дата обращения: 26.02.2021).

7. Батоврина Е. В., Сорокина Т. А., Шестоперов А. М. Механизмы вовлечения молодежи в инновационную деятельность в Союзном государстве // Государственное управление. Электронный вестник. 2013. №40. URL: <https://cyberleninka.ru/article/n/mehanizmy-vovlecheniya-molodezhi-v-innovatsionnuyu-deyatelnost-v-soyuznom-gosudarstve> (дата обращения: 20.02.2021).

## Лидеры мнений как инструмент противодействия идеологиям терроризма и экстремизма

**Глянцев Никита Сергеевич** – студент Института социологии и регионоведения Южного федерального университета, г. Ростов-на-Дону

В настоящее время угроза терроризма в России не только не снижается, но и не сходит с повестки дня. При всех существующих мерах противодействия, а это, к примеру, предотвращение терактов, задержание вербовщиков и распространителей экстремистской литературы или борьба с террористической пропагандой в сети, внешние и внутренние факторы не снижают сво-

ей деструктивной активности, что можно подтвердить словами зампреда Совета Безопасности РФ Д.А. Медведева. В ходе состоявшегося 1 февраля 2021 года интервью российским СМИ Д.А. Медведев подчеркнул, что террористическая угроза продолжает существовать по всей России, а не только на Северном Кавказе. Также он отметил, что такая активность часто связана и с внутренними



импульсами, и с иностранным вмешательством.

Согласно сообщению МВД, число преступлений террористического характера в 2020 году выросло на 33,9 %, а экстремистской направленности – на 43,4 % по сравнению с 2019 годом [1]. Поэтому работа в направлении противодействия современным террористическим вызовам должна являться одной из главных как для сотрудников госбезопасности, так и для научного сообщества, которое, например, реализует свои возможности в разработке современных методов противодействия идеологии терроризма и экстремизма.

Важной частью современной экстремисткой и террористической угрозы стал переход в информационную (сетевую) среду воздействия, вербовки и пропаганды. И ключевым аспектом, тяжело поддающимся противодействию, выступает пропаганда. Аргументом данному утверждению служит тот факт, что сетевая пропаганда в настоящее время осуществляется по большей части в сети Интернет, где своевременная блокировка такого рода контента не всегда возможна. Выдающийся пример сказанного, на наш взгляд, это попытка блокирования мессенджера Telegram. Данным мессенджером, согласно сообщению ФСБ России, активно пользовались террористы для связи между собой и со своими зарубежными кураторами. Они пользовались мессенджером, потому что он обладает высоким уровнем шифрования передаваемой

информации [2]. Эта попытка в конечном счёте оказалась безуспешной.

С помощью интернета террористическим организациям теперь не только легче распространять свои идеологические материалы, но и проще заниматься поиском и вербовкой новых сторонников. Ярким примером жертвы сетевой пропаганды служит школьник из Твери, который в 2014 году планировал совершить теракт. Как он сам заявлял оперативному сотрудникам во время своего допроса, он слушал лекции известных террористов, участников террористической группировки «Имарат Кавказ» (запрещена на территории России). Их лекции были размещены в свободном доступе в Интернете. Кроме того, согласно журналистскому расследованию, которое провел корреспондент газеты «Комсомольская правда» в 2014 году, на внушаемость радикальных идей сильно повлияло психологическое состояние подростка. По словам опрошенных соседей, членов семьи, а также учителей мальчика, он практически ни с кем не общался, не ходил в школу и большую часть времени проводил в интернете, то есть находился в некой социальной изоляции [3]. В социальной психологии такое состояние называется «социальная депривация».

Проявления социальной депривации изучаются сейчас достаточно широко. Так, например, было проведено исследование (сканирование мозга) в Университетском колледже Лондона, которое показало, что имен-

но социальная изоляция ведет к радикализации. Используя нейровизуализацию, учёные смогли отобразить то, как мозг радикализованных людей реагирует на социальную маргинализацию. Всплески агрессии зафиксировали во время виртуальной игры Cyberball, когда коренные испанцы внезапно перестали бросать мусульманам мяч, исключив их из своего общества. Последствием этого стало изменение отношения к вопросам, которые раньше не трогали молодых мусульман. Так, обучение исламу в школах или неограниченное строительство мечетей стали гораздо более важными и похожими на «священное право», которое заслуживает борьбы. Полученные исследователями результаты подтверждают, что именно изоляция от общества приводит к превращению верующих мусульман в джихадистов [4].

В итоге социальная изоляция и психологически грамотно выстроенная радикальная пропаганда оказали комплексное воздействие на школьника и привели его к поддержке идеологии терроризма. Как мы видим из вышеприведенного примера, современная сетевая пропаганда является очень эффективной, но в то же время и трудно устранимой ввиду распространения в интернете. Она становится настолько эффективной, что выступает одним из важнейших инструментов продвижения радикальных идей. Именно поэтому сетевая пропаганда – важнейший инструмент современных экстремистских и террористических организаций.

Из всех существующих методов пропаганды следует выделить один. Это метод «лидеры мнений». Теоретические подходы к определению этого понятия очень разнообразны. Отечественные и зарубежные авторы по-разному интерпретируют его, кто-то определяет «лидеров мнений» как субъектов информационного воздействия, кто-то как инструмент или метод для продвижения необходимой информации. Если говорить о противодействии идеологиям терроризма и экстремизма, то этот метод может активно применяться как инструмент контрпропаганды. Тогда под контрпропагандой здесь будем понимать совокупность мер по противодействию распространению враждебных взглядов и убеждений.

Метод «лидеры мнений» будет особо эффективен для важной части современного информационного общества – молодёжи, потому что они больше всех увлечены Интернетом и сетевыми трендами. Согласно результатам опроса, проведенного экспертной группой Финансового университета при правительстве РФ в 2018 году, абсолютное большинство молодежи (78 %) проводит в сети более четырех часов ежедневно, из них более трети (38 %) – до восьми часов в сутки [5]. Поэтому через интернет идёт активное продвижение в сознание молодёжи разнообразных идей, в том числе и идеологий экстремизма и терроризма. На этот факт указывают многие современные российские исследователи. Например, В. В. Стрюковатый в своей работе под-

черкивает, что интернет играет важную роль в воздействии исламистских идей, в особенности, на молодежь [6].

Итак, вернёмся к методу, представляющему собой значимую часть в теории пропаганды, – так называемому методу лидеры мнения. Сначала необходимо рассмотреть теоретические подходы к сущности и определениям понятия «лидер мнений». Например, В. Г. Крысько в своем фундаментальном труде «Секреты психологической войны (цели, задачи, методы, формы, опыт)» [7] выделяет авторитетность субъекта информационного воздействия как важный фактор успешности психологического воздействия на объект пропаганды. То есть, чем известнее и авторитетнее субъект (в данной работе это лидер мнений), тем проще через него транслировать нужную информацию. Кроме того, в своем сборнике материалов под названием «Информационно-психологическая война» А. Е. Тарас, ссылаясь на зарубежных авторов, указывает, что для пропаганды каких-то идей в обществе, для изменения общественных норм какой-либо группы используется метод «лидеры мнений».

Использование лидеров мнений для пропаганды, а в нашем случае для контрпропаганды, обусловлено следующими их характеристиками, выделяемыми западными исследователями: 1) лидеры мнений расположены по всей социальной структуре, а не только на вершине её иерархии; 2) лидеры мнений занимают активную политическую пози-

цию; 3) лидеры мнений сильнее подвержены информационному воздействию, чем те, кто ими не является; 4) лидеры мнений используют полученную информацию для дальнейшей передачи её в виде советов или информации [8]. А. В. Сороченков в своей работе «Энциклопедия методов пропаганды» [9] указывает, что лидеры мнений есть по всей социальной структуре общества, он называет их «лидеры микросоциальных групп». Исследователь ссылается на мнение американских специалистов, которые считают, что, для того, чтобы успешно заложить идеи, нормы или ценности в широких слоях населения, необязательно воздействовать на все слои населения, а эффективнее будет обработать только лидеров микросоциальных групп, или, как они их определяют, «медиаторов». Они-то и передадут нужную информацию подконтрольной группе людей в виде советов, рекомендаций и т. п.

А. В. Сороченков в качестве медиаторов выделяет следующие виды:

- 1) неформальные лидеры;
- 2) политические деятели;
- 3) религиозные представители;
- 4) деятели культуры, науки либо искусства;
- 5) спортсмены;
- 6) военные и т. д.

Автор подчеркивает, что в психологии влияния данный метод называется «фиксацией на авторитетах». М. В. Киселёв в работе «Психологические аспекты пропаганды» тоже поддерживает вышеуказанные тезисы. Он утверждает, что специалисты

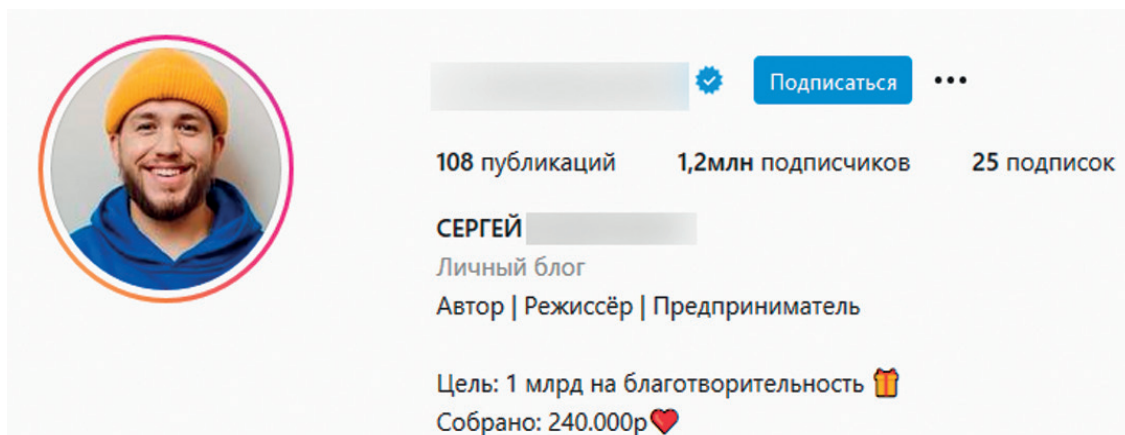


воздействуют на дополнительную ступень – лидеров мнений. С ними массовые потребители обсуждают информацию, которая затем остается в их сознании и подсознании. М. В. Киселёв определяет лидеров мнений как политически активных граждан, использующих полученные данные для информирования и совета другим [10]. По подсчетам исследователя, лидеров мнений в обществе около 10–20 %. Таким образом, подведем промежуточный итог, который заключается в следующем: метод «лидеров мнений» хорошо разработан в теоретическом и практическом аспектах как метод пропаганды.

Рассмотрим примеры использования данного метода абсолютно в других сферах. Например, Е. М. Ильиных в своей статье «Лидеры мнений как инструмент формирования общественного мнения в период избирательных кампаний» [11] называет метод «лидеров мнений» одним из эффективных инструментов формирования общественного мнения в рамках избирательных кампаний. Если говорить про избирательный контекст, то здесь автор утверждает, что лидер мнений формирует общественное мнение в отношении агитации или политической программы. А, например, Е.В. Слепцова и Р.Н. Сандул в своей работе «Лидеры мнений как маркетинговый метод продвижения услуг» предлагают использовать лидера мнения в качестве маркетингового инструмента. Они предлагают ещё понятие «инфлюенсеры». Исследователи относят к ним известных и популярных пользо-

вателей социальных сетей, медиапространства, способных своими рекомендациями влиять на широкую аудиторию людей, благодаря своей личной странице или блогу [12]. Итак, метод «лидеры мнений» является широко используемым в рамках продвижения каких-то идей, ценностей или мнений. В связи с этим, на наш взгляд, данный метод будет обладать большой эффективностью и в контрпропаганде или в информационном противодействии идеологиям экстремизма и терроризма, потому что каждый лидер социальной группы сможет внушить своей аудитории необходимую контрэкстремистскую или профилактическую информацию.

Попытаемся подтвердить выдвинутую гипотезу конкретным примером. Если говорить о российских или русскоговорящих мусульманах, то наиболее известным лидером мнений сейчас является и может стать Сергей Романович – бывший достаточно популярный актер российского кино и сериалов, который принял ислам. Сергей имеет огромную аудиторию, большая часть которой – русскоговорящие мусульмане. В социальной сети Instagram у Сергея 1,2 миллиона подписчиков, на канале видеохостинга YouTube 593 тысячи подписчиков. В своих социальных сетях Сергей активно показывает жизнь мусульманина. Ещё одним примером является страница под названием «Блог русского мусульманина», где Кирилл Джабраил представляет короткие видеофрагменты, в которых рассказывает о различных



*Профиль Сергея Романовича в социальной сети Instagram*

аспектах ислама. На его блог подписано 78 тысяч человек. Если приводить примеры мусульман из других сфер деятельности, то это, бесспорно, российский боец смешанных единоборств Хабиб Нурмагомедов. За его страницей в Instagram следят 27,2 миллиона человек. Или, например, девушка из сферы модной индустрии Сауфия Гудсон, ведущая одну из самых популярных страниц в Instagram о мусульманской моде. На эту страницу подписано около 3 миллионов человек. Итак, все выше названные люди относятся к лидерам своих социальных групп, в особенности они являются образцом для мусульманской части своей молодежной аудитории. Если бы эти люди могли продвигать идеи традиционного ислама, распространять позитивный контент, то они бы стали эффективным средством разрушения террористической пропаганды в интернете.

Кстати, примеры деятельности, продвигающей позитивный контент, уже существуют в Сети. Это «БЛОГ МУСУЛЬМАНИНА И МУСУЛЬМАНКИ», существ-

вующий на нескольких информационных площадках – YouTube, Instagram, «ВКонтакте», а также блог в Яндекс Дзен. На YouTube канале распространяется информация об исламе, полезные анимационные видео для мусульман. Количество подписчиков на канале около 300 тысяч человек.

Итак, используя лидеров социальных групп, можно распространять позитивный контент, формировать умеренную религиозную микрофлору среди молодежи, предотвращать экстремистскую пропаганду. В зависимости от того, какой контент производит лидер, через него можно распространять профилактические материалы, которые будут вписываться в тематику, привычную для его аудитории. Например, короткие ролики на социальные темы (вайны) либо видео-/аудиоматериалы. Такой позитивный контент не только отвлекает от негативных экстремистских материалов, но и оказывает профилактическое действие на подсознание аудитории, ведь, как упоминалось рань-

ше, через лидера мнений любая информация усваивается человеком лучше, потому что он ему доверяет. Сейчас важно использовать все доступные инструменты для противодействия пропаганде религиозного терроризма и любых других проявлений экстремизма. Необходимо усиливать воздействие именно через интернет, потому что большая часть молодёжи много времени проводит в сети.

#### Литература и ссылки:

1. В МВД рассказали о росте числа террористических преступлений в России / РИА Москва. 24.11.2020. [Электронный ресурс]. URL: <https://ria.ru/20201124/prestupleniya-1586012073.html> (дата обращения: 12.02.2021).
2. В России террористы активно используют Telegram для связи, заявили в ФСБ / РИА Москва. 26.06.2017. [Электронный ресурс]. URL: <https://ria.ru/20170626/1497271423.html> (дата обращения: 27.02.2021).
3. Террор не по-детски: мечтающая стать шахидом, тверской школьник принял ислам и собрал бомбу для взрыва отдела полиции / Комсомольская правда. 10.01.2014. [Электронный ресурс]. URL: <https://www.tver.kp.ru/daily/26179/3068966/> (дата обращения: 01.03.2021).
4. Townsend M. Brain scans show social exclusion creates jihadists, say researchers // The Guardian. 2019. Т. 6.
5. Эксперты: почти 80 % молодежи в РФ проводит в интернете более четырех часов в день / ТАСС Москва. 15.11.2018. [Электронный ресурс]. URL: <https://tass.ru/obschestvo/5797509> (дата обращения: 13.02.2021).
6. Стрюковатый В. В. Особенности и причины возникновения и распространения идей радикального ислама в молодежной среде (по материалам уголовных дел, возбужденных в отношении лиц, совершивших преступления террористической и экстремистской направленности на территории республики Кабардино-Балкария) // Отечественная юриспруденция. 2016. №4 (6). С. 3–4.
7. Крысько В. Г. Секреты психологической войны (цели, задачи, методы, формы, опыт) // Минск: Харвест, 1999. С. 133.
8. Информационно-психологическая война / Сост.-ред. А. Е. Тарас – Минск: Харвест, 2016. С. 19–20.
9. Сороченко В. Энциклопедия методов пропаганды // М.: Дрофа. 2002.
10. Киселёв М. В. Психологические аспекты пропаганды [Электронный ресурс] URL: <https://psyfactor.org/propaganda7.htm#41> (дата обращения 03.02.2021).
11. Ильиных Е. М. Лидеры мнений как инструмент формирования общественного мнения в период избирательных кампаний // Скиф. 2019. №9 (37). С. 115.
12. Слепцова Е. В., Сандул Р. Н. Лидеры мнений, как маркетинговый метод продвижения услуг // Международный журнал гуманитарных и естественных наук. 2019. №11-1. С. 1.

## ВСПОМНИМ



В тринадцатый день марта пришло скорбное известие о том, что перестало биться сердце Сергея Алексеевича Воронцова.

Оно вмещало в себя горячность и честность чекиста, талант и профессионализм ученого и педагога, бескомпромиссность и отвагу борца с коррупцией и криминалом, неутомимую страстность пропагандиста, яркость харизматичного оратора, убежденность блестящего полемиста.

На его лекции всегда стремилось попасть большее количество слушателей, нежели позволяла вместимость аудитории, а его выступления буквально взрывали зал, держали публику артистичной манерой изложения и глубоким знанием предмета.

Нам посчастливилось сотрудничать с Сергеем Алексеевичем в пору создания нашего Национального центра информационного противодействия терроризму и экстремизму в образовательной среде и сети Интернет. Его опыт и знания в вопросах противодействия идеологии терроризма и экстремизма оказали незаменимую помощь и поддержку, а открытость и демократичность позволяли общаться на равных с гуру правоохранительной и оперативно-розыскной деятельности.

Уход С. А. Воронцова из числа тех, что позволяют опровергнуть сентенцию об отсутствии незаменимых людей. Они есть. Наш коллега и старший товарищ был из этой категории. Вечная ему память.





PROEKT-PARALLELI.RU  
PROEKT-PARALLELI.RU  
PROEKT-PARALLELI.RU  
PROEKT-PARALLELI.RU  
PROEKT-PARALLELI.RU  
PROEKT-PARALLELI.RU  
PROEKT-PARALLELI.RU  
PROEKT-PARALLELI.RU  
PROEKT-PARALLELI.RU  
PROEKT-PARALLELI.RU



**КОНТЕНТ ШАБРИКА**  
**ПАРАЛЛЕЛИ**



ПРИ ПОДДЕРЖКЕ  
ФОНДА  
ПРЕЗИДЕНТСКИХ  
ГРАНТОВ

МИНОБРНАУКИ РОССИИ

**ЮРАЦ**


ЮЖНЫЙ РЕГИОНАЛЬНЫЙ  
АТТЕСТАЦИОННЫЙ ЦЕНТР

**ЗАЩИТА**

**ИНФОРМАЦИИ**

## ОСНОВНЫЕ НАПРАВЛЕНИЯ ДЕЯТЕЛЬНОСТИ:

- ▶ Подготовка к лицензированию на осуществление работ, связанных с использованием сведений, составляющих государственную тайну.
- ▶ Проектирование и внедрение систем защиты информации, доступ к которой ограничен федеральными законами.
- ▶ 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.
- ▶ Аттестация объектов информатизации, предназначенных для обработки информации, содержащей сведения, составляющие государственную тайну (ВП, ОВТ, СИРД), на соответствие требованиям безопасности информации.
- ▶ Реализация программ дополнительного профессионального образования в области информационной безопасности («Защита государственной тайны», «Обеспечение безопасности персональных данных при их обработке в информационных системах персональных данных»).
- ▶ Обеспечение безопасности объектов КИИ и АСУ ТП.

 +7 (863) 201-28-15

 oaoi@niisva.org

 344010, г. Ростов-на-Дону, ул. Города Волос, д. 6



юрац.рф



**НЦПТИ**

**ОБЗОР.НЦПТИ**  
СБОРНИК ИНФОРМАЦИОННЫХ  
МАТЕРИАЛОВ

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

---