



МедиаТренды

Экспертный взгляд факультета журналистики МГУ имени М. В. Ломоносова на события в СМИ

Содержание:

- Колонка редактора**1
Механизмы соблюдения этических норм, норм информационной безопасности и механизмы свободы слова прекрасно сосуществуют друг с другом, если вспомнить концепцию социальной ответственности в СМИ
- Интервью**2
Заместитель директора ИГИБ МГУ Алексей Сальников о правильных методах борьбы с неправильным контентом в Интернете
- Индикаторы**3
Типы угроз информационной безопасности в Интернете, виды DDoS-атак, финансирование федеральных программ в сфере информационных технологий и другие любопытные факты об информационной безопасности
- Тема номера**4
Информационная безопасность. Взгляд экспертов (Валерий Яценко, Владимир Соколов, Андрей Кульпин)
- Масс-медиа: теория и практика**6
Ведущий научный сотрудник ИГИБ МГУ Олег Казарин о «цифровой дипломатии» в действии
- МедиаКалендарь**6
Новый журнальный проект ИД «Hearst Shkulev Media/ИнтерМедиаГруп» – *Psychologies Luxe*; награды ABC за «Лучшие тиражи»; выход сына медиамагната Руперта Мердока – Джеймса – из советов директоров двух британских издательств; *Emirates* стремится увеличить присутствие в социальных медиа; закрытие новостной сайта об Интернете «Вебпланета»; прием работ на Пулитцеровскую премию в электронном виде; новое кадровое назначение в «Системе Масс-медиа»
- ЖЖ: жизнь журфака**7
Можно ли обеспечить информационную безопасность?
- Книжные новинки**8
Проблемы безопасности и противодействия терроризму; *Media and Terrorism Global Perspectives* by Daya K. Thussu & Des Freedman; Информационная безопасность и защита информации В. П. Мельникова, С. А. Клейменова и А. М. Петракова
- Медиатекст**8
Доцент кафедры стилистики русского языка Елена Кара-Мурза о лингвистической безопасности для всех участников масс-медиа

КОЛОНКА РЕДАКТОРА



Механизмы соблюдения этических норм, норм информационной безопасности и механизмы свободы слова прекрасно сосуществуют друг с другом, если вспомнить концепцию социальной ответственности в СМИ.

склонялись к защите информации и прав всех тех, кто в Сети существует. Встает вопрос: допустимо ли контролировать Интернет в условиях свободы слова, которые действуют в современных медиасистемах? Представляется, здесь нет противоречия. Механизмы соблюдения этических норм, норм информационной безопасности и механизмы свободы слова прекрасно сосуществуют друг с другом, если вспомнить концепцию социальной ответственности в СМИ.

Журналист должен принимать во внимание те эффекты, которые производят его сообщения. Именно поэтому сегодня пользователи Интернета, которые берут на себя отчасти журналистские функции, должны тоже соблюдать подобные требования. Все чаще встает вопрос о воспитании аудитории, о формировании у активных пользователей Интернета некоторых профессиональных навыков. Блогеры, модераторы, лидеры сообществ, имеющие дневники в Интернете, должны понимать, что их деятельность похожа на журналистскую, и как журналисты они обязаны отвечать не только перед законом, но и перед корпоративным сообществом, аудиторией и пользователями.

Елена Вартанова

Тема номера:

**ИНФОРМАЦИОННАЯ
БЕЗОПАСНОСТЬ**



«Единственный способ борьбы с неправильным контентом – заполнение Интернета правильным контентом». (А. Солдатов)

Понятие «вредоносная информация» в разных странах – разное. Есть консенсус по 2-3 позициям – терроризм, детская порнография, экстремизм. Остальное трактуется по-разному.

Алексей Сальников, заместитель директора Института проблем информационной безопасности (ИПИБ) МГУ

Это бизнес

Как бороться с вредоносным контентом: детской порнографией, экстремистскими сообщениями?

Прежде, чем отвечать, надо объяснить, что такое вредоносная информация. Понятие «вредоносная информация» в разных странах – разное. Есть консенсус по 2-3 позициям – терроризм, детская порнография, экстремизм. Остальное трактуется по-разному. По стандартам ООН – детская порнография и терроризм. Все единогласно заявляют: да, это плохо, давайте бороться, обратимся к юристам. Подключаются юристы, и все возвращается на круги своя. Хотя совершенно очевидно, что такие материалы надо запрещать. Каждая страна принимает те меры, какие считает возможными. Есть жесткие меры. Это вариант Китая и Белоруссии, где все «рубится» и запрещается. Есть полужесткие меры, как в США. В России существует Управление «К» МВД, которое все время рапортует, что ищет и пресекает порносайты.

Кого следует наказывать?

Еще один бесконечный вопрос – кто будет отвечать: владелец хостинга, тот, кто готовит контент, либо тот, кто потребляет? Должен ли провайдер отвечать за содержание тех сайтов, которые на нем «хостятся». Например, я хозяин data-центра, у меня арендуют про-

странство и машины. Должен ли я проверять, не распространяют ли они преступную информацию?

Самый правильный путь – закрывать доступ к ресурсу. Ярчайшая история на эту тему – жизнедеятельность сайта www.kavkazcenter.com. Сколько лет его пытаются «убрать»! «Рубят» в одном месте, он появляется в другом. Но это бизнес. Тот, кто финансирует такие сайты, в критический момент переводит их в другие страны и открывает заново. Есть еще понятие «тихая гавань». Это страны, как правило, африканские, где никак не борются с подобными явлениями. Мировое интернет-сообщество пока не решило, как поступать с «тихими гаванями».

Жизнь в социальных сетях: что нужно знать?

Хорошая аналогия определения социальных сетей: когда девушка приходит в бар к пьяным ирландцам и начинает рассказывать про свою жизнь. Если не боишься, пожалуйста. Не надо забывать, что информация, которую вы выкладываете для узкого круга, оказывается доступной для всех. Интернет – новая реальность. Постепенно уже приходит понимание, что, выкладывая про себя слишком много персональных данных, пользователь ставит под угрозу свою безопасность. Среди пользовате-

лей Интернета пока мало блогеров, журналистов, специалистов по безопасности, которые смогли бы доступно это объяснять.

Кто такие «хактивисты»?

«Хактивисты» – политически активные хакеры. Мотивированные либо деньгами, либо идейными побуждениями. Конечно, сленг, но в профильных кругах понятие активно применяется. Например, в Эстонии политически активные российские хакеры обрушили сайты с идейно неблизкой информацией. Их обвиняли в причастности к российским спецслужбам, но не доказали.

Как можно контролировать информацию в Интернете?

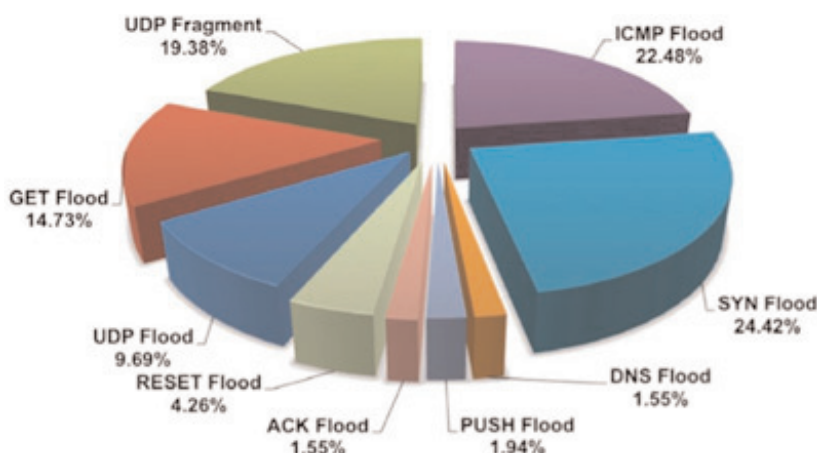
Вокруг этого часто начинаются политические спекуляции под эгидой «свободы слова и прав человека». Если посмотреть шире, то сейчас эти меры поднимаются на щит как борьба с инакомыслием, демократией. Хотя это далеко не так. По российскому законодательству цензура запрещена. В любом случае, вводить цензуру в Интернете значительно сложнее, чем в традиционных СМИ. По этому поводу можно процитировать Алексея Солдатова: «Единственный способ борьбы с неправильным контентом – заполнение Интернета правильным контентом».

Типы угроз информационной безопасности в Интернете

№	Тип угрозы	Изменение
1	вредоносное ПО	без изменений
2	кибератаки	без изменений
3	уязвимости	без изменений
4	хакеры	возросла
5	трояны	уменьшилась
6	взлом	без изменений
7	мошенничество	без изменений
8	утечки	без изменений
9	фишинг	возросла
10	DDoS	возросла

Источник: Itsec.ru, 2011

Виды DDoS-атак



Как заявила компания *Prolexic Technologies*, количество передаваемых за 1 секунду пакетов (*PPS*) увеличилось в четыре раза. Мы наблюдаем значительный рост всевозможных *DDoS*-атак в последние 12 месяцев.

Из общего числа атак приблизительно 24% составляют атаки *SYN Flood*, 22% – *ICMP Flood* и 19% – *UDP Flood*, что означает изменение в тактике атак.

Распространенность *SYN Flood* и увеличение *PPS* говорит об изменении в стратегии – атаки стали менее сложными, но чрезвычайно опасными.

Источник: Хакер.ru, 2010

Финансирование федеральных программ в сфере информационных технологий в 2009–2011 гг.

Показатель	Годы		
	2009	2010	2011
Количество крупных проектов	807	781	809
Финансирование крупных проектов, млрд долл.	37,25	40,33	40,4
Все расходы на ИКТ	71,23	78,44	79,38

Источник: ИПИБ МГУ, 2011

Факты

- В Германии только что завершилась учебная кибервойна *Luekex 2011*. Компьютеры федеральных и региональных госслужб в течение двух суток, 30 ноября – 1 декабря, подверглись симулированным хакерским атакам. К *Luekex 2011* власти готовились почти два года. Обработка результатов продлится еще четыре месяца. Следующие учения пройдут в 2013 г.
- «Лаборатория Касперского» опубликовала обзор информационных угроз в третьем квартале 2011 года. Аналитики отмечают, что в этот период количество кибератак на крупнейшие корпорации мира продолжило расти. Некоторым компаниям пришлось даже выйти из бизнеса вследствие действий хакеров.
- Сотрудники Управления «К» МВД России задержали хакера, похитившего около 10 млн рублей из платежных терминалов. Подозреваемый создал «троянца», который собирал и передавал данные с зараженных компьютеров. Среди них были коды доступа и управления электронными кошельками и работой платежных терминалов. Хакер часто менял место жительства, жил по поддельным паспортам и даже сделал пластическую операцию.
- Социальная сеть *Facebook* договорилась с Федеральной Комиссией по торговле США (*FTC*) об урегулировании претензий, касающихся приватности пользовательских данных.
- Компания *McDonald's* столкнулась сразу с несколькими случаями кражи финансовых данных клиентов ресторана своими сотрудниками. Сотрудники продавали украденные данные незаконным иммигрантам, которые также работали в ресторанах *McDonald's*.
- В Мексике учитель и радиоведущий распространяли в *Twitter* ложную информацию о том, что вооруженные преступники атаковали школу и захватили детей. Эти сообщения вызвали серьезную панику у родителей, что спровоцировало десятки автомобильных катастроф и перегруженность линий экстренного вызова.
- DEF CON* – крупнейшая в мире ежегодная конференция хакеров в Лас-Вегасе. Первый *DEF CON* прошел в июне 1993 г. Сейчас число участников приближается к 10 000 чел.

ИНФОРМАЦИОННАЯ БЕЗОПАСНОСТЬ



Валерий Яценко



Владимир Соколов



Андрей Кульпин

Валерий Яценко, заместитель директора Института проблем информационной безопасности (ИПИБ) МГУ, кандидат физико-математических наук

Разделение понятий

С развитием информационно-коммуникационных технологий, глобальных информационных сетей растет зависимость национальной безопасности от ситуации в киберпространстве. При этом сейчас уже ясно, что ни одно государство не может в одиночку обеспечить безопасность киберпространства. Поэтому данный вопрос включается в повестку самых различных межгосударственных, региональных и международных встреч и переговоров. И всякий раз возникает вопрос о базовых понятиях и терминах, в которые стороны часто вкладывают разный смысл.

По определению А. А. Стрельцова, информация – сведения (сообщения, данные), независимо от формы их представления. Важно подчеркнуть, что при таком подходе понятие «информация» не разделяется на содержание (сообщение, данные) и форму его представления. Вторая составляющая термина «информа-

ционная безопасность» – это понятие «безопасность». В России оно определяется как «состояние защищенности жизненно важных интересов личности, общества и государства от внешних и внутренних угроз».

На основе двух понятий – «информация» и «безопасность» – появилось определение «информационной безопасности»: «состояние защищенности личности, общества и государства и их интересов от угроз, деструктивных и иных негативных воздействий в информационном пространстве».

Несмотря на часто синонимичное использование в различных сочетаниях понятий слов «информационный» и «кибер-» (например, термины «информационное пространство» и «киберпространство»), существует значительное отличие обозначаемых этими терминами понятий. Как правило, термин «кибер» включает в себя только одну (четвертую) угрозу, упо-

мянутую в Доктрине информационной безопасности России, – угрозу безопасности информационно-коммуникационных средств и систем. Кибербезопасность определяется как свойство (киберпространства, киберсистемы) противостоять, намеренным и/или ненамеренным угрозам, а также реагировать на них и восстанавливаться после воздействия этих угроз. Термин «информационная безопасность» можно разделить в соответствии с видами угроз: – три из них будут составлять информационно-социальную безопасность, а четвертая – информационно-техническую безопасность. В этом случае ее содержание совпадет с содержанием термина «кибербезопасность». Так, например, противодействие распространению идеологии терроризма через Интернет не входит в угрозы технического характера, но входит в понятие информационной безопасности.

Владимир Соколов, заместитель директора Института проблем информационной безопасности (ИПИБ) МГУ, кандидат экономических наук

Интернет де-факто – мировое достояние

Что такое Интернет? Несколько компьютеров, соединенных между собой проводами.

Если я пишу кому-то письмо, сервер должен это передать. То есть выстраивается алгоритм рассылки сообщения. Я в адресной строке сообщаю адрес того сервера, куда посылаю файл. Например, я пишу *yandex.ru*, слово *yandex* переводится в цифры, которые «говорят» компьютеру, что это должно прийти на такой-то сервер. Все адресное пространство замыкается на корневом сервере, который знает куда, что и как посылать.

Естественно, что все 13 корневых серверов находятся на территории США как родоначальника Интернета. Сейчас уже нельзя говорить, что Интернет принадлежит Штатам. Интернет де-факто – мировое достояние. Корневыми серверами управляет *ICANN* – международная ассоциация, регулирую-

щая присвоение *IP*-адресов и доменных имен. Изначально это было подразделение департамента торговли США. Позже в Совет директоров вошли представители и других стран. Но вопрос влияния США на ситуацию остается актуален.

Зеркала корневых серверов размещаются в разных странах. В России такое зеркало расположено в Новосибирске. Интернет создавался не как сеть для всеобщего пользования, а для того, чтобы обеспечить прохождение команд на запуск ответных ракет в разные военные объекты в случае ядерной войны с СССР.

Российский трафик проходит через Норвегию. Но нельзя говорить, что норвежцы, если захотят, отключат нас от Интернета. Такие решения, принимает интернет-сообщество, а не отдельно взятая страна. В случае неполадок на этой линии трафик пой-

дет через Швецию, Японию или какую-то еще страну. Суть Интернета в том, чтобы информация проходила. Информация выбирает тот канал, который быстрее ее проводит.

Наиболее интернет-зависимая страна – США. Сети их минобороны разбросаны по всему миру. Поэтому в случае отключения от Интернета кого-то из игроков, они пострадают первыми.

Есть ярко выраженный китайский опыт. Это самодостаточное государство в киберпространстве. Сколько производят, столько и потребляют. Наружный трафик в Китае – минимальный. Конечно, с учетом масштабов Китая, он тоже внушительный, но относительно внутренних ресурсов – небольшой. Китайцы сделали свои аналоги поисковиков, социальных сетей, торрентов. Они живут своей жизнью, а мы остаемся зависимыми от внешних поставщиков услуг.

Андрей Кульпин, советник директора Института проблем информационной безопасности (ИПИБ) МГУ по международным связям

Кто виноват и что делать?

С 2001 г. взаимоотношения сторон в киберпространстве регулирует Будапештская конвенция по борьбе с киберпреступлениями. Она подписана 47 странами, но ратифицирована только 31. США ратифицировали ее два года назад, но с оговорками. Россия изначально подписала документ, но вскоре отозвала подпись.

Вся проблема в пункте «b» статьи 32: «Сторона может без согласия другой стороны получать через компьютерную систему на своей территории доступ к хранящимся на территории другой стороны компьютерным данным или получить их, если эта сторона имеет законное и добровольное согласие лица, которое имеет законные полномочия раскрывать эти данные этой стороне через такую компьютерную систему». А это нарушение суверенитета. Фактически все киберпреступления сейчас интернациональны. Они проводятся в различных

юрисдикциях. В одной стране – хакер, в другой – заказчик, в третьей – банкир. Как эти преступления расследовать и как судить виновных?

Например, хакер из Новосибирска взломал базы американского «Ситибанка». Согласно Конвенции, ФБР может в российских информационных сетях снять ту информацию, которая поможет расследовать преступление. Российская позиция такова: во-первых, это нарушение государственного суверенитета, во-вторых, эти проблемы решаются на уровне взаимодействия правоохранительных органов обеих сторон, но по обращению. ФБР обращается к МВД. МВД проводит расследование. Почему? Потому что расследование ведется в рамках процессуального кодекса. Все должно быть задокументировано. А если расследование проводят представители ФБР, неправомочные здесь вести розыскные и следственные работы, то о каком

юридически значимом действии идет речь? Прямое нарушение закона.

В Конвенции указано, что криминальными деяниями являются все преступления с использованием информационных технологий. Это касается, в том числе, и кражи денег.

Будапештская конвенция устарела. Сейчас российские специалисты подготовили предложения по изменению подхода к регулированию отношений в киберпространстве. Спектр проблем, рассматриваемых в документе, гораздо шире. Россия считает, что в информационном пространстве, помимо киберпреступлений, достаточно нерешенных вопросов. Например, ведение информационных войн. Это Будапештской конвенцией не покрывается. А также использование компьютерных технологий, Интернета в террористических целях. Новый документ защищает всех участников вопроса. Но он пока в стадии обсуждения.

МАСС-МЕДИА: ТЕОРИЯ И ПРАКТИКА

Олег Казарин, ведущий научный сотрудник Института проблем информационной безопасности (ИПИБ) МГУ, кандидат технических наук



«Цифровая дипломатия» в действии

В событиях, происходящих в арабских странах в этом году, обвиняют социальные сети. Дескать, благодаря *Twitter* и *Facebook* прокатилась волна революций, восстаний и прочих беспорядков на арабском востоке. Можно ли к этому относиться всерьез? Да, можно. Два года назад Хиллари Клинтон официально объявила о переходе

на «цифровую дипломатию». Лозунг этого направления – «Использование информационно-конвекционных технологий для продвижения идеалов демократии». Этот метод официально взят на вооружение Государственным департаментом США. На сайте Госдепа эта концепция находится в открытом доступе. Все методы и технологии доступны для изучения. Цели каждая страна может декларировать свои. Хочешь демократию, хочешь фундаментализм – можешь продвигать. Правда, движение это волнообразное. Типичный пример – погромы в Англии в 2011 г. В этих событиях внешнеполитические ведомства не участвовали. Соединенные Штаты серьезно развивают данное направление: в посольствах тех странах, которые им интересны, они вводят структуру, которая в случае необходимости начнет раскачивать ситуацию. В конце октября в МГИМО читал лекцию Алек Росс, старший советник Хиллари Клинтон по инновациям.

Он четко изложил взгляд Госдепа на эти вопросы.

И второй момент: после арабских революций наши друзья по ОДКБ – Казахстан, Таджикистан и Узбекистан – периодически обращаются к России с просьбой закрыть сайты, которые в их странах выступают площадками для борьбы с их режимами. На это мы им говорим, что мы – демократы и можем закрыть сайт только по постановлению суда. Дайте нам постановление вашего суда, что такой-то сайт признан вредным, мы пошлем эти материалы в российский суд. И если российский суд примет такое же решение, сайт можно будет закрыть. Но при этом мы не гарантируем, что он не откроется где-нибудь в другом месте. Не удивительно, что главной темой саммита ОДКБ в августе была борьба с «цифровой дипломатией» в рамках их государственных границ. Обсуждали возможности ее предотвращения и борьбы с ней.

МедиаКалендарь

1 декабря, в продажу поступил новый журнальный проект ИД «*Hearst Shkulev Media/ИнтерМедиаГруп*» – *Psychologies Luxe*. К проекту будут привлечены не только журналисты, но и люди, не имеющие к журналистике никакого отношения. Как отметила главный редактор ИД Ольга Косырева, в проекте будут участвовать только русские герои, возможно, «не всегда известные, но всегда интересные», что станет одной из главных его особенностей. Той же самой позиции придерживаются и во французской версии журнала, которая выпускается с 2007 г.: его героями становятся только французы.

Источник: Планета СМИ

Бюро тиражного аудита *ABC* наградило сертифицированные издания призами и дипломами за «Лучшие тиражи 2011 г.». Награды *ABC* были вручены по 18 номинациям для ежедневных газет, еженедельных газет и журналов, ежемесячных журналов с учетом позиционирования изданий по катего-

риям. Еженедельник «Аргументы и факты» получил награду в номинации «Еженедельная газета общего интереса, лучший проданный тираж в Российской Федерации». ИД «Провинция» получил приз и диплом Бюро тиражного аудита *ABC* за лучший тираж 2011 г. в номинации «Сеть еженедельных региональных газет».

Источник: Аргументы и факты, ИД «Провинция»

Джеймс Мердок, сын медиамагната Руперта Мердока, вышел из советов директоров двух британских издательств, выпускающих газеты «*The Sun*», «*The Times*» и «*The Sunday Times*». Обе компании являются частью издательского дома *News International*, контролируемого медиакорпорацией Руперта Мердока *News Corp*. При этом Джеймс Мердок сохраняет за собой пост председателя совета директоров самого *News International*.

Источник: Lenta.ru

Одна из крупнейших мировых авиакомпаний *Emirates*, объя-

вила, что намерена изменить «нехватку своего присутствия в социальных медиа» и в качестве первого шага запустить страницу в *Facebook*. Увеличение активности в социальных медиа является частью более широкой бизнес-стратегии *Emirates*, в рамках которой она стремится в течение пяти лет увеличить свой размер в 2 раза и стать крупнейшей независимой авиакомпанией в мире.

Источник: Sovetnik.ru

Новостной сайт об интернет-технологиях «Вебпланета» прекратил работу. Об этом на страничке издания «ВКонтакте» сообщила его бывший редактор Злата Николаева. Последним рабочим днем у коллектива «Вебпланеты» стало 17 ноября; этим же числом датированы последние обновления. 5 декабря сайту исполнилось бы 10 лет.

Источник: Lenta.ru

С декабря 2011 года прием работ на Пулитцеровскую премию осуществляется только в электронном виде. Прием работ на бумаге пол-

ностью прекращен. Таким образом, оргкомитет положил конец традиции, существовавшей со дня основания Пулитцеровской премии, когда материалы сдавались в виде альбомов с вырезками статей из газет и журналов. Кроме того, название номинации «За экстренный выпуск новостей» (*Local Reporting of Breaking News*) была изменена, и теперь премия будет вручаться за лучшее освещение событий в реальном времени.

Источник: Lenta.ru

Американский бизнесмен Питер Герви, основавший телеканал СТС и радио *Maxim*, стал президентом «Системы Масс-медиа» (СММ), которая объединяет медийные активы АФК «Система». Предшественник Герви Андрей Смирнов стал председателем совета директоров. От нового президента в компании ждут «международного развития» и привлечения «перспективных» сделок по слиянию и поглощению.

Источник: Lenta.ru

ЖЖЖ



МОЖНО ЛИ ОБЕСПЕЧИТЬ ИНФОРМАЦИОННУЮ БЕЗОПАСНОСТЬ?

Рамзаева Мария

Информационная безопасность как нераспространение и/или запрещение вредного контента – в первую очередь, вопрос культуры общества, этики. Если есть детская порнография или призывы к экстремизму, значит есть аудитория, для которой это предназначается. Полностью убрать подобную информацию невозможно, но можно ограничить. Некоторое время назад проблема распространения порнографии стояла в таких социальных сетях, как Одноклассники и ВКонтакте, но она частично решилась с помощью пользовательской модерации, когда сами пользователи могли пожаловаться модераторам сайта на файлы, которые они считают недопустимыми для широкого круга.

Баев Антон

Чтобы побороть такой опасный контент, надо прежде всего ужесточить уголовное и административное законодательство в СМИ, привлечь активных медийных персон для разъяснения проблемы, а также развивать каналы коммуникации, расширять кругозор среднего пользователя, нацеливая его на производство собственной полезной информации.

Китаева Ирина

За проникновение вредоносного контента в Сеть следует брать штрафы с тех, кто занимается его распространением. В социальных сетях можно установить блок на ту информацию, которую администратор посчитал опасной.

Наумов Сергей

Для того, чтобы информационная безопасность была на высоком уровне, должны существовать запреты или хотя бы ограничения на распростране-

ние вредного контента. Такой контент популярен до тех пор, пока он способен заинтересовать общество, и бороться с ним надо теми средствами, которые интересуют это общество в большей степени.

Харитоновна Елена

Информационная безопасность достигается в процессе борьбы с непроверенными, неистинными источниками информации, которые содержат аморальный или ложный контент. Такая борьба – долгий и трудный путь, на прохождение которого может понадобиться не одно десятилетие. Необходимо воспитывать культуру интернет-пользования.

Куликова Ия

Информационная безопасность – защита людей от плохой, нежелательной информации, которая идет вразрез с моральными принципами народов, религий. Надо ограничивать такие потоки. Существуют программы как предупреждающие о содержимом какого-либо интернет-источника, так и отключающие вредные баннеры, ненужную рекламу.

Бартенева Анастасия

Следует ввести возрастную цензуру на получение определенной информации. Но в силу того, что вредная информация идет через Интернет, такие меры становятся фиктивными. Информация не должна наносить вред. Можно бороться с такой информацией, но нельзя ее пресечь, пока этого не захотят те люди, которые ее получают, пока аудитория не откажется принимать это.

Магакян Карина

В идеале информационная безопасность должна обеспечиваться всегда,

но на практике это не так. За распространение вредоносного контента нужно штрафовать, привлекать к уголовной ответственности. Наказание должны понести и те, кто потребляет подобную информацию. Необходимо более пристально проверять людей, которые регистрируются на сайтах. Открытый доступ к ресурсам облегчает размножение ненужной информации.

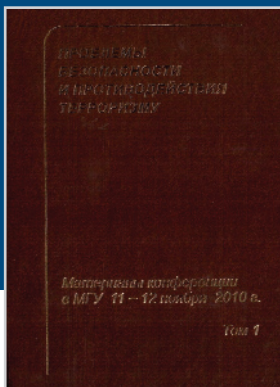
Толмачева Алина

Безопасная информация – та информация, которая будет адекватно расшифрована человеческим сознанием. Опасную информацию можно позиционировать как развращающую человеческое сознание. Бороться с таким контентом крайне тяжело. Если человек ищет его целенаправленно, то он все необходимое для себя найдет. Необходимо минимизировать попадание такой информации в массы. Также нужно «заражать» вирусными ресурсами с такой информацией, чтобы люди не заходили по сомнительным ссылкам.

Аргышева Виктория

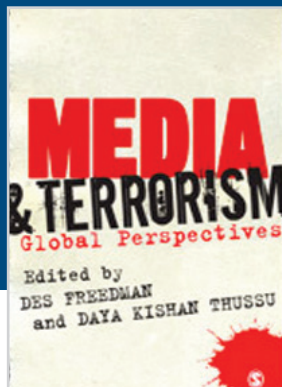
На мой взгляд, невозможно выискивать на всех сайтах запретную информацию. На видеопорталах существует кнопка «Пожаловаться». Не думаю, что человек будет жаловаться на то, что он специально искал. Наверное, нужно усложнить систему регистрации для того, чтобы выкладывать и просматривать сомнительную информацию. Существуют же определенные фильтры для детей. Но все сайты не просмотреть, а полностью надеяться на машину нет смысла. Вот и получается, что основной информационный защитник – совесть. Но она, увы, включается не всегда.

КНИЖНЫЕ НОВИНКИ



Проблемы безопасности и противодействия терроризму (М., 2011)

В сборнике собраны материалы Шестой Международной научной конференции по проблемам безопасности и противодействия терроризму, проходившей в МГУ имени М. В. Ломоносова 11-12 ноября 2010 г., а также материалы Девятой Общероссийской научной конференции «Математика и безопасность информационных технологий». Книга издана в двух томах.



Media and Terrorism Global Perspectives edited by Daya K. Thussu & Des Freedman (London, 2011)

В книге авторы анализируют, как терроризм и борьба с террором представлены в глобальных СМИ.

В издании собраны работы ведущих ученых, которые пытаются ответить на эти вопросы. Книга представляет интерес для студентов и исследователей в области медиа, коммуникации, политики и международных отношений.



Информационная безопасность и защита информации В. П. Мельников, С. А. Клейменов, А. М. Петраков (М., 2011)

В книге представлены основные положения, определения информационной безопасности общества, его различных структурных образований, организационно-правового, технического, методического, программно-аппаратного сопровождения. Особое внимание уделено проблемам методологического обеспечения деятельности самого общества и конкретных фирм и систем, функционирующих в нем.

МЕДИАТЕКСТ

Елена Кара-Мурза, доцент кафедры стилистики русского языка



Лингвистическая безопасность – для всех участников масс-медиа

На нашем факультете недавно прошел круглый стол «Роль СМИ в про-

филактике терроризма». Но СМИ способны играть не только позитивную роль – они сами могут стать источником терроризма и экстремизма. Человеческая речь обладает огромной воздействующей силой, и, к сожалению, беллетристика, журналистика, в том числе сетевые ресурсы, способны провоцировать людей на убийственные действия, возбуждать рознь из-за цвета кожи, культуры или вероисповедания. В связи с этим опасная информационно-коммуникативная деятельность радикальных сообществ находится под наблюдением структур безопасности и правопорядка. В то же время речевое воздействие вероятно: интерпретация текста адреса-

том носит субъективный характер, а его реакция не обязательно будет той, которую запланировал автор. Стихийно пользуясь репертуаром жанров, люди различают истинные намерения авторов и распространителей, они чувствуют иронию и пародию. А «силовики» плохо воспринимают языковую игру, усматривая в крепком слове, в шутке над начальством или в его критике «подрыв основ» и признаки терроризма или экстремизма.

Так возникло резонансное уголовное дело против известного пермского блогера Дмитрия Ширинкина. После массового убийства студентов в Вирджинии он в своем ЖЖ откликнулся на него в жанре рассказа от первого лица: «Я вчера купил пистолет старый „ТТ“ с затертыми номерами, коробку на 150 патронов. Патроны старые, на доннышке выбито: 1964 год. Но сохранились хорошо. Я заберу с собой два-три десятка душ». Эти слова предварялись признанием персонажа, что ему безумно надоели и конкретные властные лица, и оппозиционеры. Текст был оценен как «ложное сообщение о готовящемся теракте». Автору грозил срок до 3 лет, но он отделался 20 000 рублей.

Анонс

МедиаТренды № 12 (29)

Тема номера
СМИ в досуге современного человека



Издатель:
Факультет журналистики Московского государственного университета имени М. В. Ломоносова

Главный редактор: Елена Вартанова. Шеф-редактор: Денис Дунас. Отв. секретарь: Нонна Котрикадзе.
Фотокорреспондент: Георгий Шпикалов.
Над номером работали: Ирина Денисова, Арина Иванова, Диана Кульчицкая.
Дизайн: Арина Баланцева. Верстка: Елена Сиротина.
Адрес редакции: 125009 Москва, Моховая ул. 9, оф. 107. E-mail: mediaandtrends@gmail.com
Отпечатано в УПЛ факультета журналистики МГУ имени М. В. Ломоносова