**Обучающий семинар по теме: «Информационная безопасность»**

**Дата проведения:** 09.12.2022 г.

**Время проведения:** 14.00 час. (1 час 30 мин.)

**Место проведения:** ГБУ ДПО «Отрадненский РЦ», г. Отрадный, ул. Гайдара, д.74, каб. 25 (учебный кабинет)

**Организатор:** Денисова Т.А., методист ГБУ ДПО «Отрадненский РЦ»

**Цель:** Воспитание грамотного и ответственного пользователя сети Интернет.

Ознакомить педагогов с различными опасностями в сети Интернет и помочь избежать этих опасностей, формирование навыков безопасного поведения в Интернет - пространстве.

**Задачи:**

1. Повышение уровня знаний об основных опасностях при использовании сети Интернет.
2. Усвоение правил безопасного использования Интернета.
3. Развитие навыков поведения в опасных ситуациях в условии Интернета.

Дети и подростки — активные пользователи интернета как в мире, так в Российской Федерации.

**План семинара.**

1. Встреча и регистрация участников семинара.
2. Презентация «Информационная безопасность».

**(Слайд 1 «Информационная безопасность»)**

**(Слайд 2 «Актуальность информационной безопасности»)**

Федеральный закон от 29.12.2010 № 436-ФЗ «О защите детей от информации, причиняющей вред их здоровью и развитию» регулирует отношения, связанные с защитой детей от информации, причиняющей вред их здоровью и (или) развитию, в том числе от такой информации, содержащейся в информационной продукции.

Федеральный закон № 436 определяет перечень запрещенной для детей информации, возрастные категории детей и виды информации, разрешенной для той или иной категории, а также требования к обороту информационной продукции.

**(Слайд 3 «Информация, запрещенная для распространения среди детей»)**

* побуждающая детей к совершению действий, представляющих угрозу их жизни и (или) здоровью, в том числе к причинению вреда своему здоровью, самоубийству;
* способная вызвать у детей желание употребить наркотические средства, психотропные и (или) одурманивающие вещества, табачные изделия, алкогольную и спиртосодержащую продукцию, принять участие в азартных играх, заниматься проституцией, бродяжничеством или попрошайничеством;
* обосновывающая или оправдывающая допустимость насилия и (или) жестокости либо побуждающая осуществлять насильственные действия по отношению к людям или животным, за исключением случаев, предусмотренных настоящим Федеральным законом

**(Слайд 4 «Информация, запрещенная для распространения среди детей»)**

* отрицающая семейные ценности, пропагандирующая нетрадиционные сексуальные отношения и формирующая неуважение к родителям и (или) другим членам семьи;
* оправдывающая противоправное поведение;
* содержащая нецензурную брань;
* содержащая информацию порнографического характера;
* о несовершеннолетнем, пострадавшем в результате противоправных действий (бездействия), включая фамилии, имена, отчества, фото- и видеоизображения такого несовершеннолетнего, его родителей и иных законных представителей, дату рождения такого несовершеннолетнего, аудиозапись его голоса, место его жительства или место временного пребывания, место его учебы или работы, иную информацию, позволяющую прямо или косвенно установить личность такого несовершеннолетнего.

**(Слайд 5 «Виды информационных угроз для детей»)**

**(Слайд 6 «Компьютерные вирусы»)**

Компьютерный вирус – это разновидность компьютерных программ, отличительной особенностью которой является способность к размножению.

В дополнение к этому, вирусы могут повредить или полностью уничтожить все файлы и данные, подконтрольные пользователю, от имени которого была запущена заражённая программа, а также повредить или даже уничтожить операционную систему со всеми файлами в целом. В большинстве случаев распространяются вирусы через интернет.

**(Слайд 7«Методы защиты от вредоносных программ»)**

* Используй современные операционные системы, имеющие серьёзный уровень защиты от вредоносных программ;
* Постоянно устанавливай пачти (цифровые заплатки, которые автоматически устанавливаются с целью доработки программы) и другие обновления своей операционной системы. Скачивай их только с официального сайта разработчика ОС. Если существует режим автоматического обновления, включи его;
* Работай на своем компьютере под правами пользователя, а не администратора. Это не позволит большинству вредоносных программ инсталлироваться на твоем персональном компьютере

**(Слайд 8 «Методы защиты от вредоносных программ»)**

* Используй антивирусные программные продукты известных производителей, с автоматическим обновлением баз;
* Ограничь физический доступ к компьютеру для посторонних лиц;
* Используй внешние носители информации, такие как флэшка, диск или файл из интернета, только из проверенных источников;
* Не открывай компьютерные файлы, полученные из ненадёжных источников. Даже те файлы, которые прислал твой знакомый. Лучше уточни у него, отправлял ли он тебе их.

**(Слайд 9 «Сети Wi-Fi»)**

Wi-Fi - это не вид передачи данных, не технология, а всего лишь бренд, марка. Еще в 1991 году нидерландская компания зарегистрировала бренд «WECA», что обозначало словосочетание «Wireless Fidelity», который переводится как «беспроводная точность». До нашего времени дошла другая аббревиатура, которая является такой же технологией. Это аббревиатура «Wi-Fi». Такое название было дано с намеком на стандарт высший звуковой техники Hi-Fi, что в переводе означает «высокая точность».

**(Слайд 10 «Советы по безопасности работе в общедоступных сетях Wi-Fi»)**

* Не передавай свою личную информацию через общедоступные Wi-Fi сети. Работая в них, желательно не вводить пароли доступа, логины и какие-то номера;
* Используй и обновляй антивирусные программы и брандмауер. Тем самым ты обезопасишь себя от закачки вируса на твое устройство;
* При использовании Wi-Fi отключи функцию «Общий доступ к файлам и принтерам». Данная функция закрыта по умолчанию, однако некоторые пользователи активируют её для удобства использования в работе или учебе

**(Слайд 11 «Советы по безопасности работе в общедоступных сетях Wi-Fi»)**

* Не используй публичный WI-FI для передачи личных данных, например для выхода в социальные сети или в электронную почту;
* Используй только защищенное соединение через HTTPS, а не НТТР, т.е. при наборе веб-адреса вводи именно «https://»;
* В мобильном телефоне отключи функцию «Подключение к Wi-Fi автоматически». Не допускай автоматического подключения устройства к сетям Wi-Fi без твоего согласия.

**(Слайд 12 «Социальные сети»)**

Социальные сети активно входят в нашу жизнь, многие люди работают и живут там постоянно, а в Facebook уже зарегистрирован миллиард человек, что является одной седьмой всех жителей планеты. Многие пользователи не понимают, что информация, размещенная ими в социальных сетях, может быть найдена и использована кем угодно, в том числе не обязательно с благими намерениями.

**(Слайд 13 «Основные советы по безопасности в социальных сетях»)**

* Ограничь список друзей. У тебя в друзьях не должно быть случайных и незнакомых людей;
* Защищай свою частную жизнь. Не указывай пароли, телефоны, адреса, дату твоего рождения и другую личную информацию. Злоумышленники могут использовать даже информацию о том, как ты и твои родители планируете провести каникулы;
* Защищай свою репутацию - держи ее в чистоте и задавай себе вопрос: хотел бы ты, чтобы другие пользователи видели, что ты загружаешь? Подумай, прежде чем что-то опубликовать, написать и загрузить

**(Слайд 14 «Основные советы по безопасности в социальных сетях»)**

* Если ты говоришь с людьми, которых не знаешь, не используй свое реальное имя и другую личную информации: имя, место жительства, место учебы и прочее;
* Избегай размещения фотографий в Интернете, где ты изображен на местности, по которой можно определить твое местоположение;
* При регистрации в социальной сети необходимо использовать сложные пароли, состоящие из букв и цифр и с количеством знаков не менее 8;
* Для социальной сети, почты и других сайтов необходимо использовать разные пароли. Тогда если тебя взломают, то злоумышленники получат доступ только к одному месту, а не во все сразу.

**(Слайд 15 «Электронные деньги и банковские карты»)**

Электронные деньги - это очень удобный способ платежей, однако существуют мошенники, которые хотят получить эти деньги.

Обычно сервисы электронных денег предлагают клиентам анонимные и неанонимные аккаунты. Разница в том, что анонимные - это те, в которых разрешается проводить операции без идентификации пользователя, а в неанонимных идентификация пользователя является обязательной.

Важно помнить, что для покупок в Интернете зачастую достаточно знать только номер карты и срок ее действия, чем очень часто и пользуются злоумышленники.

Сервисы электронных денег и банки предоставляют возможность привязки к счету мобильного телефона, что позволяет не только восстановить доступ к счету или карте, а также подтверждать платежи (транзакции) с помощью одноразового пароля.

**(Слайд 16 «Виды электронных платежных систем»)**

**(Слайд 17 «Основные советы по безопасной работе с электронными деньгами»)**

* Привяжи к счету мобильный телефон. Это самый удобный и быстрый способ восстановить доступ к счету. Привязанный телефон поможет, если забудешь свой платежный пароль или зайдешь на сайт с незнакомого устройства;
* Используй одноразовые пароли. После перехода на усиленную авторизацию тебе уже не будет угрожать опасность кражи или перехвата платежного пароля;
* Выбери сложный пароль. Преступникам будет не просто угадать сложный пароль. Надежные пароли — это пароли, которые содержат не менее 8 знаков и включают в себя строчные и прописные буквы, цифры и несколько символов, такие как знак доллара, фунта, восклицательный знак и т.п. Например, $tR0ng!;
* Не вводи свои личные данные на сайтах, которым не доверяешь.

**(Слайд 18 «Что делать»)**

* Потеряна банковская карта. Сообщить по телефону в банк о произошедшем и попросить ее заблокировать. Банк предложит вместо данной карты выпустить новую карту с новым номером. Пока не будет заблокирована банковская карта, любой, у кого она окажется в руках, сможет воспользоваться ей;
* Пришло уведомление о платеже, который вы не совершали. Необходимо сообщить в банк или платежный сервис, направив заявление о чарджбеке (отмене операции), в котором максимально подробно описать произошедшее. Банк или платежный сервис рассмотрит обращение и вернет вам деньги в срок от 30 до 60 дней.
* Важно помнить, что чем раньше удастся выявить проблему и начать предпринимать меры, то тем больше шансов уменьшить ущерб, который может быть нанесен вам, вашей семье и другим лицам.

**(Слайд 19 «Электронная почта»)**

Электронная почта — это технология и предоставляемые ею услуги по пересылке и получению электронных сообщений, которые распределяются в компьютерной сети. Обычно электронный почтовый ящик выглядит следующим образом: имя\_пользователя@имя\_домена. Также кроме передачи простого текста, имеется возможность передавать файлы.

**(Слайд 20 «Основные советы по безопасной работе с электронной почтой»)**

* Надо выбрать правильный почтовый сервис. В интернете есть огромный выбор бесплатных почтовых сервисов, однако лучше доверять тем, кого знаешь и кто первый в рейтинге;
* Не указывай в личной почте личную информацию. Например, лучше выбрать «музыкальный\_фанат@» или «рок2013» вместо «тема13»;
* Используй двухэтапную авторизацию. Это когда помимо пароля нужно вводить код, присылаемый по SMS;
* Выбери сложный пароль. Для каждого почтового ящика должен быть свой надежный, устойчивый к взлому пароль

**(Слайд 21 «Основные советы по безопасной работе с электронной почтой»)**

* Если есть возможность написать самому свой личный вопрос, используй эту возможность;
* Используй несколько почтовых ящиков. Первый для частной переписки с адресатами, которым ты доверяешь. Это электронный адрес не надо использовать при регистрации на форумах и сайтах;
* Не открывай файлы и другие вложения в письмах даже если они пришли от твоих друзей. Лучше уточни у них, отправляли ли они тебе эти файлы;
* После окончания работы на почтовом сервисе перед закрытием вкладки с сайтом не забудь нажать на «Выйти».

**(Слайд 22 «Кибербуллинг или виртуальное издевательство»)**

Кибербуллинг - преследование сообщениями, содержащими оскорбления, агрессию, запугивание; хулиганство; социальное бойкотирование с помощью различных интернет-сервисов.

**(Слайд 23 «Основные советы по борьбе с кибербуллингом»)**

* Не бросайся в бой. Лучший способ: посоветоваться как себя вести и, если нет того, к кому можно обратиться, то вначале успокоиться. Если ты начнешь отвечать оскорблениями на оскорбления, то только еще больше разожжешь конфликт;
* Управляй своей киберрепутацией;
* Анонимность в сети мнимая. Существуют способы выяснить, кто стоит за анонимным аккаунтом;
* Не стоит вести хулиганский образ виртуальной жизни. Интернет фиксирует все твои действия и сохраняет их. Удалить их будет крайне затруднительно

**(Слайд 24 «Основные советы по борьбе с кибербуллингом»)**

* Игнорируй единичный негатив. Одноразовые оскорбительные сообщения лучше игнорировать. Обычно агрессия прекращается на начальной стадии;
* Бан агрессора. В программах обмена мгновенными сообщениями, в социальных сетях есть возможность блокировки отправки сообщений с определенных адресов;
* Если ты свидетель кибербуллинга. Твои действия: выступить против преследователя, показать ему, что его действия оцениваются негативно, поддержать жертву, которой нужна психологическая помощь, сообщить взрослым о факте агрессивного поведения в сети.

**(Слайд 25 «Мобильный телефон»)**

Современные смартфоны и планшеты содержат в себе вполне взрослый функционал, и теперь они могут конкурировать со стационарными компьютерами. Однако, средств защиты для подобных устройств пока очень мало.

**(Слайд 26 «Основные советы для безопасности мобильного телефона»)**

* Ничего не является по-настоящему бесплатным. Будь осторожен, ведь когда тебе предлагают бесплатный контент, в нем могут быть скрыты какие-то платные услуги;
* Думай, прежде чем отправить SMS, фото или видео. Ты точно знаешь, где они будут в конечном итоге?
* Необходимо обновлять операционную систему твоего смартфона;
* Используй антивирусные программы для мобильных телефонов

**(Слайд 27 «Основные советы для безопасности мобильного телефона»)**

* Не загружай приложения от неизвестного источника, ведь они могут содержать вредоносное программное обеспечение;
* После того как ты выйдешь с сайта, где вводил личную информацию, зайди в настройки браузера и удали cookies;
* Периодически проверяй какие платные услуги активированы на твоем номере;
* Давай свой номер мобильного телефона только людям, которых ты знаешь и кому доверяешь;
* Bluetooth должен быть выключен, когда ты им не пользуешься. Не забывай иногда проверять это.

**(Слайд 28 «Online-игры»)**

Современные онлайн-игры – это красочные, захватывающие развлечения, объединяющие сотни тысяч человек по всему миру. Игроки исследуют данный им мир, общаются друг с другом, выполняют задания, сражаются с монстрами и получают опыт. За удовольствие они платят: покупают диск, оплачивают абонемент или приобретают какие-то опции. Все эти средства идут на поддержание и развитие игры, а также на саму безопасность: совершенствуются системы авторизации, выпускаются новые патчи (цифровые заплатки для программ), закрываются уязвимости серверов. В подобных играх стоит опасаться не столько своих соперников, сколько кражи твоего пароля, на котором основана система авторизации большинства игр.

**(Слайд 29 «Основные советы по безопасности твоего игрового аккаунта»)**

* Если другой игрок ведет себя плохо или создает тебе неприятности, заблокируй его в списке игроков;
* Пожалуйся администраторам игры на плохое поведение этого игрока, желательно приложить какие-то доказательства в виде скринов;
* Не указывай личную информацию в профайле игры;
* Уважай других участников по игре;
* Не устанавливай неофициальные патчи и моды;
* Используй сложные и разные пароли;
* Даже во время игры не стоит отключать антивирус. Пока ты играешь, твой компьютер могут заразить.

**(Слайд 30 «Сетевое мошенничество»)**

Злоумышленники могут использовать различные методы социальной инженерии (угрозы, шантаж, игру на чувствах жертвы — например, жадности или сочувствии), чтобы выманить деньги и получить личные и конфиденциальные данные: к таким данным относятся логины и пароли от различных сервисов, в том числе банковских, номера и пин-коды банковских карт и другие персональные данные.

**(Слайд 31 «Сетевое мошенничество имеет множество методов»)**

Фишинг (англ. phishing, от fishing — рыбная ловля, выуживание) предполагает за счет использования различных методов заманивания пользователя на поддельный сайт, например, через ссылку в письме, баннер или ссылку в тексте.

Иногда вредоносная ссылка маскируется под правильную ссылку – так злоумышленники часто используют похожие имена сайтов, чтобы ввести жертву в заблуждение с помощью опечатки в адресе сайта, или сайты, копирующие интерфейс известных ресурсов. Примеры: http://www.sberbank.ru/ и http://www.sbenbank.ru/ либо www.yandex.ru и www.yadndex.ru.

На подобных сайтах пользователю предлагается ввести логин и пароль или данные счета, после чего зачастую происходит перенаправление на реальный сайт, но данные уже попадают в руки мошенников.

**(Слайд 32)**

Вишинг является разновидностью фишинга, в которой используется телефон. Мошенник может позвонить и представиться сотрудником банка или платежного сервиса и попросить продиктовать какие-либо платежные данные, например, пароль или код, пришедший на телефон. Его цель – выманить платежные данные, с помощью которых можно украсть деньги с карты или кошелька. Часто дополнительно присылается СМС со ссылкой, которая ведет на фишинговый сайт.

**(Слайд 33)**

Фарминг или скрытое перенаправление является также разновидностью фишинга, но направляет пользователя вирус или взломанная программа на поддельный сайт, являющийся полной копией официального ресурса.  
**(Слайд 34 «Сетевое мошенничество имеет также множество видов»)**

* Липовые акции и фальшивые выигрыши в лотереи. Пользователь может получить сообщение (по телефону, почте или SMS), что выиграл некий приз, а для его получения необходимо «уплатить налог», «оплатить доставку» или просто пополнить какой-то счет;
* Признаки фальшивой лотереи: пользователь никогда не принимал участие в лотерее; пользователь никогда не оставлял своих личных данных на этом ресурсе; почтовый адрес отправителя – общедоступный почтовый сервис, например, gmail.com, mail.ru, yandex.ru;

**(Слайд 35)**

* Просьба «друзей» сообщить пароль, когда знакомый в социальной сети сообщает о потере телефона, просит напомнить ваш номер, вам приходит SMS с неким кодом, а тот же друг в социальной сети сообщает, что заказывает товар или регистрируется на сайте и случайно указал ваш телефон вместо своего. Он просит сообщить пришедший код. Таким образом, ваш номер будет подключен к платной подписке и с вас начнут списывать деньги;
* Ложная блокировка аккаунта в социальной сети: на баннере подробно расписан вариант «спасения» от блокирования страницы в социальный сети, который включает отправку SMS на «короткий» номер или введение кода подтверждения. В первом случае происходит разовое списание денег, а во втором оформляется ежедневная подписка на какую-либо платную услугу;

**(Слайд 36)**

* Рекламные сообщения и баннеры о необходимости обновления браузера имеют риск подписаться на платную загрузку или получить вирус с архивом платной программы;
* Бесплатное скачивание файлов и просмотр каких-либо файлов с подпиской по номеру телефона, после чего включится подписка и с указанного номера могут начать списываться деньги;

**(Слайд 37)**

* Пользователю предлагается бесплатный антивирус, под видом которого на устройство попадет вредоносная программа, либо создается иллюзия, что компьютер уже заражен и для уничтожения угрозы нужно воспользоваться специальным антивирусом, который, опять же, окажется вирусом. Примером является появление надписи на экране компьютера о блокировке операционной системы, устранить которую можно только при отправке SMS с кодом, пришедшим на телефон при подтверждении, – после чего запускается сам вирус;

**(Слайд 38)**

* Предложения очень выгодных покупок, реклама больших скидок или анонс распродаж, которые размещаются на сайтах, в социальных сетях и присылаются смс или на электронную почту. Такие предложения обычно предполагают перевод денег на банковскую карту, электронный кошелек или мобильный номер. В настоящее время стала актуальна следующая разновидность данной угрозы – пользователям рассылаются на оплату мобильного телефона, домашнего интернета, ЖКХ и т.д. Зачастую мошенники направляют поддельные квитанции раньше официальной даты оплаты, чтобы успеть собрать свои платежи;

**(Слайд 39)**

* Мошенник может попросить денег в долг под видом знакомого, например, через взломанный аккаунт в социальных сетях. При этом перевести деньги он может попросить любым удобным способом – на электронный кошелек, банковскую карту, через интернет-банк.

**(Слайд 40 «Фишинговые сообщения содержат»)**

* сведения, вызывающие тревогу, или угрозы, например, закрытие ваших банковских счетов;
* обещания большой денежной выгоды с минимальными усилиями или вовсе без них;
* сведения о сделках, которые слишком хороши для того, чтобы быть правдой;
* запросы о пожертвованиях от лица благотворительных организаций после сообщений в новостях о стихийных бедствиях;
* и другую информацию.

**(Слайд 41 «Мобильное мошенничество»)**

предполагает получение смс-сообщений с незнакомых номеров, которые могут содержать:

* ссылки на фишинговые или зараженные ресурсы;
* информацию о выигрышах, которых не существует;
* ложные просьбы о помощи;
* о переводе денег на сотовый, прямые просьбы о переводе денег;
* SMS из несуществующего банка;
* просьбы перезвонить на платный номер;
* требования выкупа;
* просьбы отправить СМС, которые активируют платные услуги;
* и другую информацию.

**(Слайд 42 «Формы мобильного мошенничества»)**

Wangiri («Очень дорогой звонок») – когда человек звонит с неизвестного номера, но, как только человек берет трубку, звонок внезапно обрывается. Вы перезваниваете на неизвестный номер и попадаете на автоинформатор, задача которого – как можно дольше удержать абонента на линии, пока со счета списываются деньги;

**(Слайд 43)**

Требования выкупа – когда кто-то звонит вам с неизвестного номера, но, как только вы берете трубку, звонок внезапно обрывается. Вы перезваниваете на неизвестный номер и попадаете на автоинформатор, задача которого – как можно дольше удержать абонента на линии, пока со счета списываются деньги. Когда вам позвонили или прислали SMS с неизвестного номера с просьбой о помощи близкому человеку: не впадайте в панику, не торопитесь переводить деньги. Перезвоните родным и узнайте, все ли у них в порядке. Уточните, где находятся близкие.

**(Слайд 44 «Основные советы по борьбе с фишингом»)**

* Следи за своим аккаунтом. Если ты подозреваешь, что твоя анкета была взломана, то необходимо заблокировать ее и сообщить администраторам ресурса об этом как можно скорее;
* Используй безопасные веб-сайты, в том числе, интернет-магазинов и поисковых систем;
* Используй сложные и разные пароли. Таким образом, если тебя взломают, то злоумышленники получат доступ только к одному твоему профилю в сети, а не ко всем;
* Если тебя взломали, то необходимо предупредить всех своих знакомых, которые добавлены у тебя в друзьях, о том, что тебя взломали и, возможно, от твоего имени будет рассылаться спам и ссылки на фишинговые сайты;
* Установи надежный пароль (PIN) на мобильный телефон;
* Отключи сохранение пароля в браузере;
* Не открывай файлы и другие вложения в письмах даже если они пришли от твоих друзей. Лучше уточни у них, отправляли ли они тебе эти файлы.

**(Слайд 45 «Что делать если уже возникли проблемы?»)**

* Если СМС-подписка была оформлена, то необходимо обратиться по телефону в службу поддержки оператора и попросить отключить её;
* Если аккаунт был взломан, то необходимо заблокировать аккаунт, сообщить администрации сайта о взломе, поменять пароль к сайту, а также предупредить всех своих знакомых о том, что произошел взлом и, возможно, от вашего имени будет рассылаться спам и ссылки на фишинговые сайты;
* Если деньги или другие важные данные вашей банковой карты были предоставлены неизвестным лицам, то необходимо как можно быстрее обратиться в банк для блокировки карты и возврата средств.

**(Слайд 46 «Цифровая репутация»)**

«Цифровая репутация» - это твой имидж, который формируется из информации о тебе в интернете. Твое место жительства, учебы, твое финансовое положение, особенности характера и рассказы о близких – все это накапливается в сети.  
**(Слайд 47 «Основные советы по защите цифровой репутации»)**

* Подумай, прежде чем что-то публиковать и передавать у себя в блоге или в социальной сети;
* В настройках профиля установи ограничения на просмотр твоего профиля и его содержимого, сделай его только «для друзей»;
* Не размещай и не указывай информацию, которая может кого-либо оскорблять или обижать.

**(Слайд 48 «Авторское право»)**

Авторские права – это права на интеллектуальную собственность на произведения науки, литературы и искусства. Авторские права выступают в качестве гарантии того, что интеллектуальный/творческий труд автора не будет напрасным, даст ему справедливые возможности заработать на результатах своего труда, получить известность и признание. Никто без разрешения автора не может воспроизводить его произведение, распространять, публично демонстрировать, продавать, импортировать, пускать в прокат, публично исполнять, показывать/исполнять в эфире или размещать в Интернете.

**(Слайд 49, 50 «Спам»)**

Согласно статье 18 Федерального закона от 13.03.2006 № 38-ФЗ "О рекламе" распространение рекламы допускается только при условии предварительного согласия абонента или адресата на получение рекламы.

В свою очередь юридически спам можно определить как рекламу, распространяемую без предварительного согласия абонента или адресата.

Важно, что допускается реклама при условии предварительного согласия абонента, причем согласие должно быть не устным, а в спорных ситуациях, касающихся рассылок, распространитель обязан доказать наличие такого согласия.

Также согласно закону распространитель такой рекламы обязан немедленно прекратить распространение данной рекламы в адрес лица, обратившегося к нему с таким требованием.

**(Слайд 51)**

Для этого необходимо:

* В электронном сообщении найти кнопку «Отказаться от рассылки», пройдя по которой подтвердить отказ от получения рекламных сообщений;
* По телефону или электронной почте организации или лицу, направившему сообщение СМС или в мессенджере, сообщить о необходимости исключить из рекламной рассылки.
* Также сервисы электронной почты и мессенджеры позволяют отметить сообщение или адресата как спам или распространитель спама соответственно. Для этого необходимо выделить нужное письмо и нажать кнопку «Это спам», после чего письмо или сообщение будет перемещено в папку Спам или удалено. При этом администрация сервиса сможет отследить отправителя спама и заблокировать распространение данной информации или отправителя для других пользователей.

**(Слайд 52 «Информационные источники»)**

Надеюсь, что предоставленная информация, помогающая узнать об опасностях в Интернете и о том, как им противостоять, будет в дальнейшем полезна вам и вашим детям!

И в заключении хочется пожелать: Пусть путешествие по океану информации в Сети будет для вас приятным, увлекательным, полезным, а главное безопасным!