Управление Министерства внутренних дел Российской Федерации по Смоленской области
(УМВД России по Смоленской области)

Лекционный материал на тему: «Безопасный Интернет»

Смоленск 2024

СОДЕРЖАНИЕ

1. Раздел **I**. Понятие и виды сети «Интернет»	стр. 3
1.1. Как работает "Интернет"	стр. 3
1.2. Интернет-сайт	стр. 3
1.3. Социальная сеть	стр. 3-4
1.4. Мессенджеры	стр. 4-6
2. Раздел II. Что необходимо знать каждому пользователю сети «Интернет».	стр. 6
2.1. Спроси совета у взрослого	стр. 6-7
2.2. Не делись своими личными данными	стр. 7
2.3. Не делись своими личными данными знакомых	стр. 7
2.4. Фильтруй информацию	стр. 7
2.5. Не верь рекламным объявлениям	стр. 8
2.6. Опасайся незнакомцев	стр. 8
2.7. Используй сложные пароли	стр. 8
2.8. Пользуйся только официальными сайтами	стр. 8-9
2.9. Отличай поддельные аккаунты	стр. 9
2.10. Соблюдай правила сетевого этикета	стр. 9
2.11. Информация напоследок	стр. 9
3. Раздел III. «Безопасный Интернет».	стр. 9-10
3.1. Памятка для детей «Безопасный Интернет»	стр. 10
3.2. Памятка для детей и подростков:	стр. 11
4. Раздел IV. Правила безопасности школьников в сети «Интернет»	стр. 11
4.1. Основные правила для школьников младших классов	стр. 11
4.2. Основные правила для школьников средних классов	стр. 11-12
4.3. Основные правила для школьников старших классов	стр. 12
5. Раздел V. Правила безопасности при посещении сайтов и по приему электронной почты	стр. 12-13
6. Раздел VI. Ответственность	стр. 13-14

1. Раздел I. Понятия и виды сети «Интернет».

1.1. Как работает «Интернет»

Интернет - это глобальная сеть взаимосвязанных компьютеров и устройств, которые общаются друг с другом с помощью стандартизированных протоколов. Интернет позволяет людям обмениваться информацией, общаться друг с другом, вести бизнес и получать доступ к широкому спектру **онлайн - услуг**. Интернет состоит из миллионов взаимосвязанных сетей, включая локальные сети **(LAN)**, глобальные сети **(WAN)** и беспроводные сети.

Когда вы выходите в Интернет, ваше устройство подключается к локальной сети, например, к домашней сети **Wi-Fi** или же к сотовой сети передачи данных. Затем эта сеть подключается к поставщику интернет — услуг **(ISP)**, который, в свою очередь, подключается к более широкому Интернету. Когда вы заходите на **веб-сайт** или **онлайн-сервис**, ваше устройство отправляет запрос по сети на сервер, на котором расположен этот веб-сайт или сервис. Затем сервер отправляет запрашиваемую информацию обратно на ваше устройство, которое уже отображает ее на экране.

1.2. «Интернет-сайт»

Интернет-сайт — это комплекс взаимосвязанных веб-страниц, объединенных под общим доменным именем.

Это пространство, где пользователи могут искать, обмениваться данными, приобретать продукцию или услуги, находить контакты для общения или получать удовольствие от контента, соответствующего их увлечениям.

Интернет-сайты могут включать в себя тексты, графические изображения, видеоролики и разнообразные мультимедийные компоненты.

1.3. «Социальная сеть»

Социальные сети — это интернет-платформы и приложения, предназначенные для построения виртуальных социальных взаимоотношений и обмена информацией между людьми.

Социальные сети позволяют:

- Создать персональные профили (аккаунты), размещать информацию о себе, фотографии, указывать интересы и другие данные.
- Общаться друг с другом, делиться своими мыслями, чувствами, фотографиями, видео и другим контентом, просматривать публикации других пользователей, обмениваться личными сообщениями, оставлять

комментарии.

- Находить друзей и единомышленников, объединяться в группы и сообщества.
- Следить за новостями, получать информацию о том, что происходит в мире.
- Развлекаться, играть в игры, смотреть видео, слушать музыку.
- Продвигать себя или свой бизнес, использовать для рекламы и маркетинга.

Основные виды социальных сетей:

- Общие социальные сети (Facebook (*4 марта 2022 года заблокирован Роскомнадзором, данная сеть признана экстремистской*), Одноклассники, Vkontakte, Twitter (*в начале марта 2022 года заблокирован Роскомнадзором*) — ориентированны на общее общение людей.
- Профессиональные социальные сети (Linkedln, Xing)- ориентированны на карьеру и профессиональные связи.
- Изображения-ориентированные социальные сети (Instagram *(4 марта 2022 года заблокирован Роскомнадзором, данная сеть признана экстремистской)*, Pinterest)- позволяют пользователям делиться фотографиями и изображениями.
- Микроблоги (Tumblr, LiveJournal)- позволяют пользователям публиковать короткие сообщения.
- Социальные сети для знакомств (Tinder, Baboo) — позволяют пользователям находить новых друзей и партнеров для отношений.

1.4. «Мессенджеры»

Мессенджер — это программа для мгновенного обмена текстовыми сообщениями и мультимедиа между зарегистрированными пользователями через сеть «Интернет».

С помощью мессенджера можно:

- общаться с другими пользователями один на один или в групповых беседах;
- отправлять текстовые или голосовые сообщения, а также стикеры, фото, видео и другие файлы;
- звонить и разговаривать по видеосвязи — один на один или в режиме конференции;
- создавать публичные каналы и подписываться на них;
- пользоваться чат-ботами.

Отличие мессенджеров от социальных сетей

И социальные сети, и мессенджеры предназначены для общения, но функциональность социальных сетей все равно шире — обычно они

сочетают чат, новостную ленту, аудио- и видеостриминг, игровой хостинг, маркетплейс товаров. Сервис знакомств и т. д.

У некоторых социальных сетей, таких как «Vkontakte», есть собственный мессенджер, связанный с платформой, но выделенный в отдельный сервис.

Некоторые мессенджеры, в свою очередь, дают пользователям и бизнесу возможность развивать сообщества. Так, в Telegram и WhatsApp они могут создавать каналы и публиковать в них контент для широкой аудитории.

Самые распространенные мессенджеры в России:
- WhatsApp;
- Viber;
- Telegram.

WhatsApp — позволяет отправлять текстовые и голосовые сообщения, создавать беседы до 256 пользователей, редактировать фото и видео перед отправкой, звонить общаться по видеосвязи — в том числе в режиме конференции. Есть режим исчезающих сообщений.

Доступен в мобильной, десктопной и веб-версии. Последняя синхронизируется с клиентом на смартфоне и работает только если он включен.

Версия **WhatsApp Business** предназначена для мессенджер-маркетинга. В ней можно создавать каталоги товаров, запускать рассылки, настраивать автоматическую отправку ответов на часто задаваемые вопросы и транзакционных сообщений об оплате или доставке.

Viber - позволяет отправлять текстовые и голосовые сообщения, создавать беседы до 250 пользователей, звонить по аудио и видео один на один и в конференц-режиме. В режиме видеосвязи на десктопе можно транслировать экран. Есть режим исчезающих сообщений.

Тариф **Viber Out** позволяет звонить даже пользователям, не авторизированным в приложении и с выключенным доступом к интернету — на мобильный номер.

Доступен в мобильной, десктопной и веб-версии, которые автоматически синхронизируются и могут работать не зависимо. Звонки можно переводить между устройствами.

Есть опция создания сообщества. Это групповой чат с неограниченным количеством участников, которым можно разрешить или запретить самим писать в него. Модерация происходит через роли администраторов и супер-администраторов. Аудитория наращивается с помощью пригласительных ссылок, для администраторов сообщества есть статистика.

Пакет решений Viber для бизнеса включает возможность

верификации аккаунта, медийную рекламу, настройки рассылок, отправки транзакционных и промосообщений, а также диалогов с клиентами через чат-бот или интеграцию с CRM. Все бизнес-сообщения от брендов хранятся в отдельной папке на основном экране.

Telegram- позволяет отправлять текстовые и голосовые сообщения, причем голосовые можно воспроизводить в ускоренном и замедленном режиме. Также здесь можно создавать беседы до 200 000 участников, звонить и общаться по видеосвязи.

Чаты можно группировать в папки и закреплять. Есть чат с самим собой- в него можно отправлять на хранение информацию и файлы без ограничения по объему.

Доступен в мобильной, десктопной и веб-версии, которые автоматически синхронизируются и работают независимо. Есть режим секретного чата, который виден только на устройстве, на котором он был начат.

Платная подписка **Telegram Premium** удваивает лимиты количества папок и закрепленных чатов, увеличивает скорость загрузки файлов, включает опции расшифровки голосовых и динамического перевода сообщений с иностранных языков, дает доступ к анимированным эмоджи, отключает рекламу в каналах и т. д.

Отдельной версии для бизнеса здесь нет, но есть возможности для продвижения личных и коммерческих брендов: публичные каналы, реклама через официальную платформу **«Telegram Ads»**, боты для автоматизации рутинный задач и расширения функциональности каналов и чатов. Например, с помощью бота канал можно укомплектовать каталогом, витриной, корзиной товаров и добавить возможность оплаты.

2. Раздел II. Что необходимо знать каждому пользователю сети «Интернет».

2.1. Спроси совета у взрослого

Если ребенок собирается пройти регистрацию на каком-либо интернет-сайте, опубликовать свои фотографии и поделиться личной информацией, сначала желательно сообщить об этом взрослым (родителями, законными представителями). Родители проанализируют ситуацию и определят, насколько опасен сайт, можно ли загружать туда фотографии и какие именно снимки подходят для публикации.

Подростки, столкнувшиеся с травлей и преследованием в сети, не должны бояться рассказать об этом. О любом случае, вызвавшем смущение или тревогу, следует сообщать взрослым.

2.2. Не делись своими личными данными

Одно из самых главных правил – никогда не рассказывать в сети информацию, которая помогла бы незнакомцу найти ребенка в реальности и поставить под вопрос его безопасность. Даже если кажется, что человек, с которым происходит онлайн-общение, хороший и не сделает ничего плохого, личные данные стоит оставить при себе. Речь идет о номере телефона, адресе проживания, номере школы и класса, графике работы родителей, данных из документов и даже названии спортивной команды, в которой занимается ребенок.

2.3. Не делись личными данными знакомых

Рассказывать в интернете о своих знакомых, друзьях и одноклассниках – плохая идея. Любые персональные данные, будь они самого ребенка, его родителей или других людей, должны оставаться в тайне. Не стоит публиковать фотографии со своими друзьями в профиле и пересылать их в частной переписке. Перед тем как выложить совместное фото со спортивной тренировки или с праздника, сообщите об этом детям, изображенным на снимке, а они, в свою очередь, пусть посоветуются с родителями, можно ли публиковать снимок в сети.

2.4. Фильтруй информацию

Злоумышленники очень хитры – они манипулируют людьми, давят на страх и жалость, шантажируют полученными данными. Детям стоит понимать, что слепая вера каждому слову в интернете может привести к краже денег и личных данных, травле и преследованию. Не доверяйте всему написанному в интернете, игнорируйте подозрительные письма и сообщения от незнакомцев, не переходите по ссылкам, обещающим бесплатные подарки, тщательно обдумывайте каждое нажатие.

Если кто-то из друзей или знакомых просит в сообщении помощи, уточните, что произошло и перезвоните этому человеку, чтобы убедиться, что его страница не попала в руки мошенников.

2.5. Не верь рекламным объявлениям

Никто не защищен от мошеннических действий, даже взрослые. Иногда требуется слишком много времени, чтобы понять, что перед тобой обманщик. Однако есть четкие признаки подозрительных и опасных сайтов: обилие яркой рекламы на странице, «кричащие заголовки», предлагающие «прямо сейчас» и «бесплатно» – такой информации в сети доверять не следует.

Чтобы убедиться, что информация не несет вреда и соответствует действительности, можно сравнить ее в других источниках, а также уточнить у родителей и друзей, стоит ли доверять опубликованному.

2.6. Опасайся незнакомцев

Конечно, если вы уже не первый месяц играете с сетевым другом в онлайн-игру и немного друг друга знаете, никто не помешает вам с ним весело проводить время. Однако если незнакомый человек назойливо стучится в личные сообщения, отвечать на них не стоит. Постоянные обращения, частые письма, просьбы прислать свои данные и фото – это повод прекратить общение, заблокировать человека и рассказать о произошедшем взрослым.

2.7. Используй сложные пароли

Простой пароль легко запомнить и легко взломать, поэтому стоит все-таки более серьезно отнестись к его созданию. Детям необходимо придумать сложные комбинации из заглавных и строчных букв, с добавлением цифр и символов. Также для разных сайтов в интернете должны быть придуманы разные пароли, чтобы при взломе одного профиля доступ к остальным остался закрыт.

2.8. Пользуйся только официальными сайтами

Фишинг – способ, который используют мошенники для выманивания личных данных через интернет. Происходит это так: пользователь получает ссылку, похожую на адрес соцсети или почтового сервиса, переходит по ней, вводит на поддельном сайте конфиденциальные данные и становится жертвой злоумышленников. Система автоматически устанавливает вредоносные программы на устройство и крадет персональные данные.

Чтобы этого не произошло, важно внимательно проверять все, что вам присылают, прежде чем переходить по ссылкам. Обращайте внимание на детали, проверяйте адрес сайта, на который вам предстоит зайти. Чаще всего разница заключается в одной букве: например, для mail.ru может быть создан meil.ru, а для vk.com – vc.com.

2.9. Отличай поддельные аккаунты

В интернете любой может придумать себе личность – проверить информацию не так просто, как кажется. Это затрудняет распознавание тех, кто скрывается под фейковым именем. Подделку отличить все-таки

можно, и вот основные ее признаки:

- минимум друзей или их отсутствие;
- страница обычно только что созданная и пустая;
- незнакомец постоянно соглашается, указывает на вашу с ним схожесть;
- назойливость, не готовность прерывать разговор;
- большая разница в возрасте – взрослый человек не должен настойчиво набиваться в друзья детям.

2.10. Соблюдай правила сетевого этикета

Не груби, будь вежлив даже в тех случаях, когда кажется, что человек тебя обманывает. Постарайся держать эмоции под контролем, чтобы не терять концентрацию. Помни об осторожности даже в стрессовой ситуации. Не используй «капслок» – такие предложения считаются громким криком и могут спровоцировать человека на агрессию. Если разговор становится неприятным, закрой тему или вовсе выйди из сети и сделай себе перерыв. Еще лучше заблокировать обидчика, не отвечая оскорблениями на оскорбления.

2.11. Информация напоследок

Не нужно делать в интернете то, что ты бы не сделал в реальной жизни. Интернет – такой же мир, в нем также действуют правила, от соблюдения которых зависит твоя безопасность. Если ты столкнулся с любым неприятным и неприемлемым поступком, сообщи об этом родителям. Мошенникам и злоумышленникам тяжело противостоять в одиночку, не бойся просить поддержки у близких людей.

3. Раздел III. «Безопасный Интернет».

3.1. Памятка для детей «Безопасный Интернет» содержит следующие рекомендации:

1. Никому и никогда не разглашай свои пароли.
2. При регистрации на сайтах и в социальных сетях старайся не указывать личную информацию.
3. Помни, что фотография, размещенная в Интернете, доступна для просмотра всем.
4. Не встречайся с теми, с кем ты знакомишься лишь в Интернете.
5. В Интернете и социальных сетях старайся общаться только с теми, с кем ты лично знаком.

6. Не используй веб-камеру при общении с незнакомыми людьми, помни о необходимости сохранять дистанцию с незнакомцами.

7. Уважай собеседников в Интернете. Никогда и ни при каких обстоятельствах не угрожай другим, не размещай агрессивный и провокационный материал.

8. Не вступай в незнакомые сообщества и не распространяй по чьей-либо просьбе информационные, провокационные и агрессивно-настроенные материалы и сообщения.

9. Не все, что ты можешь прочесть или увидеть в интернете, правда. Не ленись и перепроверяй информацию в других поисковых системах или спроси у родителей.

10. Расскажи все, что ты увидел, выучил или узнал нового, взрослому. Доверяй своим родителям, поскольку только они смогут помочь в трудной ситуации.

11. Никогда не указывай свой номер телефона или электронный адрес, не отправляй с него смс-сообщения на незнакомые номера в Интернете. Если тебе пришло сообщение с незнакомого адреса, его лучше не открывать.

12. Если тебе показалось, что твои друзья отправляют тебе «странную» информацию или программы, переспроси у них, отправляли ли они тебе какие-либо файлы. Иногда мошенники могут действовать от имени чужих людей, в том числе твоих друзей и родственников.

13. Если ты хочешь купить в Интернете какую-либо услугу или игру, обратись к взрослому. Он подскажет тебе, как избежать мошенничества.

14. Не загружай файлы, программы или музыку без согласия взрослых - они могут содержать вирусы и причинить вред компьютеру.

3.2. Памятка для детей и подростков:

1. Нормы поведения и нравственные принципы одинаковы как в виртуальном, так и в реальном мире.

2. Незаконное копирование продуктов труда других людей (музыки, игр, программ и т.д.) считается плагиатом (умышленное присвоение авторства чужого произведения).

3. Не верьте всему, что в видите или читаете в интернете. При наличии сомнений в правдивости какой-то информации следует обратиться за советом к взрослым.

4. Нельзя сообщать другим пользователям интернета свою личную информацию (адрес, номер телефона, номер школы, любимые места для игр и т.д.).

5. Если вы общаетесь в чатах, пользуетесь программами мгновенной передачи сообщений, играете в сетевые игры, занимаетесь в интернете чем-то, что требует указания идентификационного имени пользователя, тогда выберите это имя вместе со взрослыми, чтобы убедиться, что оно не содержит

никакой личной информации.

6. Интернет-друзья могут на самом деле быть не теми, за кого они себя выдают, поэтому вы не должны встречаться с интернет-друзьями лично.

7. Нельзя открывать файлы, присланные от неизвестных вам людей. Эти файлы могут содержать вирусы или фото/видео с нежелательным содержанием.

8. Научитесь доверять интуиции. Если что-нибудь в интернете будет вызывать у вас психологический дискомфорт, поделитесь своими впечатлениями с взрослыми.

4. Раздел IV. Правила безопасности школьников в Интернет

4.1. Основные правила для школьников младших классов

Вы должны это знать:

1. Всегда спрашивайте родителей о незнакомых вещах в интернете. Они расскажут, что безопасно делать, а что нет.

2. Прежде чем начать дружить с кем-то в интернете, спросите у родителей как безопасно общаться.

3. Никогда не рассказывайте о себе незнакомым людям. Где вы живете, в какой школе учитесь, номер телефона должны знать только ваши друзья и семья.

4. Не отправляйте фотографии людям, которых вы не знаете. Не надо чтобы незнакомые люди видели ваши личные фотографии.

5. Не встречайтесь без родителей с людьми из интернета вживую. В интернете многие люди рассказывают о себе неправду.

6. Общаясь в интернете, будьте дружелюбны с другими. Не пишите грубых слов, читать грубости так же неприятно, как и слышать. Вы можете нечаянно обидеть человека.

7. Если вас кто-то расстроил или обидел, обязательно расскажите родителям.

4.2. Основные правила для школьников средних классов

Вы должны это знать:

1. При регистрации на сайтах старайтесь не указывать личную информацию, т.к. она может быть доступна незнакомым людям. Также не рекомендуется размещать свою фотографию, давая тем самым представление о том, как вы выглядите посторонним людям.

2. Используйте веб-камеру только при общении с друзьями. Проследите, чтобы посторонние люди не имели возможности видеть вас во время разговора, т.к. он может быть записан.

3. Нежелательные письма от незнакомых людей называются «спам». Если вы получили такое письмо, не отвечайте на него. В случае, если вы ответите

на подобное письмо, отправитель будет знать, что вы пользуетесь своим электронным почтовым ящиком и будет продолжать посылать вам спам.

4. Если вам пришло сообщение с незнакомого адреса, его лучше не открывать. Подобные письма могут содержать вирусы.

5. Если вам приходят письма с неприятным и оскорбляющим вас содержанием, если кто-то ведет себя в вашем отношении неподобающим образом, сообщите об этом.

6. Если вас кто-то расстроил или обидел, расскажите все взрослому.

4.3. Основные правила для школьников старших классов

Вы должны это знать:

1. Нежелательно размещать персональную информацию в интернете.

2. Персональная информация — это номер вашего мобильного телефона, адрес электронной почты, домашний адрес и личные фотографии.

3. Если вы публикуете фото или видео в интернете — каждый может посмотреть их.

4. Не отвечайте на спам (нежелательную электронную почту).

5. Не открывайте файлы, которые прислали неизвестные Вам люди. Вы не можете знать, что на самом деле содержат эти файлы – в них могут быть вирусы или фото/видео с «агрессивным» содержанием.

6. Не добавляйте незнакомых людей в свой контакт лист в IM (ICQ, MSN messenger и т.д.)

7. Помните, что виртуальные знакомые могут быть не теми, за кого себя выдают.

8. Если рядом с вами нет родственников, не встречайтесь в реальной жизни с людьми, с которыми вы познакомились в интернете. Если ваш виртуальный друг действительно тот, за кого он себя выдает, он нормально отнесется к вашей заботе о собственной безопасности!

9. Никогда не поздно рассказать взрослым, если вас кто-то обидел.

5. Раздел V. Правила безопасности при посещении сайтов и по приему электронной почты

1. Не ходите на незнакомые сайты.

2. Если к вам по почте пришел файл Word или Excel, даже от знакомого лица, прежде чем открыть, обязательно проверьте его на макровирусы.

3. Если пришел exe-файл, даже от знакомого, ни в коем случае не запускайте его, а лучше сразу удалите и очистите корзину в вашей программе чтения почты.

4. Не заходите на сайты, где предлагают бесплатный Интернет (не бесплатный e-mail, это разные вещи).

5. Никогда никому не посылайте свой пароль.

6. Старайтесь использовать для паролей трудно запоминаемый набор цифр и букв.

Распространение сведений, содержащих инструкции по самодельному изготовлению взрывчатых веществ и взрывных устройств, незаконному изготовлению или переделке оружия, основных частей огнестрельного оружия, если эти действия не содержат признаков уголовно наказуемого деяния, — по части 5 ст. 13.15 КоАП РФ;

Распространение информации, содержащей предложения о розничной продаже дистанционным способом алкогольной продукции, спиртосодержащей пищевой продукции, этилового спирта, или спиртосодержащей непищевой продукции, розничная продажа которой ограничена или запрещена законодательством о государственном регулировании производства и оборота этилового спирта, алкогольной и спиртосодержащей продукции и об ограничении потребления (распития) алкогольной продукции, — по части 8.ст. 13.15 КоАП РФ;

Пропаганду наркотических средств, психотропных веществ или их прекурсоров, растений, содержащих наркотические средства или психотропные вещества либо их прекурсоры, и их частей, содержащих наркотические средства или психотропные вещества либо их прекурсоры, новых потенциально опасных психоактивных веществ – по части 1.1 статьи 6.13 КоАП РФ;

Пропаганду закиси азота – по статье 13.1 КоАП РФ;

Склонение к потреблению наркотических средств, психотропных веществ или их аналогов – по п. «д» части 2, частям 3, 4 статьи 230 УК РФ.

6. Раздел VI. Ответственность

За преступления в сфере компьютерной информации:

Неправомерный доступ к охраняемой законом компьютерной информации, если это деяние повлекло уничтожение, блокирование, модификацию либо копирование компьютерной информации, — сведения (сообщения, данные), представленные в форме электрических сигналов, независимо от средств их хранения, обработки и передачи — по статье 272 УК РФ;

Создание, распространение или использование компьютерных программ либо иной компьютерной информации, заведомо предназначенных для несанкционированного уничтожения, блокирования, модификации, копирования компьютерной информации или нейтрализации средств защиты компьютерной информации, — по статье 273 УК РФ.

За преступления против общественной нравственности с использованием сети Интернет (включая «секстинг» – склонение несовершеннолетних к пересылке личных фотографий, сообщений интимного содержания):

Распространение, публичная демонстрация или рекламирование порнографических материалов или предметов – по п. «б» части 3 статьи 242 УК РФ;

Распространение, публичная демонстрация или рекламирование материалов или предметов с порнографическими изображениями несовершеннолетних, – по п. «г» части 2 статьи 242.1 УК РФ.

За противоправные действия террористического и экстремистского характера, совершенные с использованием сети Интернет:

Публичные призывы к осуществлению террористической деятельности, публичное оправдание терроризма (то есть публичное заявление о признании идеологии и практики терроризма правильными, нуждающимися в поддержке и подражании) или пропаганда терроризма (то есть деятельность по распространению материалов или информации, направленных на формирование у лица идеологии терроризма, убежденности в ее привлекательности либо представления о допустимости осуществления террористической деятельности) – по части 2 статьи 205.2 УК РФ;

Заведомо ложное сообщение об акте терроризма, то есть о готовящихся взрыве, поджоге или иных действиях, создающих опасность гибели людей, причинения значительного имущественного ущерба либо наступления иных общественно опасных последствий, совершенное из хулиганских побуждений либо в целях дестабилизации деятельности органов власти, — по статье 207.1 УК РФ;

Массовое распространение экстремистских материалов, включенных в опубликованный федеральный список экстремистских материалов****, а равно их производство либо хранение в целях массового распространения, — по статье 20.29 КоАП РФ;

Распространение сведений, содержащих инструкции по самодельному изготовлению взрывчатых веществ и взрывных устройств, незаконному изготовлению или переделке оружия, основных частей огнестрельного оружия, если эти действия не содержат признаков уголовно наказуемого деяния, — по части 5 ст. 13.15 КоАП РФ;