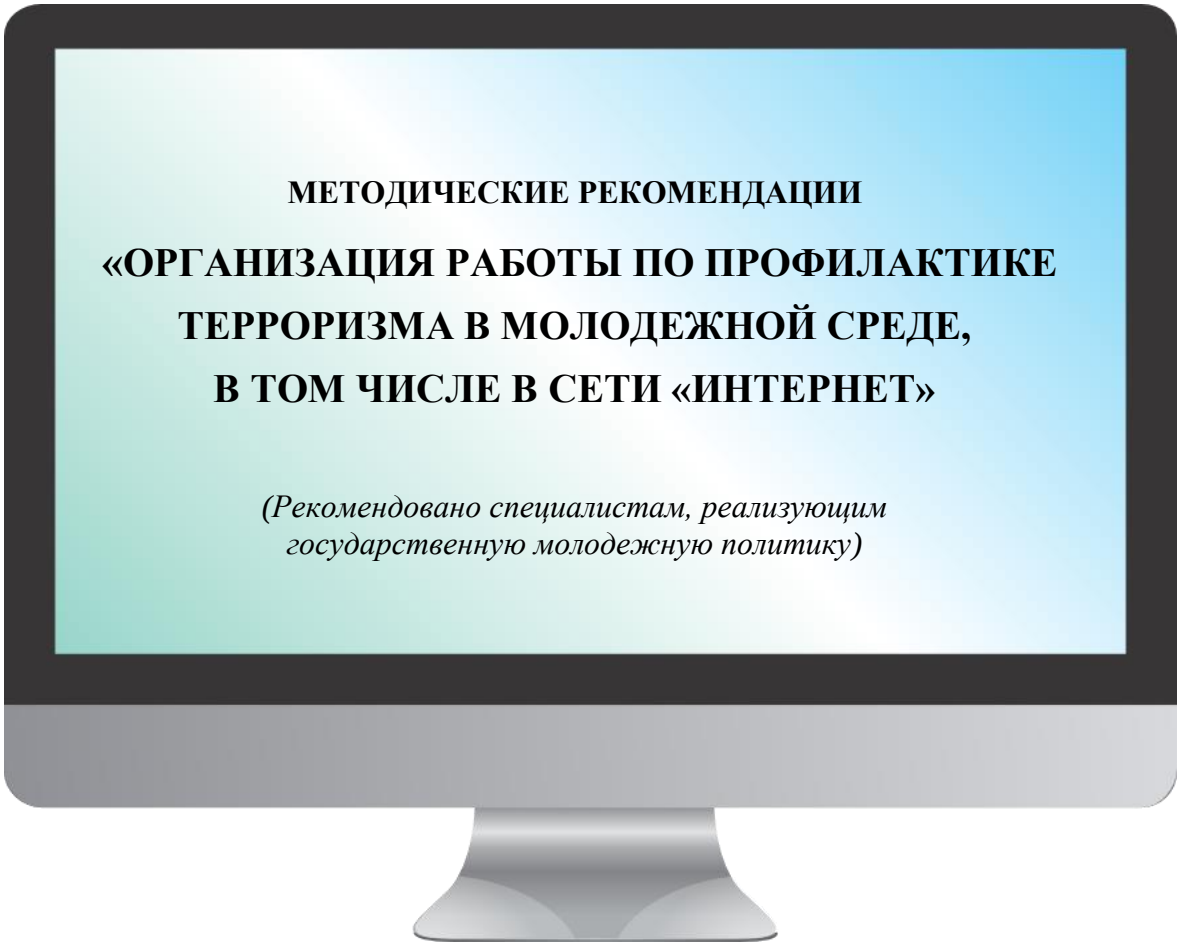
МИНИСТЕРСТВО ПО ДЕЛАМ МОЛОДЕЖИ РЕСПУБЛИКИ ДАГЕСТАН

АНО «ЦИФРОВЫЕ ВОЛОНТЕРЫ»



МЕТОДИЧЕСКИЕ РЕКОМЕНДАЦИИ

«ОРГАНИЗАЦИЯ РАБОТЫ ПО ПРОФИЛАКТИКЕ ТЕРРОРИЗМА В МОЛОДЕЖНОЙ СРЕДЕ, В ТОМ ЧИСЛЕ В СЕТИ «ИНТЕРНЕТ»

(Рекомендовано специалистам, реализующим государственную молодежную политику)

г. Махачкала

СОДЕРЖАНИЕ

1. ВВЕДЕНИЕ…….. 2
2. FAKE NEWS: ЧТО ЭТО?..... 5
3. РЕКОМЕНДАЦИИ ПО ОРГАНИЗАЦИИ РАБОТЫ В СФЕРЕ ПРОФИЛАКТИКИ ИДЕОЛОГИИ ТЕРРОРИЗМА В СТУДЕНЧЕСКОЙ И МОЛОДЕЖНОЙ СРЕДЕ..... 8
4. ТЕХНОЛОГИИ И ПРИОРИТЕТНЫЕ НАПРАВЛЕНИЯ ПРОФИЛАКТИЧЕСКОЙ РАБОТЫ В СФЕРЕ ТЕРРОРИЗМА, В ТОМ ЧИСЛЕ, В СЕТИ ИНТЕРНЕТ……... 12
5. ВНИМАНИЕ! САЙТ С ЭКСТРЕМИСТСКИМ КОНТЕНТОМ. ЧТО ДЕЛАТЬ?..... 14
6. ГРАНИЦЫ КОМПЕТЕНЦИЙ СПЕЦИАЛИСТОВ УЧРЕЖДЕНИЙ ОРГАНОВ ПО ДЕЛАМ МОЛОДЕЖИ В ОБЛАСТИ ПРОФИЛАКТИКИ ТЕРРОРИЗМА…… 15
7. ОТВЕТСТВЕННОСТЬ В СЕТИ ИНТЕРНЕТ……...…… 16
8. СРЕДСТВА РЕАЛИЗАЦИИ КОМПЛЕКСНОЙ ЗАЩИТЫ ИНФОРМАЦИИ…… 19
9. ПРОСТЫЕ ПРИМЕРЫ ДЛЯ РЕШЕНИЯ СЛОЖНЫХ ПРОБЛЕМ…….. 20
10. ИНФОРМАЦИОННОЕ ВОЛОНТЕРСТВО КАК РЕСУРС…… 27
11. РАБОТА СО СРЕДСТВАМИ МАССОВОЙ ИНФОРМАЦИИ…….. 28
12. ГЛОСАРИЙ……..... 32

1. ВВЕДЕНИЕ

«Кто владеет информацией — тот владеет миром»
Уинстон Черчилль

Потребность в информации — одна из базовых потребностей человека. В самых простых формах она начинает проявляться с рождения. Психологи считают, что высшие познавательные потребности человека развиваются на основе потребности в новых впечатлениях, возникающей у младенцев.

С возрастом потребность в информации претерпевает ряд существенных изменений. В школьном возрасте в процессе обучения у ребенка начинают складываться новые формы познавательной активности и мотивации, приобретающие осознанный и произвольный характер.

Это интересно! *Объем информации, которую обычный человек в XVIII веке воспринимал за целую жизнь, сегодня соответствует информации в ленте крупного новостного портала всего за 2–3 дня. Для записи информации, которая появляется в Сети каждый час, потребуется около 7 млн. DVD-дисков. На популярном видеохостинге YouTube ежеминутно появляется более 100 часов видео — это как если бы Голливуд выпускал около 260 000 новых полнометражных фильмов каждую неделю.*

С развитием постиндустриального общества потребность в информации становится все более актуальной и значимой для современного человека. Во второй половине XX века Абрахам Маслоу предложил классификацию потребностей, для отображения которых используют метафору пирамиды. Основание её составляют физиологические потребности: в еде, питье, жилье — потребности, связанные с поддержанием жизни, а вершину образуют высшие социальные потребности - в любви, признании, познании и самоактуализации, то есть потребности, связанные с развитием личности.

По данным онлайн-опросов, проведенных Фондом Развития Интернет, у российских подростков потребность в доступе к Интернету занимает второе место по значимости, превысив по степени важности потребность в материальном благополучии, но уступив потребности в еде. В исследовании Фонда подросткам предлагалось представить, что после кораблекрушения они оказались на необитаемом острове, на котором нужно будет прожить несколько лет. Им задавался вопрос: что бы они взяли с собой на остров в первую, вторую и третью очередь? В своем первом желании большинство опрошенных поставили Интернет на второе место после друзей и родственников. Во втором и третьем желании Интернет опередил родных и близких, оказавшись на первом месте. Суммарно по всем трем желаниям потребность в Интернете и потребность в близких людях оказались равны. Современные школьники, у которых удовлетворены базовые потребности в еде, тепле, комфорте и безопасности, стремятся к удовлетворению более высоких потребностей — в любви и внимании, в признании, в самореализации и личностном росте. Дети и подростки пытаются реализовать вышеперечисленные потребности и в Интернете. Если общение в Интернете нередко создает лишь иллюзию удовлетворения потребности в любви и принятии, то в реализации познавательной потребности — жажды знаний и желания воспринимать как можно больше информации — Интернет играет сегодня ключевую роль.

Современные российские школьники существенно отличаются от детей и подростков, ходивших в школу 10–15 лет назад. Сегодня они в дополнение к домашнему

компьютеру пользуются гаджетами разного калибра — мобильниками, смартфонами, айпадами; легко совмещают реальность и виртуальность. Интернет становится важным инструментом социализации подрастающих поколений. Жить в цифровой среде — это «круто», поэтому дети и подростки усердно постигают азы компьютерной грамотности, а некоторые из ребят в техническом смысле становятся искушенными пользователями. Они беззаботно чувствуют себя в киберпространстве, узнают о новых технологиях и возможностях практически одновременно с их появлением. Вырастает новое цифровое поколение, вооруженное разнообразными гаджетами и чувствующее себя естественно и непринужденно не только в Рунете, но и в глобальной Сети в целом.

Число пользователей Интернета неуклонно растет с каждым днем, а самыми активными среди них являются молодые люди, подростки и дети. Аудитория Рунета на март 2016 года составила 80,5 млн. взрослых пользователей, детская аудитория (в возрасте до 14 лет) насчитывает 8-10 млн. пользователей. По разным исследованиям, дети начинают пользоваться Интернетом в возрасте 6-8 лет.

Дополнительными факторами вовлечения детей в Интернет стали снижение цены на электронные устройства и тарифы доступа в Интернет, а также развитие мобильного Интернета. Тенденции к развитию общения в социальных сетях, облачных технологий стирают границу между локальным и сетевым использованием вычислительной техники. Многие даже не задумываются о том, что используют Интернет - настолько этот технологический феномен стал частью повседневной жизни.

Интернет для детей, рано и интенсивно начинающих им пользоваться, выступает новым инструментом, опосредующим формирование у них высших психических процессов. Эти процессы, в соответствии с культурно-исторической теорией Льва Выготского, являются социальными по происхождению. Они не заданы природой, а формируются обществом и его культурой. Их адекватное развитие является основой успешного обучения. Если до эпохи новых инфокоммуникационных технологий высшие психические процессы развивались в непосредственном социальном взаимодействии взрослого и ребенка и детей между собой, то сегодня Интернет в значительной степени опосредует такое взаимодействие.

Рассмотрим некоторые изменения, связанные с высшими психическими функциями.

Память. У детей, активно пользующихся поисковыми системами Интернета, по-другому начинает функционировать память: в первую очередь запоминается не содержание какого-либо источника информации в Сети, а место, где эта информация находится, а еще точнее «путь», способ, как до нее добираться. Взрослые сами понемногу перестают запоминать телефоны, адреса и другую ежедневно необходимую информацию, которая раньше естественно удерживалась в нашей памяти. Дети же с рождения живут в цифровом мире. Доступность практически любой информации в любое время с раннего возраста меняет структуру мнемонических процессов. Память становится не только «неглубокой», но и «короткой» («клиповое мышление»). У детей и подростков формируются другое запоминание, другая память, другие механизмы удержания информации.

Внимание. Средняя продолжительность концентрации внимания по сравнению с той, что была 10–15 лет назад, уменьшилась в десятки раз. Если прежде ребенок на уроке

мог удерживать внимание в течение 40 минут, и это считалось нормой, то сейчас в классе на такую сосредоточенность способны буквально единицы.

Мышление. Особенности внимания, а также процессов восприятия тесно связаны с широко обсуждаемым феноменом «клипового мышления». Оно построено скорее на визуальных образах, чем на логике и текстовых ассоциациях, и предполагает переработку информации короткими порциями. О существовании и особенностях «клипового мышления» спорят с 1990-х годов, и некоторыми исследователями оно рассматривается как защитная реакция на информационную перегрузку.

В то же время в жизни цифрового поколения есть немало преимуществ, обретенных благодаря эпохе Интернета. Возьмем, например, загадочный и ошеломляющий феномен детской многозадачности, который также связан с мышлением. Мы, взрослые, нередко наблюдаем картину, когда ребенок, сидя за компьютером, одновременно общается в чате, занимается поиском в Сети, скачивает музыку, отслеживает обновления френдленты, периодически разговаривает по скайпу, слушает музыку из плейера, пытается делать домашнее задание и при этом пьет сок и жует бутерброд. Такой режим деятельности характерен не только для работы за домашним компьютером — это происходит и на уроках в школе. Если учитель будет понимать суть происходящего, его не будут раздражать дети, которые на первый взгляд невнимательны и стремятся заняться посторонними делами. Другой образ жизни предполагает другой темп, надо успеть многое увидеть, сделать, на многое отреагировать. Феномен многозадачности характерен для представителей цифрового поколения и не свойственен взрослым людям, которые в нормальном состоянии, как правило, могут эффективно заниматься лишь чем-то одним. После 50 лет многозадачность вообще затруднена. Основное препятствие для эффективности многозадачности — скорость, с которой определенный участок префронтальной коры головного мозга обрабатывает информацию: позволяет планировать долговременные цели, запоминать незаконченные задачи, отвечать за разделение больших заданий на мелкие части и доводить их до завершения. Информацию, связанную с одним делом, кора успевает обработать, с двумя — уже сложнее, т.к. скорость обработки значительно уменьшается. В то же время эта скорость может существенно возрастать благодаря практике и тренировкам, что и происходит с нашими детьми в перенасыщенном инфокоммуникационном потоке. Навигация в Сети предполагает многозадачность. Дети, включенные в этот процесс, с ранних лет вырастают нацеленными на одновременное решение различных задач. Соответственно, и их мозг начинает работать в другом режиме.

Однако предоставляя множество новых возможностей, глобальная сеть несет и новые риски. Исследователи выделяют 4 вида рисков:

Контентные риски возникают в процессе использования находящихся в Сети материалов (текстов, картинок, аудио- и видеофайлов, ссылок на различные ресурсы), содержащих противозаконную, неэтичную и вредоносную информацию.

Коммуникационные риски возникают в процессе общения и межличностного взаимодействия пользователей в Сети. Примерами таких рисков могут быть кибербуллинг, незаконные контакты (например, груминг, сексуальные домогательства), знакомства в Сети и последующие встречи с интернет-знакомыми в реальной жизни. С коммуникационными рисками можно столкнуться при общении в чатах, онлайн-мессенджерах, социальных сетях, сайтах знакомств, форумах, блогах.

Потребительские риски возникают в процессе приобретения товаров и услуг через Интернет. Они включают риск приобретения товара низкого качества, контрафактной и фальсифицированной продукции, риск потери денежных средств без приобретения товара или услуги, хищения финансовой информации с целью мошенничества.

Технические риски определяются возможностями повреждения программного обеспечения компьютера, хранящейся на нем информации, нарушения ее конфиденциальности или взлома аккаунтов, хищения паролей и персональной информации посредством вредоносных программ (вирусов, червей, троянских коней, шпионских программ, ботов и др.).

Ребенок, захваченный безграничными возможностями современных технологий, зачастую не может разглядеть этих угроз Сети и в результате оказывается среди наиболее уязвимых ее пользователей. Сталкиваясь с опасностью при использовании Интернета или мобильной связи, дети часто не знают, как поступить и к кому обратиться в такой ситуации, а потому вынуждены действовать методом проб и ошибок. Такая ситуация сформировала понятие об интернет-угрозах, необходимость их распознавать и им противостоять.

Использованная литература:

Солдатова Г., Зотова Е., Лебешева М., Шляпников В. Интернет: возможности, компетенции, безопасность. Методическое пособие для работников системы общего образования. Часть 1. Лекции — М.: Google, 2013. — С. 6, 11, 71, 79.

2. FAKE NEWS: ЧТО ЭТО?

Фальши́вые (подде́льные, «фе́йковые», ло́жные) но́вости — это информационная мистификация или намеренное распространение дезинформации в социальных медиа и традиционных СМИ с целью введения в заблуждение, для того чтобы получить финансовую или политическую выгоду.

Главный принцип генерирования фальшивых новостей — максимально негативная или абсурдная информация, которая регулярно тиражируется в онлайн-пространстве.

И если одни фейки условно безвредны, то большая их часть представляет угрозу здоровью людей или является инструментом для манипулирования сознанием.

Фейк вызывает максимально сильные, негативные эмоции — гнев, беспокойство, страх, тревогу, ненависть, которые возникают у человека из-за попадания в его точку боли. Например, проблемы в бизнесе, низкие зарплаты, отсутствие социальных гарантий, рост цен на продукты.

Например, весной 2020 года в Британии пытались поджечь 20 сотовых вышек из-за появления слуха о том, что 5G распространяет коронавирус. А ещё раньше поджог, который совершили поверившие в этот фейк, уничтожил оборудование для передачи связи, которой пользовались аварийно-спасательные службы и несколько мобильных операторов, лишив кого-то тем самым, возможно, надежды на спасение.

Также в СМИ активно гулял фейк на тему того, что домашние животные могут заразиться COVID-19, вакцинация населения опасна, а защититься от заразы можно с помощью обильного горячего питья, пребывания на солнце и даже водки.

Но дело тут не только в коронавирусе, главная цель - это введение в заблуждение, для того чтобы получить финансовую или политическую выгоду.

Есть три составляющих фейковых новостей: *соцсети, телекоммуникационные технологии и специфическая мотивация.*

Фейковые новости практически всегда либо про политику, либо про деньги. Политических манипуляторов привлекает в соцсетях их «народный» характер, а коммерческих злоумышленников — ещё и монетизация.

Политика. Чаще всего fake news генерируются для влияния на выборы или какую-либо политическую фигуру. Традиционные источники информации для этого не совсем подходят, ведь обычный человек всё более склонен верить «таким же простым людям, как и он» в соцсетях, а не «аффилированным с государством или корпорациями» СМИ. Именно поэтому фейковые новости создаются с прицелом на соцсети — здесь у каждого участника есть определённый «соседский» круг доверия.

Деньги. Создавая фейковые новости, можно усиливать активность определённых групп потенциальных клиентов. «Только три знака зодиака переживут 2020 год…» — кликбейт-заголовок, который в итоге может привести на посадочную страницу сервиса платной рассылки гороскопов. Соцсеть в этом случае играет роль хирургически точного инструмента вовлечения нужных групп потенциальных клиентов в орбиту влияния бренда. А пережив 2020 год, представители «неудачливых» знаков уже и не вспомнят о короткой новости, репост которой они увидели в тематической группе.

В будущем появится ещё и третий мотив — конкуренция, то есть фейковые новости всё чаще будут создавать для подрыва репутации бизнеса.

Далее разберём, как, собственно, работает механизм создания и распространения фейковых новостей.

Фейковые новостные кампании обычно проходят в несколько этапов, хотя это процесс творческий, и в зависимости от целей или особенностей аудитории некоторые стадии могут быть опущены.

1. **Разведка**

   На первом этапе организатор кампании изучает целевую аудиторию. Он отвечает на три основных вопроса: «Кому врать?», «О чём врать?» и «Зачем врать?». Анализ проводится самый широкий — от образовательного уровня и информационной грамотности будущих читателей до их взглядов на жизнь. Собственно, на этом этапе и были пойманы специалисты Cambridge Analytica, которые собирали персональные данные пользователей Facebook для политических целей.

Примечание: *21 марта Тверской районный суд Москвы вынес решение о том, что компания Meta Platforms, которой принадлежат «Инстаграм», «Фейсбук» и «Вотсап», считается экстремистской организацией, а ее деятельность запрещена в России.*

2. **Вооружение**

На втором этапе создаётся, собственно, фейковая новость. Её главная особенность в том, что почти всегда «декорации» фальсифицированной истории, то есть участники события, место и время действий, — реальные, а фейком является, собственно, само событие. В зависимости от масштабов компании, фейковых новостей может быть несколько. К примеру, первая история сообщает о событии, а последующие — развивают тему. Иногда к ним примешиваются даже настоящие новости, которые дополняют картину выдуманной истории. Они направлены на скептическую часть потенциальной аудитории.

Помимо новостей, на втором этапе создаются агенты распространения: фейковые пользователи соцсетей, фейковые новостные сайты, фейковые группы и сообщества. Для этого в ход идут чёрные и белые технологии SMM, позволяющие за деньги плодить и продвигать поддельных пользователей соцсетей. К примеру, в соцсети Weibo (китайский аналог Twitter) селебрити с 300 тыс. подписчиков можно создать примерно за 2,5 тыс. долларов всего за месяц.

3. Распространение

Обычно фейковая новость сперва появляется на таком же фейковом сайте новостей или на любой другой площадке, где публикации никак не контролируются. Далее в дело вступает «гуру» — прокачанный и авторитетный у целевой аудитории блогер, который публикует новость у себя. Сообщение подхватывают боты — реальные пользователи соцсетей или роботы, созданные/привлечённые специально для фейковой новостной кампании. Помимо распространения, они выполняют очень важную функцию — изолируют скептиков, которые остаются в меньшинстве и предпочитают сохранять молчание вместо противостояния фейкам.

4. Эксплуатация

На следующем этапе новость доходит до целевой аудитории и начинает жить своей жизнью. Наиболее вдохновлённые читатели лайкают и репостят фейковое сообщение, делятся им в мессенджерах. Возникает вирусный эффект, который привлекает внимание ещё более широкой аудитории — журналистов и других профессиональных участников медиаполя. Фейковая новость попадает в мейнстрим-медиа.

5. Промывка

Этот этап используется в долгосрочных кампаниях, призванных коренным образом изменить отношение целевой аудитории к каким-либо явлениям, причём иногда диаметрально противоположным образом. Для этого запускается не одна, а несколько последовательных фейковых новостных кампаний. Одна и та же история раскрывается через различные аспекты, появляются все новые герои событий, а вирусный эффект генерируется многократными волнами.

6. «Домашняя работа»

После достижении заданной цели могут потребоваться дополнительные, закрепляющие действия. К примеру, если речь идёт о кампании, подрывающей репутацию какого-либо политика, в информационное поле могут быть запущены позитивные новости о нём, которые не имеют прямого отношения к фейковой истории, но несколько корректируют образ жертвы в глазах общественности. Такие действия призваны устранить у общественности ощущение травли или спланированной акции в отношении политика.

7. Заметание следов

Последний этап — сокрытие следов активности. Наиболее распространённая технология, позволяющая это сделать, — отвлекающая новость. Используя уже созданную инфраструктуру из ботов можно вбросить новое «информационное» сообщение. По своей тематике оно должно совершенно отличаться от прежней фейковой истории, быть ещё более громким и резонансным. Такая фейковая новость переключает внимание общественности на новую проблему и «глушит» голоса тех, кто, возможно, к этому моменту сумел идентифицировать прежний фейк.

Теперь, разобравшись в алгоритмах, давайте посмотрим на фейковую новость не глазами создателей, а со стороны аудитории. И выясним параллельно, как противостоять fake news?

Вырабатываем «иммунитет» к фейкам.

Поскольку fake news бьют прямой наводкой по пользователям, первый рубеж обороны могут составить только сами читатели. Прежде всего, они должны определять фейковые новости по следующим признакам:

1. **Гиперболизированные и кликбейтные заголовки.** Заголовки новостей коротко описывают суть произошедшего. В противном случае лучше новость проигнорировать.
2. **Подозрительные домены или искажённые названия сайтов популярных медиа, похожие на настоящие**. Забейте в поисковик название интересующего вас СМИ — на первых позициях в выдаче будут оригиналы. Сравните их интернет-адресом подозрительного источника.
3. **Большое количество ошибок или опечаток в тексте новости**. Попробуйте найти на сайтах известных вам СМИ эту же историю, но в более развёрнутом виде. Если поиски не увенчаются успехом, то, скорее всего, перед вами автоматически сгенерированный контент.
4. **Поддельные фото или коллажи.** Попробуйте сохранить подозрительное фото и поискать его копии через фотопоисковики (Google, TinEyE и т.п.). Если копий нет в авторитетных источниках, то скорее всего перед вами фотошоп.
5. **Отсутствие отметок о времени публикации новости**. Даты публикации скрывается для того, чтобы максимально продлить «жизнь» фейковой новости. Такое сообщение будет казаться актуальным сколь угодно долго, пока не будет явно противоречить действительности. Забейте заголовок подозрительной новости и попробуйте поискать его, используя фильтры времени. Скажем, укажите прошлый год или прошлый месяц. Если вы найдёте аналогичную новость в архивах, то скорее всего это фейк.
6. **Отсутствие указания автора и источника**. Многие фейки генерируются автоматизировано, поэтому никаких упоминаний ни автора, ни источника не остаётся. Тем не менее в последнее время фейковые новости выходят за авторством никому не известных журналистов — скорее всего их имена также случайны, и за ними не стоят реальные люди.

Попытайтесь найти новость или её авторов в мейнстрим-media. Прежде всего — в информационных агентствах.

Если же источники указаны, то попробуйте изучить их. Зачастую под видом копий, действующих официальных информационных ресурсов, совершают попытки скрыть реальные источники информации или их отсутствие.

3. РЕКОМЕНДАЦИИ ПО ОРГАНИЗАЦИИ РАБОТЫ В СФЕРЕ ПРОФИЛАКТИКИ ИДЕОЛОГИИ ТЕРРОРИЗМА В СТУДЕНЧЕСКОЙ И МОЛОДЕЖНОЙ СРЕДЕ

Профилактика идеологии терроризма в образовательных организациях должна быть ориентирована на недопущение распространения идеологии терроризма среди

обучающихся и формирование в молодежной среде неприятия идеологии терроризма в различных ее проявлениях.

Для решения указанных задач представляется целесообразным:

- на регулярной основе проводить опрос мнения молодых людей, с целью выявления радикальных настроений в студенческой среде. В качестве образца можно использовать анкетирование, представленное в приложении к указанным рекомендациям. Анкетирование позволит выявить мнение молодежи относительно проблемы терроризма как способа решения проблем (политических, религиозных и т.п.), имеющихся в обществе. Кроме того, в случае проведения подобного анкетирования по каждому факультету отдельно, образовательная организация будет в итоге иметь представление о ситуации на каждом факультете. Это даст возможность выявить те из них, в которых студенты наиболее подвержены идеологии терроризма (далее – выделенная категория лиц). Далее, образовательной организации предстоит провести с выявленной категорией лиц адресные профилактические мероприятия;

- проводить адресные профилактические мероприятия с выявленной категорией лиц необходимо с привлечением специалистов органов власти, имеющих практический опыт профилактики идеологии терроризма. Таковыми в Республике Дагестан являются представители Министерства по национальной политике и делам религий РД, Министерства по делам молодежи РД, а также Центра противодействия экстремизма Министерства внутренних дел по РД. Также, учитывая, что идеология терроризма, так или иначе, связана на сегодняшний день с религий, в частности с исламом, видится целесообразным привлекать к указанным встречам со студентами представителей ЦИРО «Муфтият Республики Дагестан»;

- проводить адресные профилактические мероприятия с выявленной категорией лиц в небольших группах (до 30 человек) с целью достижения большего эффекта и возможности построения встречи в формате диалога между экспертами и молодыми людьми. Ни в коем случае адресные профилактические мероприятия не должны принимать формат лекции;

- следует обращать внимание на вопросы, которые молодые люди задают экспертам в ходе бесед. Содержание задаваемых вопросов позволит в определенной степени определить уровень подверженности студентов влиянию представителей радикальных сообществ (например, если студент задается вопросом о том, можно ли слушать проповедника, находящегося в федеральном розыске либо являющегося последователем запрещенной в РФ организации, либо можно ли доброжелательно относиться к представителям другой религии/конфессии, и т.п.);

- создавать на базе образовательной организации дискуссионные площадки для предоставления студентам возможности обсуждать, к примеру, в формате дебатов, проблемы связанные с радикализацией молодежи, протестным настроением в молодежной среде и т.д.;

- организовывать конкурсы либо олимпиады среди студентов на знание законодательства РФ о противодействии терроризму. Знание антитеррористического законодательства в определенной степени будет способствовать предотвращению вовлечения молодых людей в противоправную деятельность. (К примеру, наиболее распространенным на сегодняшний день преступлением, связанным с терроризмом, и совершаемым молодыми людьми является оправдание терроризма, либо призывы к

совершению террористических действий в Интернет пространстве. Уголовным кодексом РФ за совершение подобного рода преступлений предусмотрена ответственность, о которой молодые люди могут не знать);

- привлекать студентов к созданию позитивного видео контента, который, в свою очередь, выступит определенной альтернативой активно распространяемым в Интернет пространстве деструктивным публикациям.

Образец проведения опроса с целью выявления среди студентов лиц, подверженных воздействию идеологии терроризма:

Анкетирование

1. Укажите Ваш пол
   - Мужской
   - Женский

2. Считаете ли Вы себя верующим человеком?
   - Да
   - Нет

3. Как Вы относитесь к представителям других религий?
   - Доброжелательно
   - Нейтрально
   - Неодобрительно
   - Негативно

4. Как Вы считаете, допустимо ли насильственное навязывание какой-либо веры?
   - Да, все люди должны придерживаться правильной веры.
   - Нет, нельзя навязывать веру
   - Не задумывался (ась)

5. Откуда Вы в основном получаете информацию о религии?
   - В общении с родственниками
   - Из религиозных мероприятий (посещение мечети, храма, синагоги и т.д.)
   - Из неофициальных источников в Интернете (просмотр видеороликов, социальных сетей и т.п.)
   - Из официальных религиозных интернет ресурсов
   - Обращаюсь к религиозным деятелям
   - Не интересуюсь этой темой

6. Как Вы поступаете, когда Вам нужно принять сложное для себя решение, сделать нравственный выбор?
   - Советуюсь с родителями, родственниками
   - Советуюсь с друзьями
   - Принимаю самостоятельное решение
   - Ищу ответ в Интернете

7. На Ваш взгляд, салафизм - это:
   - Настоящий, "чистый" Ислам, воспроизводящий образ жизни и веру ранней мусульманской общины

- Обычное направление в Исламе, не сильно отличающиеся от других
- Секта, которая неправильно, крайне радикально трактует Ислам
- Использование веры людей в политических целях

8. Могли ли бы Вы при каких-нибудь обстоятельствах найти оправдание для экстремиста / террориста?

- Да
- Скорее да
- Нет
- Скорее нет
- Затрудняюсь ответить

9. Какие внешние причины, по Вашему мнению, могут подтолкнуть человека к участию в террористических (экстремистских) группах?

- Влияние религиозных течений
- Финансовые проблемы, долги
- Психические травмы, отклонения
- Идеологические мотивы
- Стремление избежать уголовной ответственности за совершенные ранее преступления
- Отомстить за что-то властям

10. Как Вы полагаете, какие внутренние причины, мотивы толкают человека на то, чтобы стать экстремистом/террористом? Отметьте все подходящие варианты

- Стремление распространить свою веру, религиозные убеждения
- Стремление достичь материального благополучия
- Стремление переделать мир
- Стремление достичь справедливости
- Стремление ощутить власть над людьми
- Любовь к острым ощущениям, риску и т.д.
- Стремление обрести соратников, быть частью какой-то группы
- Стремление к самореализации

11. Какие проблемы актуальны лично для Вас на сегодняшний день?

- Найти вторую половинку, жениться
- Успешно завершить учёбу в вузе
- Устроиться на работу
- Неопределённость по поводу будущего
- Нет проблем
- Другое:

Интерпретация результатов:

1. Указание пола в анкете позволит определить при анализе степень подверженности идеологии терроризма отдельно ребят и девушек.

2. Результаты ответа на второй вопрос позволят иметь представление об уровне религиозности студентов отдельно взятого факультета.

3. Ответ на 3 вопрос будет уже первым индикатором подверженности студентов влиянию идеологии терроризма. Вместе с тем, наличие даже небольшой доли тех, кто неодобрительно относится к представителям других конфессий, говорит о необходимости рассмотрения возможности проведения тематических встреч, посвященных обсуждению вопросов межрелигиозного диалога, в частности на примере Дагестана.

4. Четвертый вопрос в анкете, по сути, является одним из ключевых, позволяющих определить уровень радикализации молодых людей. Наличие даже небольшого в целом процента ответов молодых людей, допускающих насильственное навязывание веры, подтверждает приведенный выше тезис о необходимости проведения соответствующей просветительской (межрелигиозного характера) и профилактической работы со студентами.

5. Результаты ответов на пятый вопрос дадут представление о том, откуда молодые люди черпают информацию о религии. Нет поводов для беспокойства, если студенты отдают предпочтение традиционным способам получения информации о религии (в общении с родственниками, из официальных религиозных интернет ресурсов, из посещения религиозных мероприятий (мечети, храмы, синагоги и т.д.). Однако, возможен немалый процент опрошенных, которые обращаются за указанной информацией к неофициальным источникам в интернете. Это не может не настораживать, поскольку, как показывает практика, молодежь в основном заражается радикальной идеологией через Интернет. В этой связи в качестве выхода можно предложить организацию тематических встреч либо круглых столов с участием представителей религиозных организаций с целью доведения до студентов информации о популярных СМИ и Интернет-ресурсов, на которых молодые люди могли бы получать достоверную информацию о религии.

6. Ответы респондентов на шестой вопрос позволят иметь представление о том, как поступят молодые люди в случае возникновения в их жизни тех или иных сложных ситуаций. Также определится радиус доверия студентов.

7. Результаты ответов на седьмой вопрос дадут представление о том, как понимают молодые люди термин «салафизм», который, исходя из печального опыта нашего региона, выглядел как радикальное направление в исламе. Учитывая то, что большинство молодых людей может не знать точного определения указанного термина, а также с учетом того, что такие понятия как «салафизм» «джихад», «шахид» активно используются радикалами в вербовочной деятельности, появляется необходимость доведения до студентов правильного понимания подобной лексики с позиции традиционного ислама.

8. Ответы на восьмой вопрос дадут четкое понятие об отношении молодых людей к террористам. Наличие даже относительно небольшого процента респондентов, готовых оправдать действия террористов будет говорить о необходимости проведения мероприятий, раскрывающих деструктивный характер деятельности террористов.

9. Результаты ответов на девятый вопрос позволят узнать мнение молодых людей о внешних причинах, подталкивающих человека к участию в террористических (экстремистских) группах.

10. Соответственно ответы на 10 вопрос позволят узнать мнение студентов о внутренних причинах, подталкивающих человека к участию в террористических (экстремистских) группах. Следует принять во внимание наиболее популярные ответы

по двум указанным вопросам о причинах участия человека в террористических группах. Они позволят правильно расставить акценты и эффективнее выстроить профилактическую работу с молодежью.

11. Результаты ответов на одиннадцатый вопрос позволять выявить те проблемы, которые являются наиболее актуальными для молодых людей в данный момент. Определение реальных проблем молодых людей позволит лицам, задействованным в работе с молодежью, правильно выстроить свою работу.

4. ТЕХНОЛОГИИ И ПРИОРИТЕТНЫЕ НАПРАВЛЕНИЯ ПРОФИЛАКТИЧЕСКОЙ РАБОТЫ В СФЕРЕ ТЕРРОРИЗМА, В ТОМ ЧИСЛЕ, В СЕТИ ИНТЕРНЕТ

Главной особенностью современного общества является сеть Интернет. Однако помимо положительных свойств интернета существует и негативная, которая может причинить вред не одному человеку: торговля оружием, распространение запрещённых веществ, мошенничество, вербовка. В глобальной сети размещаются противоправные материалы пропагандистского характера, направленные на возбуждение ненависти либо вражды.

Международные террористические организации активно используют ресурсы сети Интернет, и, как правило, проводят агитационную и вербовочную деятельность, направленную на увеличение числа их сторонников.

По статистике верховного суда РФ около 70 % совершённых преступлений были зафиксированы в социальных сетях. Можно выделить несколько основных проблем, которые мешают успешному противодействию экстремизма в сети Интернет:

1) отсутствие взаимодействия на международном уровне по вопросам правового регулирования функционирования Интернета, борьбы с преступностью [4, с. 48];

2) отсутствие правовых механизмов и технических возможностей по противодействию анонимности пользователей сети Интернет (например, VPN — обобщённое название технологий, позволяющих обеспечить одно или несколько сетевых соединений поверх другой сети);

3) активная деятельность криминалитета, выражающаяся в совершенствовании средств, методов, способов совершения преступлений и сокрытия следов.

Выходом из сложившейся ситуации является проведение последовательной работы по следующим направлениям:

1) совершенствование нормативно-правовой базы на основе мониторинга зарубежного законодательства;

2) разработка эффективных технических средств противодействия распространению идей экстремизма в сети Интернет;

3) международное сотрудничество и обмен передовым опытом;

4) подготовка соответствующих профессиональных кадров, способных противостоять современной преступности. Насущной является необходимость в качественном улучшении методов профилактики, которая должна быть нацелена на нейтрализацию объективных факторов, способствующих совершению преступлений; корректирующее воздействие, снижающий криминогенный потенциал субъективного фактора — умысел совершения преступлений; внесение дисфункции в цепочку криминогенных взаимодействий объективных и субъективных факторов, ведущее к

саморазрушению самого процесса приближения к посягательству на совершение преступления. Стратегия противодействия экстремизму в Российской Федерации до 2025 года (утв. Президентом РФ 28.11.2014 № Пр-2753) предусматривает следующие направления государственной политики в сфере противодействия экстремизму в сфере образования и государственной молодежной политики, носящие преимущественно профилактический характер и нацеленные на молодежь:

1) включение в региональные и муниципальные программы по развитию образования и воспитанию несовершеннолетних мероприятий по формированию у подрастающего поколения уважительного отношения ко всем этносам и религиям;

2) организация досуга детей, подростков, молодежи, семейного досуга, обеспечение доступности для населения объектов культуры, спорта и отдыха, создание условий для реализации творческого и спортивного потенциала, культурного роста граждан;

3) осуществление мер государственной поддержки системы воспитания молодежи на основе традиционных для российской культуры духовных, нравственных и патриотических ценностей Складывающаяся международная обстановка, внутриполитическая ситуация и тенденции развития информационно-телекоммуникационных технологий позволяют прогнозировать дальнейшее нарастание объемов использования информационных сетей в экстремистской и террористической деятельности. Своевременное предотвращение и пресечение имеющихся угроз зависит от эффективности, систематичности и согласованности проводимых мероприятий, а также от качества взаимодействия всех правоохранительных органов Российской Федерации и всех заинтересованных иностранных государств.

5. ВНИМАНИЕ! САЙТ С ЭКСТРЕМИСТСКИМ КОНТЕНТОМ. ЧТО ДЕЛАТЬ?

Относительно контента, размещенного в сети Интернет следует руководствоваться Федеральным законом от 25 июля 2002 г. № 114-ФЗ «О противодействии экстремистской деятельности» и Федеральным законом от 28.12.2013 № 398-ФЗ «О внесении изменений в Федеральный закон "Об информации, информационных технологиях и о защите информации». Согласно Федерального закона от 28.12.2013 № 398-ФЗ «О внесении изменений в Федеральный закон «Об информации, информационных технологиях и о защите информации», вступившего в силу с 01.02.14, генеральный прокурор РФ и его заместители уполномочены обращаться в Роскомнадзор с заявлением о принятии мер по ограничению доступа к информационным ресурсам, распространяющим призывы к массовым беспорядкам, осуществлению экстремистской деятельности и участию в массовых публичных мероприятиях. Такая процедура может быть инициирована генеральным прокурором РФ и его заместителями на основании мониторинга интернета, а также полученных от органов власти, организаций и граждан уведомлений.

Как это работает?

После получения требования генеральной прокуратуры Роскомнадзор незамедлительно направляет по системе взаимодействия операторам связи требование об ограничении доступа к информационному ресурсу или к размещенной на нем противоправной информации. Операторы связи после получения данного требования обязаны незамедлительно ограничить доступ к информационному ресурсу или к размещенной на нем незаконной информации. В дальнейшем Роскомнадзор определяет провайдера хостинга Интернет-ресурса, на котором содержится противозаконная

информация, и направляет ему уведомление о необходимости удаления такой информации. Провайдер хостинга должен сообщить владельцу информационного ресурса об обязанности незамедлительно удалить противоправный контент. Доступ к информационному ресурсу возобновляется после того, как Роскомнадзор получит от владельца сайта или хостинг-провайдера сообщение о том, что незаконная информация удалена, и удостоверится в этом.

Заметим, что до 01.02.14 досудебная блокировка могла применяться только к сайтам, распространяющим детскую порнографию, содержащим пропаганду наркотиков или самоубийств, а также ресурсам, на которых размещен пиратский видеоконтент. Как показывает обширная практика закон работает.

Руководство к действию: Если Вы обнаружили сайт экстремистской организации или просто сайт, нарушающий нормы ст.1 Закона от 25 июля 2002 г. № 114-ФЗ «О противодействии экстремистской деятельности», то немедленно обращайтесь в прокуратуру. Такие проявления экстремизма в Интернете требуется немедленно блокировать. В данном случае никаких переговоров с сетевыми экстремистами вести не следует. Просто блокировка ресурса на законных основаниях. Тем более прокуратура займется и непосредственными «хозяевами» ресурса. Последнее очень важно, потому что зачастую экстремисты в Интернете владеют целыми сетевыми структурами. И очень важно выявить такие структуры целиком. Ваше немедленное обращение - это сотни, а может быть тысячи не вовлеченных людей в экстремистские сети.

6. ГРАНИЦЫ КОМПЕТЕНЦИЙ СПЕЦИАЛИСТОВ УЧРЕЖДЕНИЙ ОРГАНОВ ПО ДЕЛАМ МОЛОДЕЖИ В ОБЛАСТИ ПРОФИЛАКТИКИ ТЕРРОРИЗМА

Практическая роль органов местного самоуправления наиболее высока, поскольку именно их представители имеют повседневный устойчивый контакт с населением, возможности для проведения адресной работы с конкретными гражданами, подверженными воздействию радикальных идеологий. В соответствии со статьей 5 «Профилактика экстремистской деятельности» Федерального закона от 2002 года № 114-ФЗ «В целях противодействия экстремистской деятельности органы местного самоуправления в пределах своей компетенции в приоритетном порядке осуществляют профилактические, в том числе воспитательные, пропагандистские, меры, направленные на предупреждение экстремистской деятельности».

В соответствии с **Федеральным законом от 06.03.2006 N 35-ФЗ (ред. от 18.04.2018, с изм. от 29.03.2019) "О противодействии терроризму"**(статья 5.2. Полномочия органов местного самоуправления в области противодействия терроризму (введена Федеральным законом от 06.07.2016 N 374-ФЗ)) органы местного самоуправления при решении вопросов местного значения по участию в профилактике терроризма, а также в минимизации и (или) ликвидации последствий его проявлений:

1) разрабатывают и реализуют муниципальные программы в области профилактики терроризма, а также минимизации и (или) ликвидации последствий его проявлений;

2) организуют и проводят в муниципальных образованиях информационно-пропагандистские мероприятия по разъяснению сущности терроризма и его общественной опасности, а также по формированию у граждан неприятия идеологии терроризма, в том числе путем распространения информационных материалов, печатной продукции, проведения разъяснительной работы и иных мероприятий;

3) участвуют в мероприятиях по профилактике терроризма, а также по минимизации и (или) ликвидации последствий его проявлений, организуемых федеральными органами исполнительной власти и (или) органами исполнительной власти субъекта Российской Федерации;

4) обеспечивают выполнение требований к антитеррористической защищенности объектов, находящихся в муниципальной собственности или в ведении органов местного самоуправления;

5) направляют предложения по вопросам участия в профилактике терроризма, а также в минимизации и (или) ликвидации последствий его проявлений в органы исполнительной власти субъекта Российской Федерации;

6) осуществляют иные полномочия по решению вопросов местного значения по участию в профилактике терроризма, а также в минимизации и (или) ликвидации последствий его проявлений.

Итак, основными направлениями работы по противодействию экстремизму и идеологии терроризма в молодежной среде являются: получение качественного, образования, социальная защищенность (трудоустройство), создание условий и возможностей для успешной социализации и эффективной самореализации молодежи, для развития ее потенциала в интересах России, патриотического и гражданского воспитание, формирование культуры межнационального общения и установок толерантного сознания.

7. ОТВЕТСТВЕННОСТЬ В СЕТИ ИНТЕРНЕТ

За совершение преступлений и административных правонарушений, в том числе в сети «Интернет», граждане подлежат привлечению к уголовной и административной ответственности.

Уголовная ответственность – ответственность за совершение преступлений, предусмотренных Уголовным кодексом Российской Федерации (далее – УК РФ).

В соответствии со статьей 14 УК РФ преступление – виновно совершенное общественно опасное деяние, запрещенное УК РФ под угрозой наказания.

УК РФ предусматривает ответственность за преступления, совершаемые в том числе с использованием сети «Интернет»:

- доведение до самоубийства (статья 110);
- склонение к совершению самоубийства или содействие совершению самоубийства (статья 110.1);
- организация деятельности, направленной на побуждение к совершению самоубийства (статья 110.2);
- вовлечение несовершеннолетнего в совершение действий, представляющих опасность для жизни несовершеннолетнего (статья 151.2);
- незаконные организация и проведение азартных игр (171.2);
- манипулирование рынком (статья 185.3);
- публичные призывы к осуществлению террористической деятельности, публичное
- оправдание терроризма или пропаганда терроризма (статья 205.2);
- незаконные производство, сбыт или пересылка наркотических средств, психотропных веществ или их аналогов, а также незаконные сбыт или пересылка растений, содержащих наркотические средства или психотропные вещества, либо их частей, содержащих наркотические средства или психотропные вещества (статья 228.1);

- обращение фальсифицированных, недоброкачественных и незарегистрированных лекарственных средств, медицинских изделий и оборот фальсифицированных биологически активных добавок (статья 238.1);

- незаконные изготовление и оборот порнографических материалов или предметов (статья 242);

- изготовление и оборот материалов или предметов с порнографическими изображениями несовершеннолетних (статья 242.1);

- использование несовершеннолетнего в целях изготовления порнографических материалов или предметов (статья 242.2);

- жестокое обращение с животными (статья 245);

- незаконные добыча и оборот особо ценных диких животных и водных биологических ресурсов, принадлежащих к видам, занесенным в Красную книгу Российской Федерации и (или) охраняемым международными договорами Российской Федерации (статья 258.1);

- публичные призывы к осуществлению экстремистской деятельности (статья 280);

- публичные призывы к осуществлению действий, направленных на нарушение территориальной целостности Российской Федерации (статья 280.1);

- возбуждение ненависти либо вражды, а равно унижение человеческого достоинства (статья 282).

Так, в соответствии с частью 2 статьи 205.2 УК РФ публичные призывы к осуществлению террористической деятельности, публичное оправдание терроризма или пропаганда терроризма, совершенные с использованием средств массовой информации либо электронных или информационно-телекоммуникационных сетей, в том числе сети «Интернет», наказываются штрафом в размере от трехсот тысяч до одного миллиона рублей или в размере заработной платы или иного дохода осужденного за период от трех до пяти лет либо лишением свободы на срок от пяти до семи лет с лишением права занимать определенные должности или заниматься определенной деятельностью на срок до пяти лет.

Согласно пункту «б» части 2 статьи 228.1 УК РФ сбыт наркотических средств, психотропных веществ или их аналогов, совершенный с использованием средств массовой информации либо электронных или информационно-телекоммуникационных сетей (включая сеть «Интернет»), наказывается лишением свободы на срок от пяти до двенадцати лет со штрафом в размере до пятисот тысяч рублей или в размере заработной платы или иного дохода осужденного за период до трех лет либо без такового и с ограничением свободы на срок до одного года либо без такового.

В соответствии с пунктом «г» части 2 статьи 242.2 УК РФ фото-, кино- или видеосъемка несовершеннолетнего в целях изготовления и (или) распространения порнографических материалов или предметов либо привлечение несовершеннолетнего в качестве исполнителя для участия в зрелищном мероприятии порнографического характера, совершенные лицом, достигшим восемнадцатилетнего возраста, с использованием информационно-телекоммуникационных сетей (включая сеть «Интернет»), наказываются лишением свободы на срок от восьми до пятнадцати лет с лишением права занимать определенные должности или заниматься определенной деятельностью на срок до двадцати лет либо без такового и с ограничением свободы на срок до двух лет либо без такового.

Административная ответственность за совершение правонарушений, в том числе с использованием сети «Интернет», предусмотрена Кодексом Российской Федерации об административных правонарушениях (далее – КоАП РФ).

В соответствии со статьей 2.1 КоАП РФ административным правонарушением признается противоправное, виновное действие (бездействие) физического или юридического лица, за которое КоАП РФ или законами субъектов Российской Федерации об административных правонарушениях установлена административная ответственность.

КоАП РФ предусмотрена ответственность за такие правонарушения, совершаемые в том числе с использованием сети «Интернет»:

- размещение в информационной продукции для детей, включая информационную продукцию, размещаемую в информационно-телекоммуникационных сетях (в том числе в сети «Интернет»), объявления о привлечении детей к участию в создании информационной продукции, причиняющей вред их здоровью и (или) развитию. Влечет наложение административного штрафа на граждан в размере от одной тысячи до полутора тысяч рублей; на должностных лиц - от двух тысяч до трех тысяч рублей; на юридических лиц - от двадцати тысяч до тридцати тысяч рублей (часть 3 статьи 6.17);

- пропаганда нетрадиционных сексуальных отношений среди несовершеннолетних, выразившаяся в распространении информации, направленной на формирование у несовершеннолетних нетрадиционных сексуальных установок, привлекательности нетрадиционных сексуальных отношений, искаженного представления о социальной равноценности традиционных и нетрадиционных сексуальных отношений, либо навязывание информации о нетрадиционных сексуальных отношениях, вызывающей интерес к таким отношениям, совершенные с применением средств массовой информации и (или) информационно-телекоммуникационных сетей (в том числе сети «Интернет»), если эти действия не содержат уголовно наказуемого деяния. Влечет наложение административного штрафа на граждан в размере от пятидесяти тысяч до ста тысяч рублей; на должностных лиц - от ста тысяч до двухсот тысяч рублей; на юридических лиц - одного миллиона рублей либо административное приостановление деятельности на срок до девяноста суток (часть 2 статьи 6.21);

- реализация фальсифицированных, контрафактных, недоброкачественных или незарегистрированных лекарственных средств или фальсифицированных биологически активных добавок либо реализация фальсифицированных, контрафактных или недоброкачественных медицинских изделий, совершенные с использованием средств массовой информации или информационно-телекоммуникационных сетей, в том числе сети «Интернет», если эти действия не содержат уголовно наказуемого деяния. Влечет наложение административного штрафа на граждан в размере от семидесяти пяти тысяч до двухсот тысяч рублей; на должностных лиц - от ста пятидесяти тысяч до шестисот тысяч рублей; на индивидуальных предпринимателей - от ста пятидесяти тысяч до шестисот тысяч рублей или административное приостановление деятельности на срок до девяноста суток; на юридических лиц - от двух миллионов до шести миллионов рублей или административное приостановление деятельности на срок до девяноста суток (часть 3 статьи 6.33);

- включение недостоверных сведений о санитарном и лесопатологическом состоянии лесов в акт лесопатологического обследования либо размещение на официальном сайте органа государственной власти или органа местного самоуправления в информационно-

телекоммуникационной сети «Интернет» утвержденного акта лесопатологического обследования, содержащего недостоверные сведения о санитарном и лесопатологическом состоянии лесов. Влечет наложение административного штрафа на должностных лиц в размере от пяти тысяч до двадцати тысяч рублей (часть 2 статьи 8.5.2);

- публичное распространение выражающих явное неуважение к обществу сведений о днях воинской славы и памятных датах России, связанных с защитой Отечества, либо публичное осквернение символов воинской славы России, в том числе совершенные с применением средств массовой информации и (или) информационно-телекоммуникационных сетей (в том числе сети «Интернет»). Влечет наложение административного штрафа на юридических лиц в размере от четырехсот тысяч до одного миллиона рублей (часть 4 статьи 13.15);

- неисполнение оператором связи, оказывающим услуги по предоставлению доступа к информационно-телекоммуникационной сети «Интернет», обязанности по ограничению или возобновлению доступа к информации, доступ к которой должен быть ограничен или возобновлен на основании сведений, полученных от федерального органа исполнительной власти, осуществляющего функции по контролю и надзору в сфере связи, информационных технологий и массовых коммуникаций. Влечет наложение административного штрафа на должностных лиц в размере от десяти тысяч до тридцати тысяч рублей; на юридических лиц - от ста тысяч до пятисот тысяч рублей. (статья 13.34);

- организация и (или) проведение азартных игр с использованием игрового оборудования вне игорной зоны, либо без полученной в установленном порядке лицензии на осуществление деятельности по организации и проведению азартных игр в букмекерских конторах и тотализаторах вне игорной зоны, либо без полученного в установленном порядке разрешения на осуществление деятельности по организации и проведению азартных игр в игорной зоне, либо с использованием информационно-телекоммуникационных сетей (в том числе сети «Интернет») или средств связи (в том числе подвижной связи), за исключением случаев приема интерактивных ставок организаторами азартных игр в букмекерских конторах и (или) тотализаторах. Влечет наложение административного штрафа на юридических лиц в размере от восьмисот тысяч до одного миллиона пятисот тысяч рублей с конфискацией игрового оборудования (часть 1 статьи 14.1.1);

- распространение в информационно-телекоммуникационных сетях, в том числе в сети «Интернет», информации, выражающей в неприличной форме, которая оскорбляет человеческое достоинство и общественную нравственность, явное неуважение к обществу, государству, официальным государственным символам Российской Федерации, Конституции Российской Федерации или органам, осуществляющим государственную власть в Российской Федерации, за исключением случаев, предусмотренных статьей 20.3.1 КоАП РФ, если эти действия не содержат уголовно наказуемого деяния. Влечет наложение административного штрафа в размере от тридцати тысяч до ста тысяч рублей (часть 3 статьи 20.1);

- действия, направленные на возбуждение ненависти либо вражды, а также на унижение достоинства человека либо группы лиц по признакам пола, расы, национальности, языка, происхождения, отношения к религии, а равно принадлежности к какой-либо социальной группе, совершенные публично, в том числе с использованием средств массовой информации либо информационно-телекоммуникационных сетей,

включая сеть «Интернет», если эти действия не содержат уголовно наказуемого деяния. Влечет наложение административного штрафа на граждан в размере от десяти тысяч до двадцати тысяч рублей, или обязательные работы на срок до ста часов, или административный арест на срок до пятнадцати суток; на юридических лиц - от двухсот пятидесяти тысяч до пятисот тысяч рублей (статья 20.3.1).

8. СРЕДСТВА РЕАЛИЗАЦИИ КОМПЛЕКСНОЙ ЗАЩИТЫ ИНФОРМАЦИИ

Рассмотрим основные средства, используемые для создания механизмов защиты.

Все средства защиты делятся на формальные (выполняющие защитные функции строго по заранее предусмотренной схеме без непосредственного участия человека) и неформальные (определяются целенаправленной деятельностью человека либо регламентируют эту деятельность).

Технические средства представляют собой электрические, электромеханические и электронные устройства. Вся совокупность технических средств делится на аппаратные и физические.

Под аппаратными техническими средствами принято понимать устройства, встраиваемые непосредственно в телекоммуникационную аппаратуру, или устройства, которые сопрягаются с подобной аппаратурой через стандартный интерфейс. Физические средства включают в себя автономные устройства и системы. Это могут быть, например, замки на дверях помещений, где размещена аппаратура или носители особо конфиденциальной информации, решетки на окнах, электронно-механическое оборудование охранной сигнализации.

Программные средства представляют собой программное обеспечение, специально предназначенное для выполнения функций защиты информации.

Указанные выше средства и составляли основу механизмов защиты на первой фазе развития технологии обеспечения безопасности связи в каналах телекоммуникаций. При этом считалось, что основными средствами защиты являются программные. Практика показала, что надежность подобных механизмов защиты является явно недостаточной. Особенно слабым звеном оказалась защита с помощью пароля. Поэтому в дальнейшем механизмы защиты становились все более сложными, к ним начали привлекать другие средства обеспечения безопасности.

Организационные средства защиты представляют собой организационно-технические и организационно-правовые мероприятия, осуществляемые в процессе создания и эксплуатации аппаратуры телекоммуникаций для обеспечения защиты информации. Организационные мероприятия охватывают все структурные элементы системы на всех этапах их жизненного цикла (строительство помещений, проектирование системы, монтаж и наладка оборудования, испытания и эксплуатация).

Законодательные средства защиты определяются законодательными актами, которыми регламентируются правила использования, обработки и передачи информации ограниченного доступа и устанавливаются меры ответственности за нарушение этих правил.

Морально-этические средства защиты реализуются в виде всевозможных норм, которые сложились традиционно или складываются по мере развития техники и средств связи в нашем обществе. Эти нормы большей частью не являются обязательными, как законодательные меры, однако несоблюдение их ведет обычно к потере авторитета человека или престижа организации.

9. ПРОСТЫЕ ПРИМЕРЫ ДЛЯ РЕШЕНИЯ СЛОЖНЫХ ПРОБЛЕМ

Пока в организацию не пришел профессиональный специалист, способный системно обеспечить решение вопросов информационной безопасности, мы рекомендуем руководителям и сотрудникам паллиативных служб придерживаться простых правил и внедрять базовые принципы безопасности:

1. НАДЕЖНЫЙ ПАРОЛЬ.

Использование надежных паролей далеко не такой простой вопрос, как может показаться на первый взгляд. И хотя большинство пользователей знают фундаментальные требования к надежному паролю, в повседневной жизни они забывают о них, предпочитая надежному паролю простой и легко запоминающийся.

Самые важные пароли должны быть максимально надежными и фиксироваться только в памяти.

Разберем схему выше. Вся информация на вашем компьютере должна быть зашифрована, и для ее дешифровки вам нужно будет вводить пароль. Это пароль высокой степени важности, его вы храните в памяти. Вы расшифровали жесткий диск, все ваши пароли обычной степени важности хранятся в зашифрованном файле ключей менеджера паролей (KeePassXC). Для расшифровки этого файла также используется пароль высокой степени важности.

Теперь поговорим о создании практически очень надежных паролей. «Очень надежных» – потому что рано или поздно можно подобрать любой пароль, но время подбора может занять не одну тысячу лет.

Требования к надежному паролю:

- Это не должны быть слова или фразы.
- Пароль arC2397_1 всегда будет более надежным, нежели car23971.
- Это не должны быть даты, особенно знаковые даты.
- Пароль должен содержать не менее 20 символов.
- Пароль должен включать символы верхнего и нижнего регистра, более одной цифры, специальные символы.
- Этот пароль не должен содержать информацию, связанную с вами: адрес, клички домашних животных, дату рождения, номер телефона, название любимой спортивной команды.

Каждый пароль должен быть уникальным, пароли не должны быть похожими.

Ни в коем случае не используйте один и тот же пароль в двух местах.

Придумать надежный пароль, который бы соответствовал всем вышеизложенным требованиям и в то же время был максимально простым для запоминания, – не самая простая задача, но в ваших интересах с ней справиться.

2. ДВОЙНАЯ АУТЕНТИФИКАЦИЯ

Аутентификация – проверка подлинности чего-либо, например, проверка введенного пароля путем сравнивания с указанным при регистрации.

Пароль сегодня – самый популярный инструмент защиты доступа, но даже очень надежный пароль уязвим, а потому многими сервисами и программами предлагается помимо пароля использовать какой-либо инструмент дополнительной защиты.

В целом аутентификация не обязательно должна быть именно двойной, она может быть и тройной: например, сначала вы вводите постоянный пароль, потом получаете СМС с одноразовым паролем, а затем подтверждаете свою личность отпечатком пальца.
Наличие двойной аутентификации зависит от сервиса или используемого программного обеспечения: вы не можете использовать ее там, где она не заложена разработчиком. Да и сама двойная аутентификация бывает различной.

SMS-КОДЫ

SMS-коды – средство дополнительной защиты, подразумевающее отправку СМС с авторизационным кодом на номер, указанный в профиле пользователя. Механизм можно считать довольно надежным, но только в том случае, когда ваш номер неизвестен злоумышленникам. К сожалению, восстановить номер или перехватить СМС сегодня не сложно. Есть разные способы перехвата СМС: восстановление сим-карты, доступ к данным на уровне оператора, взлом устройства, принимающего СМС, использование уязвимостей SS7 или поддельной базовой станции. Необходимо помнить, что СМС – это ненадежно, хотя и лучше, чем отсутствие двойной аутентификации.

По возможности откажитесь от СМС в пользу более надежных способов двойной аутентификации.

EMAIL-КОДЫ

Метод можно назвать вполне надежным только в том случае, если есть доступ к электронной почте с другого устройства. Если вы авторизуетесь со своего компьютера и на этом же компьютере принимаете email с кодом, смысл двойной аутентификации теряется.

Не принимайте email-коды на том же устройстве, с которого осуществляется авторизация.

ТАБЛИЦА С КОДАМИ

Таблица с кодами – способ дополнительной защиты, предусматривающий наличие таблицы с нумерованными кодами, один из которых запрашивается при авторизации. Такую таблицу надо обязательно распечатать, не имеет смысла хранить ее в электронном виде. Это позволит защититься, например, от вредоносного программного обеспечения, которое используется мошенниками для кражи пароля. Злоумышленники могут получить доступ к вашему компьютеру и украсть у вас пароль, но он им ничего не даст, так как для авторизации будет необходимо указать код из таблицы, которой нет на вашем компьютере. К сожалению, пользователи часто не понимают этого и хранят таблицу с кодами в электронном виде. Этим они облегчают мошенникам задачу, фактически сводя на нет двухфакторную аутентификацию.

Распечатайте таблицу с кодами и никогда не храните ее в электронном виде.

3. ***ЗАЩИТА РОУТЕРА***

Так сложилось, что многие несерьезно относятся к защите своей домашней и корпоративной Wi-Fi-сети и самого маршрутизатора. Даже если Wi-Fi-сеть защищают каким-то паролем, заводской пароль маршрутизатора оставляют неизмененным. Очень часто пользователи оставляют Wi-Fi-сеть полностью открытой. По доброте душевной или просто лень устанавливать, а потом еще и вводить этот пароль.

УСТАНОВИТЕ НАДЕЖНЫЙ ПАРОЛЬ WI-FI-СЕТИ

Ваша Wi-Fi-сеть должна быть защищена паролем. Хорошим паролем. Никаких «11111111», «12345678», «qwertyui» и т. д. Не поленитесь придумать надежный пароль, в котором будут заглавные буквы, цифры и специальные знаки (~ ! @ # $ % & *).

Настройки безопасности беспроводной сети – это не только пароль. В настройках необходимо выбрать современный и надежный тип безопасности и шифрования беспроводной сети. Оптимальный выбор защиты – WPA2 – Personal с шифрованием AES.

Защитите настройки маршрутизатора паролем

Этот пароль никак не относится к Wi-Fi. Он используется исключительно для защиты настроек роутера. Чтобы никто, кроме вас, не смог зайти в веб-интерфейс роутера и сменить там какие-то настройки. Как правило, устанавливается логин и пароль (иногда только пароль). На некоторых роутерах он установлен по умолчанию. Обычно используется admin/ admin. Если по умолчанию пароль не установлен, то в процессе первой настройки роутер предлагает установить его. Но это в любой момент можно сделать на панели управления. ***Отключите функцию WPS***

С помощью WPS можно быстро и без ввода пароля подключать устройства к беспроводной сети. Но, как показывает практика, WPS мало кто пользуется. Можно найти много материалов, где говорится о разных проблемах с безопасностью функции WPS. Поэтому, для защиты роутера от взлома, эту функцию лучше отключить.

Кроме этого, из-за WPS очень часто не удается подключить некоторые устройства к Wi-Fi или настроить маршрутизатор в режиме моста.

Спрячьте Wi-Fi-сеть от посторонних глаз

В настройках Wi-Fi-сети на маршрутизаторе есть такая функция как «Скрыть SSID» (Hide SSID), или «Отключить широковещание SSID». После ее активации устройства перестанут видеть вашу Wi-Fi-сеть. А чтобы к ней подключиться, нужно будет указать не только пароль, но и имя самой сети (SSID). А это дополнительная защита.

Эта настройка обычно находится в разделе с настройками беспроводной сети. Можете посмотреть, например, как сделать Wi-Fi-сеть невидимой на роутерах TP-Link.

4. ***ОПАСНЫЕ ФЛЕШКИ***

Классифицируем угрозы, которые могут исходить от флешки или иного USB-носителя, например, внешнего жесткого диска.

Первое – это вредоносное программное обеспечение, записанное на флешку с целью заразить компьютер жертвы. Об этой угрозе знает большинство читателей. Однако автозапуск файлов сегодня блокируют практически все операционные системы и тем более антивирусы, потому простое открытие флешки с трояном в большинстве ситуаций неопасно.

Второе – это флешки, на которых размещены сами по себе безопасные файлы, цель которых – привести пользователя на сайт злоумышленника.

Третье – это мошенничество. Например, на флешке могут оказаться доступы к интернет-банку с тысячами долларов на счету.

Флешка может оказаться и USB-киллером, способным вывести из строя компьютер жертвы – это четвертый вариант атаки.

Пятый вариант – BadUSB. На наш взгляд, это самый опасный способ атаки. В данном случае флешка выдает себя за другое устройство, подключаемое через USB.

Шестой вариант – флешка-жучок, которая не наносит вреда компьютеру, разве что заряжается от него, но используется как микрофон для прослушки периметра и/или как

GPS-трекер для отслеживания местоположения. Подобные устройства можно легко купить, и с помощью такой флешки можно шпионить за кем угодно.

Никогда и ни при каких обстоятельствах не используйте найденные чужие флешки. Делать исключение не стоит даже для флешек, полученных от людей, которым вы доверяете. Многие популярные вредоносные программы умеют самостоятельно записывать себя на внешние носители информации, подключаемые к скомпрометированному устройству, таким образом заражая все новые компьютеры.

Не доверяйте даже флешкам, полученным от доверенных лиц.

Есть еще одна адресная атака, которая обычно применяется против руководителей организаций и о которой вам стоит знать. У многих из нас есть USB-флешки, и большинство из них – стандартные модели, которые каждый может приобрести в магазине. Злоумышленник выясняет, какую флешку использует жертва, и приобретает аналогичную. На нее записывается вредоносная программа. Для программы используется ярлык в виде папки, и жертва думает, что это папка, хотя на самом деле это исполняемый файл. Вставив флешку, жертва не обнаруживает файлов, зато видит «папку» Kingston, которую непременно попытается открыть. В этом случае система уведомит о попытке запуска приложения, которое может называться Kingston security update. Оно будет подписано не связанным с Kingston разработчиком, и никто этого не заметит.

После этого жертве будет сообщено, что это важные обновления, установка которых необходима для дальнейшего использования продукта. В процессе установки у жертвы будут запрошены права администратора, после чего на рабочем столе появится ярлык программы «Kingston Update», а флешка будет очищена. Жертва, скорее всего, удалит установленную программу, проверит ее на вирусы. Но антивирусам придраться будет не к чему, программа служит только для отвлечения внимания и не представляет никакой угрозы. Настоящая угроза уже тайно установлена в систему с правами администратора, и это дает атакующему фактически неограниченную власть над устройством жертвы.

Не недооценивайте угрозу, исходящую от USB-носителей информации, и это не только флешки, но и внешние жесткие диски. Постарайтесь вообще не подключать чужие носители к своему компьютеру, это лучшая защита.

5. ФИШИНГ И ЗАЩИТА ОТ НЕГО

Фишинг – это вид интернет-мошенничества, построенный на принципах социальной инженерии. Главная цель фишинга – получить доступ к критически важным данным (например, паспортным), учетным записям, банковским реквизитам, закрытой служебной информации, чтобы использовать их в дальнейшем для кражи денежных средств. Работает фишинг через перенаправление пользователей на поддельные сетевые ресурсы, являющиеся полной имитацией настоящих.

Классический фишинг – фишинг подмены

К этой категории можно отнести большую часть всех фишинговых атак. Злоумышленники рассылают электронные письма от имени реально существующей компании с целью завладеть учетными данными пользователей и получить контроль над их личными или служебными аккаунтами. Вы можете получить фишинговое письмо от имени платежной системы или банка, службы доставки, интернет-магазина, социальной сети, налоговой и т.д.

Фишинговые письма создают с большой скрупулезностью. Они практически ничем не отличаются от тех писем, которые пользователь регулярно получает в рассылках от настоящей компании. Единственное, что может насторожить, – просьба перейти по ссылке для выполнения какого-либо действия. Переход этот однако ведет на сайт мошенников, являющийся «близнецом» страницы сайта банка, социальной сети или другого легального ресурса.

Побудительным мотивом для перехода по ссылке в подобных письмах может выступать как «пряник» («Вы можете получить 70% скидку на услуги, если зарегистрируетесь в течение суток»), так и «кнут» («Ваша учетная запись заблокирована в связи с подозрительной активностью. Чтобы подтвердить, что вы владелец аккаунта, перейдите по ссылке»).

Примеры фишинга:

ВАША УЧЕТНАЯ ЗАПИСЬ БЫЛА ИЛИ БУДЕТ ЗАБЛОКИРОВАНА /ОТКЛЮЧЕНА.

Тактика запугивания пользователя может быть очень эффективной. Угроза того, что аккаунт был или в ближайшее время будет заблокирован, если пользователь сейчас же не зайдет в учетную запись, заставляет тут же потерять бдительность, перейти по ссылке в письме и ввести свой логин и пароль.

В ВАШЕЙ УЧЕТНОЙ ЗАПИСИ ОБНАРУЖЕНЫ ПОДОЗРИТЕЛЬНЫЕ ИЛИ МОШЕННИЧЕСКИЕ ДЕЙСТВИЯ. ТРЕБУЕТСЯ ОБНОВЛЕНИЕ НАСТРОЕК БЕЗОПАСНОСТИ.

В таком письме пользователя просят срочно войти в учетную запись и обновить настройки безопасности. Действует тот же принцип, что и в предыдущем пункте. Пользователь паникует и забывает о бдительности.

ВЫ ПОЛУЧИЛИ ВАЖНОЕ СООБЩЕНИЕ. ПЕРЕЙДИТЕ В ЛИЧНЫЙ КАБИНЕТ, ЧТОБЫ ОЗНАКОМИТЬСЯ.

Чаще всего такие письма присылают от имени финансовых организаций. Пользователи склонны верить правдивости писем, поскольку финансовые организации действительно не пересылают конфиденциальную информацию по электронной почте.

ФИШИНГОВЫЕ ПИСЬМА НАЛОГОВОЙ ТЕМАТИКИ.

Такие письма входят в тренд, как только близится время платить налоги. Темы писем могут быть самыми разными: уведомление о задолженности, просьба выслать недостающий документ, уведомление о праве на получение возврата налога и т.д.

На данном рисунке изображены два экрана: первый экран – поддельная страница авторизации в популярной социальной сети, которая открылась у «жертвы». Второе окно – у злоумышленника, в котором он видит логин с паролем от входа в личный профиль, которые ввел человек, перейдя по фишинговой ссылке.

Типичное предупреждение от браузера, которое не стоит игнорировать. Получив такое предупреждение, обязательно проверьте в строке ввода адреса сайта его название, которое должно совпадать с тем, куда вы пытаетесь зайти.

Защита о т фишинга – основные правила

1. Обязательно проверить URL-адрес, по которому рекомендуется перейти, на наличие незначительных ошибок в написании.

2. Использовать лишь безопасные https-соединения. Отсутствие всего одной буквы “s” в адресе сайта должно насторожить.

3. С подозрением относиться к любым письмам с вложениями и ссылками. Даже если они пришли со знакомого адреса, это не дает гарантии безопасности: он мог быть взломан.

4. Получив неожиданное подозрительное письмо, стоит связаться с отправителем каким-либо альтернативным способом и уточнить, он ли послал сообщение.

5. Если все же необходимо посетить ресурс, лучше ввести его адрес вручную или воспользоваться ранее сохраненными закладками (увы, от фарминга это не убережет).

6. Не использовать для доступа к онлайн-банкингу и другим финансовым сервисам открытые Wi-Fi-сети: часто их создают злоумышленники. Даже если сеть оригинальна, подключиться к незащищенному соединению не составляет сложности для хакеров.

7. На всех аккаунтах, где это возможно, подключить двухфакторную аутентификацию. Эта мера может спасти положение, если основной пароль стал известен взломщикам.

6. ИСПОЛЬЗОВАНИЕ VPN

Более половины популярных бесплатных VPN-приложений имеют связь с Китаем, где интернет жестко контролируется.

Почти 60% самых популярных бесплатных VPN-приложений в Google Play Store и Apple App Store созданы китайскими разработчиками или принадлежат владельцам из Китая. Об этом сообщается в отчете компании Metric Labs. «Как показало наше исследование, более половины самых популярных бесплатных VPN-приложений или принадлежат китайцам, или были созданы в Китае, где за последний год усилилось давление на VPN-сервисы, а интернет жестко контролируется», – сообщил глава исследовательского отдела Metric Labs.

В ходе исследования специалисты изучили первую двадцатку бесплатных VPN-приложений из поисковой выдачи Google Play Store и Apple App Store в США и Великобритании. У 17 из 30 приложений (10 приложений были в обоих магазинах) исследователи обнаружили юридическую связь с Китаем – они либо были зарегистрированы в КНР, либо принадлежали китайским владельцам.

У большинства проанализированных приложений практически отсутствует юридически закрепленная защита приватности и поддержка пользователей. У 86% сервисов политика конфиденциальности является «неприемлемой». К примеру, в некоторых не уточняется, регистрируется ли трафик, а некоторые сформулированы лишь в общих чертах даже без упоминания слова VPN.

В ряде приложений политика конфиденциальности и вовсе отсутствует. Более того, в пользовательских соглашениях нескольких приложений прописано, что они обмениваются данными с третьими сторонами, отслеживают пользователей и отправляют данные в Китай.

Ваши личные данные, которые «шифруются» подобными приложениями, могут попасть не в те руки. Приватностью и анонимностью это назвать сложно, так как функционал напоминает *proxy-сервер (простая подмена ip)*.

Почти у половины исследованных приложений политика конфиденциальности размещена в текстовых файлах на Pastebin, серверах AWS или IP-адресах без указания

доменного имени. У 64% сервисов отсутствует сайт, а работа осуществляется непосредственно из магазина приложений.

10. ИНФОРМАЦИОННОЕ ВОЛОНТЕРСТВО КАК РЕСУРС

Сегодня уже ни у кого не вызывает сомнений ценность, эффективность и незаменимость волонтерства в решении самых разных социальных проблем. В паллиативной помощи детям добровольчество стало неотъемлемым элементом профессиональной работы, обеспечивающим высокое качество жизни детей с тяжелыми заболеваниями.

Вместе с тем практика показывает, что даже организации паллиативной помощи детям, в которых уровень развития волонтерских программ довольно высок, зачастую недооценивают возможности информационного или киберволонтерства.

Добровольческие инициативы в интернет-пространстве находятся на этапе развития, поэтому остановимся подробнее на задачах, которые способно решить информационное волонтерство.

Спектр задач информационных волонтеров в контексте паллиативной помощи детям очень широк. Это и преодоление общественных стереотипов в отношении тяжелобольных детей, и распространение информации о возможностях получения помощи, и продвижение философии паллиативной помощи, и консультирование детей и родителей в вопросах безопасного использования интернета и социальных сетей.

Не следует забывать, что для пациентов паллиативных служб интернет служит не только источником информации. Для детей с тяжелыми заболеваниями, находящихся в детском хосписе или дома, интернет играет важную роль, помогая в социализации, обеспечивая возможность общения, дружбы и развития. Именно этот факт делает пациентов паллиативных организаций особенно уязвимыми перед лицом угроз и рисков, с которыми сопряжены современные интернет-коммуникации. Поэтому для специалистов паллиативной помощи так важно понимание интернет-рисков и умение идентифицировать и предотвратить опасности современного виртуального пространства. В этом огромную помощь могут оказать информационные волонтеры.

Опыт Детского хосписа Санкт-Петербурга показывает, что результативность программы информационного волонтерства зависит от ряда факторов:

1. Подготовка информационных волонтеров.

«Школа волонтера» является понятной и привычной ступенькой для всех, кто хочет бескорыстно помогать тяжелобольным детям и семьям, столкнувшимся с неизлечимым заболеванием ребенка. Если паллиативные службы не допускают к общению с детьми людей без специальной подготовки, то ровно такой же подход должен применяться к информационному волонтерству. Влияние информационного волонтера и степень его погруженности в личную историю подопечных может быть очень велика.

2. Наличие информационных волонтеров не отменяет необходимость мер безопасности интернет-пространства, обеспечиваемых со стороны организации паллиативной помощи, таких, например, как обновление программного обеспечения, контроль настроек роутера, антивирусная защита, своевременное обучение сотрудников по вопросам интернет-безопасности.

3. Грамотная организация документационного и организационного сопровождения программ информационного волонтерства.

Несмотря на то что информационное волонтерство пока не относится к областям, жестко регулируемым законодательством, наш опыт показывает, что заключение договоров о волонтерской деятельности в хосписе, неукоснительное требование не только соблюдения законодательства в отношении персональных данных, но и этического кодекса волонтера обеспечивают первичную защиту прав подопечных организации паллиативной помощи.

4. Оценка и профилактика рисков информационного волонтерства.

Информационное волонтерство в паллиативной помощи связано с доступом к персональной информации и медицинским сведениям, поэтому крайне важно контролировать данное направление и проводить регулярный мониторинг информационного пространства. Как правило, данная обязанность ложится на координатора волонтерских программ.

В заключение хотелось бы добавить, что параллельно с развитием паллиативной помощи в России развивается и рынок IT- и информационной безопасности. Многие компании, профессионально работающие в области информационной безопасности, постепенно приходят к пониманию необходимости развития корпоративной социальной ответственности. Мы рекомендуем рассматривать IT и IB компании как перспективный ресурс для развития собственных программ информационного волонтерства.

11. РАБОТА СО СРЕДСТВАМИ МАССОВОЙ ИНФОРМАЦИИ

Идеологию современного общества формируют средства массовой информации: радио и телевидение, газеты и журналы, социальные сети и информационные Интернет-ресурсы и др.

Для эффективной работы с молодежью необходимо активно работать со СМИ, а именно: участвовать и готовить репортажи для радио и телевидения, освещать и распространять материалы через печатные издания, информационные Интернет-ресурсы, социальные сети т.п.

Также для работы с молодежью желательно иметь собственные ресурсы - сайт организации, занимающейся реализацией молодежной политики, странички или сообщества в социальных сетях, информационное печатное издание, видеоролики и т.д.

Для своевременной подачи информации в СМИ организации необходимо составить список с контактной информацией представителей (ФИО руководителя или журналиста, наименование СМИ, электронная почта, номер телефона и т.д.) всех печатных СМИ, информационных интернет-ресурсов, групп или сообществ в социальных сетях, блогосферы, радио и телепередач и т.д.

Информацию о предстоящем мероприятии необходимо подавать своевременно, а именно:

- за 10дней рассылка в СМИ пресс-релиза о предстоящем мероприятии;
- за 3 дня рассылка в СМИ анонса мероприятия;
- за день до мероприятия рассылка в СМИ статьи о предстоящем мероприятии;
- сразу после мероприятия рассылка в СМИ основной статьи по мероприятию.

Следуя нижеизложенным рекомендациям, орган по делам молодежи сможет собственными силами вести свой собственный сайт, а также эффективно сотрудничать со

СМИ и Минмолодежи РД, поскольку наряду со статусом официального сайта Министерства по делам молодежи РД сайт http://minmol.e-dag.ru/ с 30.12.2016 года имеет и статус средств массовой информации (категория «Сетевые издания»).

Рекомендации по подготовке и размещению материалов на сайте Minmol.ru

1. Материалы для размещения на сайте Министерства по делам молодежи РД http://minmol.e-dag.ru/ и официальных страницах министерства в социальных сетях необходимо отправлять на почтовый ящик отдела информационного и методического сопровождения ГКУ РД «Республиканский молодежный центр» Минмолодежи РД **press@minmol.ru**.
2. В «Теме» письма необходимо указывать заголовок материала. Фото- и видеоматериалы должны быть прикреплены отдельными файлами или (когда объем материалов большой) в письме должна быть прямая ссылка на хранилище данных («Облако»), где они размещены. Текстовые материалы должны быть прикреплены к письму отдельным word-файлом. Не допускается отправка текстовых материалов, размещенных в окне самого электронного письма.
3. Редакция сайта http://minmol.e-dag.ru/, сформированная на основе отдела информационного и методического сопровождения ГБУ РД «РМЦ», оставляет за собой право вносить любые необходимые изменения в текстовые, фото- и видеоматериалы, присылаемые на свой адрес.

КАК ПИСАТЬ ТЕКСТОВЫЕ МАТЕРИАЛЫ?

1. При указании организаторов мероприятия выделяются главные или общие в соответствии с установленной иерархией.
2. За исключением особых случаев в качестве организаторов мероприятия не указываются имена отдельно взятых людей.
3. Любые сокращения, аббревиатуры (за исключением «вуз») при первом использовании в тексте необходимо привести в расшифрованном (полном) виде, в скобках указать «далее – сокращенный вариант/аббревиатура», например, государственная молодежная политика (далее – ГМП) и в дальнейшем можно уже использовать в виде сокращений или аббревиатур.
4. Личные имена в новостном материале должны приводиться в формате полного имени и фамилии. Имя следует располагать перед фамилией. Не допускается использование инициалов и отчеств. Исключение – биографии в юбилейных текстах и некрологи.
5. При указании должности участников мероприятия необходимо приводить только основную должность. Исключение составляют случаи, продиктованные контекстом, когда необходимо указывать дополнительные регалии, должности, ученые степени, звания и т.д. при наличии указания на основную должность.

ФОТО- И ВИДЕОМАТЕРИАЛЫ

1. Фотоматериалы не должны быть меньше 1024 px по широкой стороне.
2. Видеоматериалы не должны быть меньше 640×480 (соотношение 4:3) или 1280×720 (соотношение 16:9).

3. Не рекомендуется делать вертикальные фото.

4. Видеоматериалы, сделанные в режиме вертикальной съемки, не принимаются.

5. Фотоиллюстрации к новостным материалам должны быть в динамике, «рабочими», показывать ход мероприятия, а не его участников, выстроившихся в ряд у стены (баннера, доски и т.п.).

6. За исключением особых случаев (культурно-массовые мероприятия) не рекомендуется использовать фотоматериалы, на которых взгляд участников акцентирован в фотокамеру.

7. Не допускается отправка фотоматериалов, вставленных в word-документ.

8. Не допускается отправка фотоматериалов в виде коллажей и с содержанием, скорректированным при помощи фоторедакторов.

9. Не допускается отправка фотоматериалов, на которых использованы фотофильтры. При этом допускается коррекция по контрасту, резкости, глубине и свету с помощью фоторедактора.

10. При фото-, видеосъёмке не рекомендуется использовать цифровое увеличение.

11. За исключением особых случаев не рекомендуется водить камерой при видеосъемке из стороны в сторону.

12. Не рекомендуется фото- и видеосъемка, произведенные в движении. Лучше остановиться, снять кадр/видео в одной ракурсе, пройти необходимое расстояние и повторить съемку с другой позиции.

СТРУКТУРА НОВОСТИ

- Заголовок.
- Лид (лидер-абзац).
- «Тело» текста (основное содержание).
- Цитаты *(не всегда обязательный элемент текста).*
- Бэкграунд *(желательный, но не обязательный элемент текста).*

ЗАГОЛОВОК

- Концентрированное выражение лида новости.
- Должен дать читателю возможность понять, чему посвящен текст.
- В практике размещения материалов на сайте http://minmol.e-dag.ru/ запрещено использовать метафорические («игровые») заголовки.
- Идеальный заголовок – не более 70 символов.
- Рекомендуется использовать в заголовке короткие слова, аббревиатуры и т.п.

Примеры:

Хорошо:

В Минмолодежи РД обсудили новый закон «Об образовании».

Волонтеры Дагестана посетили детский приют в Махачкале.

Плохо:

В Министерстве по делам молодежи РД прошло обсуждение нового Федерального Закона № 273-ФЗ «Об образовании в Российской Федерации».

Волонтеры Республики Дагестан посетили детский приют Министерства труда и социального развития РД, расположенный в Махачкале.

В Дагестанском государственном университете прошел финал Дагестанской лиги Клуба веселых и находчивых.

Сотрудники Министерства по делам молодежи Республики Дагестан прошли стажировку в городе Москве.

ЛИД (лидер-абзац)

- Лид – это концентрированное выражение всей новости.
- Минимум лид должен отвечать на вопросы: **Когда? Где? Что? (Кто?)** (Очередность ответов при этом не имеет большого значения).
- Идеальный лид – 140-160 символов (или три-четыре строки 12 px).
- Простой язык, отсутствие бюрократизмов.
- В идеале читатель должен понять суть новости из лида.

Примеры:

Хорошо:

3 февраля в Министерстве по делам молодежи Дагестана прошла встреча волонтерских организаций и объединений республики.

На базе Республиканского молодежного центра Министерства по делам молодежи РД будут организованы студенческие стройотряды. Об этом 10 января сообщил руководитель ведомства на встрече с активами вузов Дагестана.

Запрещено использовать в лиде:

Как известно…

Мир не без добрых людей…

В погожий летний день… и подобное.

«ТЕЛО» ТЕКСТА (основное содержание)

- В основной части текста излагается, раскрывается подробно и с деталями то, о чем было сказано в заголовке и лиде.
- «Тело» текста должно быть логически выстроено. У него должно быть начало, середина и финал.
- В этой части текста читателю необходимо рассказать (в зависимости от события!) о том:
  - кто организатор;
  - кто присутствовал на мероприятии;
  - максимально полно рассказать о том, что происходило;
  - кто выступал;
  - к каким решениям, выводам, итогам пришли и т.д.
- При этом нет необходимости перечислять поименно всех гостей или участников. Достаточно указать самых главных, а остальных обозначить в виде групп: «общественные деятели», «сотрудники министерства», «студенты», «представители администрации города» и т.д.

- Нет необходимости также приводить всех выступивших – лучше ограничиться лишь основными спикерами.
- Описывая мероприятия, на которых есть выступления гостей, докладчиков и т.д., рекомендуется включать в текст несколько небольших цитат. При этом необходимо соблюдать баланс прямой и косвенной речи.
- При описании спортивных мероприятий, викторин, конкурсов и т.п. обязательным условием является указание имен победителей и призеров.
- Тональность освещения события, мероприятия со стороны автора текста должна быть нейтральной.
- Автору новостного материала запрещаются оценочные суждения, выводы, мнения и т.д. (как положительные, так и отрицательные). При этом всё это допустимо со стороны участников мероприятия в своей речи, и автору необходимо указывать их принадлежность.

ЦИТАТЫ ***(не всегда обязательный элемент текста)***

- Приводя цитаты, важно не забывать главный принцип: «Не навреди!».
- Далеко не все владеют русским языком на должном уровне, а некоторые докладчики отходят от темы (т.н. «лирические отступления»). Поэтому автор материала имеет право при написании текста исправлять допущенные выступающими ошибки, пропускать отступления от темы выступающих, сокращать сказанное, но при этом не менять смысл сказанного.
- В самых сложных ситуациях необходимо своими словами передать основной смысл сказанного, а не приводить неудачную цитату.
- Цитата не должна быть перегружена большим количеством предложений.
- Цитаты должны быть правильно оформлены с точки зрения правил пунктуации русского языка.

БЭКГРАУНД ***(желательный, но не обязательный элемент текста)***

- Бэкграунд включает расширяющую, детализирующую или дополняющую информацию о факте, событии, мероприятии, описанном в тексте. Дает предысторию вопроса или справочную информацию.
- Бэкграунд может быть первичным, то есть таким, который содержит информацию, необходимую для понимания сути новости. Такой бэкграунд должен располагаться в лиде или сразу после него.
- Бэкграунд может быть и вторичным (чаще всего). Вторичный бэкграунд дополняет материал, дает справочную и/или дополнительную информацию к описанному событию, факту, дополняет новость предысторией. Располагается в середине или в конце материала – в наиболее подходящей части текста.
- В роли бэкграунда можно также использовать комментарии, впечатления организаторов, участников, гостей мероприятия и т.д.
- Включать или нет бэкграунд в текст, зависит от характера информационного повода, имеющейся в наличии дополнительной информации, истории вопроса и т.д.

12. ГЛОССАРИЙ

Основные термины и определения правовых понятий в области информационных отношений и защиты информации

Основные термины и определения правовых понятий в изучаемой области установлены в Федеральном законе «Об информации, информационных технологиях и о защите информации».

Информация – сведения (сообщения, данные) независимо от формы их представления.

Информационные технологии – процессы, методы поиска, сбора, хранения, обработки, предоставления, распространения информации и способы осуществления таких процессов и методов.

Информационная система – комплекс, включающий вычислительное (компьютеры, серверы, микрокомпьютеры) и коммуникационное оборудование (точки доступа WiFi, маршрутизаторы, концентраторы, кабели), программное обеспечение (операционные системы, приложения для различных задач) и информационные ресурсы, а также системный персонал, обеспечивающий поддержку динамической информационной модели некоторой части реального мира для удовлетворения информационных потребностей пользователей.

Информационно-телекоммуникационная сеть – технологическая система, предназначенная для передачи по линиям связи информации, доступ к которой осуществляется с использованием средств вычислительной техники. **Обладатель информации** – лицо, самостоятельно создавшее информацию либо получившее на основании закона или договора право разрешать или ограничивать доступ к информации, определяемой по каким-либо признакам.

Также к правовым понятиям следует отнести понятие прав доступа к защищаемой информации. Ограничения доступа устанавливаются к сведениям, составляющим государственную тайну и иные виды тайны. В качестве собственников информации рассматриваются государство, организации и граждане (юридические и физические лица).

Доступ к информации – возможность получения информации и ее использования.

Предоставление информации – действия, направленные на получение информации определенным кругом лиц или передачу информации определенному кругу лиц.

Распространение информации – действия, направленные на получение информации неопределенным кругом лиц или передачу информации неопределенному кругу лиц. **Защищаемая информация** – информация, являющаяся предметом собственности и подлежащая защите в соответствии с требованиями правовых документов или требованиями, устанавливаемыми собственником информации.

Собственником информации может быть: государство, юридическое лицо, группа физических лиц, отдельное физическое лицо.

Защита информации – принятие правовых, организационных и технических мер, направленных на:

1) обеспечение защиты информации от неправомерного доступа, уничтожения, модифицирования, блокирования, копирования, предоставления, распространения, а также от иных неправомерных действий в отношении такой информации;

2) соблюдение конфиденциальности информации ограниченного доступа;

3) реализацию права на доступ к информации.

Защита информации от утечки – деятельность, направленная на предотвращение неконтролируемого распространения защищаемой информации в результате ее разглашения, несанкционированного доступа к информации и получения защищаемой информации разведками.

Защита информации от несанкционированного воздействия – деятельность по предотвращению воздействия на защищаемую информацию с нарушением установленных прав и (или) правил на изменение информации, приводящего к ее искажению, уничтожению, блокированию доступа к информации, а также к утрате, уничтожению или сбою функционирования носителя информации.

Защита информации от непреднамеренного воздействия – деятельность, направленная на предотвращение воздействия на защищаемую информацию ошибок ее пользователя, сбоя технических и программных средств информационных систем, природных явлений или иных нецеленаправленных на изменение информации мероприятий, приводящих к искажению, уничтожению, копированию, блокированию доступа к информации, а также к утрате, уничтожению или сбою функционирования носителя информации.

Защита информации от разглашения – деятельность, направленная на предотвращение несанкционированного доведения защищаемой информации до потребителей, не имеющих права доступа к этой информации.

Защита информации от несанкционированного доступа – деятельность, направленная на предотвращение получения защищаемой информации заинтересованным субъектом с нарушением установленных правовыми документами или собственником, владельцем информации прав или правил доступа к защищаемой информации.

Заинтересованным субъектом, осуществляющим несанкционированный доступ к защищаемой информации, может быть: государство; юридическое лицо; группа физических лиц, в т ом числе общественная организация; отдельное физическое лицо.

Защита информации от разведки – деятельность, направленная на предотвращение получения защищаемой информации разведкой.

Примечание. Получение защищаемой информации может быть осуществлено как иностранной, так и отечественной разведкой.

Защита информации от технической разведки – деятельность, направленная на предотвращение получения защищаемой информации разведкой с помощью технических средств.

Защита информации от агентурной разведки – деятельность, направленная на предотвращение получения защищаемой информации агентурной разведкой.

Цель защиты информации – заранее намеченный результат защиты информации. Целью защиты информации может быть предотвращение ущерба собственнику, владельцу, пользователю информации в результате возможной утечки информации (или) несанкционированного и непреднамеренного воздействия на информацию.

Замысел защиты информации – основная идея, раскрывающая состав, содержание, взаимосвязь и последовательность осуществления технических и организационных мероприятий, необходимых для достижения цели защиты информации.

Эффективность защиты информации – степень соответствия результатов защиты информации поставленной цели.

Показатель эффективности защиты информации – мера или характеристика для оценки эффективности защиты информации.

Нормы эффективности защиты информации – значения показателей эффективности защиты информации, установленные нормативными документами.

Организация защиты информации – содержание и порядок действий, направленных на обеспечение защиты информации.

Система защиты информации – совокупность органов и (или) исполнителей, используемой ими техники защиты информации, а также объектов защиты, организованная и функционирующая по правилам, установленным соответствующими правовыми, организационно-распорядительными и нормативными документами в области защиты информации. **Мероприятие по защите информации** – совокупность действий, направленных на разработку и (или) практическое применение способов и средств защиты информации.

Мероприятие по контролю эффективности защиты информации – совокупность действий, направленных на разработку (или) практическое применение способов и средств контроля эффективности защиты информации.

Техника защиты информации – средства защиты информации, средства контроля эффективности защиты информации, средства и системы управления, предназначенные для обеспечения защиты информации.

Объект защиты информации – информация или носитель информации, или информационный процесс, которые необходимо защищать в соответствии с поставленной целью защиты информации.

Способ защиты информации – порядок и правила применения определенных принципов и средств защиты информации.

Категорирование защищаемой информации (объекта защиты) – установление градации важности защищаемой информации (объекта защиты).

Контроль состояния защиты информации – проверка соответствия организации и эффективности защиты информации установленным требованиям и (или) нормам зашиты информации.