Информационная памятка для несовершеннолетних по вопросам кибербезопасности в сети «Интернет»

Компьютерные вирусы

Компьютерный вирус - это разновидность компьютерных программ, отличительной особенностью которой является способность к размножению (копированию). 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.

Методы защиты от вредоносных программ:

1. Используй современные операционные системы, имеющие серьёзный уровень защиты от вредоносных программ;
2. Постоянно устанавливай патчи (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;
3. Работай на своем компьютере под правами пользователя, а не администратора. Это не позволит большинству вредоносных программ инсталлироваться на твоем персональном компьютере;
4. Используй антивирусные программные продукты известных производителей, с автоматическим обновлением баз;
5. Ограничь физический доступ к компьютеру для посторонних лиц;
6. Используй внешние носители информации, такие как флешка, диск или файл из Интернета, только из проверенных источников;
7. Не открывай компьютерные файлы, полученные из ненадёжных источников. Даже те файлы, которые прислал твой знакомый. Лучше уточни у него, отправлял ли он тебе их.

Сети WI-FI

С помощью WI-Fi можно получить бесплатный интернет-доступ в общественных местах: кафе, отелях, торговых центрах и аэропортах. Так же является отличной возможностью выхода в Интернет. Но многие эксперты считают, что общедоступные WiFi сети не являются безопасными.

Советы по безопасности работы в общедоступных сетях Wi-fi

1. Не передавай свою личную информацию через общедоступные Wi-Fi сети. Работая в них, желательно не вводить пароли доступа, логины и какие-то номера;
2. Используй и обновляй антивирусные программы и брандмауэр. Тем самым ты обезопасишь себя от закачки вируса на твое устройство;
3. 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;
4. Не используй публичный WI-FI для передачи личных данных, например, для выхода в социальные сети или в электронную почту;
5. Используй только защищенное соединение через HTTPS, а не HTTP, т.е. при наборе веб-адреса вводи именно «https://»;
6. В мобильном телефоне отключи функцию «Подключение к Wi-Fi автоматически». Не допускай автоматического подключения устройства к сетям Wi-Fi без твоего согласия.

Социальные сети

Социальная сеть - это сайт, который предоставляет возможность людям осуществлять общение между собой в интернете. Чаще всего в них для каждого человека выделяется своя личная страничка, на которой он указывает о себе различную информацию, начиная от имени, фамилии и заканчивая личными фотографиями. 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.

Основные советы по безопасности в социальных сетях:

1. Ограничь список друзей. У тебя в друзьях не должно быть случайных и незнакомых людей;

2. 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;

3. 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;

4. Если ты говоришь с людьми, которых не знаешь, не используй свое реальное имя и другую личную информации: имя, место жительства, место учебы и прочее;

5. Избегай размещения фотографий в Интернете, где ты изображен на местности, по которой можно определить твое местоположение;

6. При регистрации в социальной сети необходимо использовать сложные пароли, состоящие из букв и цифр и с количеством знаков не менее 8;

7. 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.

Электронные деньги

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

Электронные деньги появились совсем недавно и именно из-за этого во многих государствах до сих пор не прописано про них в законах.

В России же они функционируют и о них уже прописано в законе, где их разделяют на несколько видов - анонимные и не анонимные. Разница в том, что анонимные - это те, в которых разрешается проводить операции без идентификации пользователя, а в не анонимных идентификации пользователя является обязательной.

Также следует различать электронные фиатные деньги (равны государственным валютам) и электронные нефиатные деньги (не равны государственным валютам).

Основные советы по безопасной работе с электронными деньгами:

1. 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;
2. Используй одноразовые пароли. После перехода на усиленную авторизацию тебе уже не будет угрожать опасность кражи или перехвата платежного пароля;
3. 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, StROng!;;
4. Не вводи свои личные данные на сайтах, которым не доверяешь.

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.

Основные советы по безопасной работе с электронной почтой:

1. Надо выбрать правильный почтовый сервис. В Интернете есть огромный выбор бесплатных почтовых сервисов, однако лучше доверять тем, кого знаешь и кто первый в рейтинге;
2. Не указывай в личной почте личную информацию. Например, лучше выбрать «музыкальный_фанат@» или «рок2013» вместо «тема13»;
3. Используй двухэтапную авторизацию. Это когда помимо пароля нужно вводить код, присылаемый по SMS;

4. Выбери сложный пароль. Для каждого почтового ящика должен быть свой надежный, устойчивый к взлому пароль;

5. Если есть возможность написать самому свой личный вопрос, используй эту возможность;

6. 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;

7. 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;

8. После окончания работы на почтовом сервисе перед закрытием вкладки с сайтом не забудь нажать на «Выйти».

Кибербуллинг или виртуальное издевательство

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

Основные советы по борьбе с кибербуллингом:

1. 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;

2. Управляй своей киберрепутацией;

3. Анонимность в сети мнимая. Существуют способы выяснить, кто стоит за анонимным аккаунтом;

4. Не стоит вести хулиганский образ виртуальной жизни. Интернет фиксирует все твои действия и сохраняет их. Удалить их будет крайне затруднительно;

5. Веди себя вежливо;

6. Игнорируй единичный негатив. Одноразовые оскорбительные сообщения лучше игнорировать. Обычно агрессия прекращается на начальной стадии;

7. Бан агрессора. В программах обмена мгновенными сообщениями, в социальных сетях есть возможность блокировки отправки сообщений с определенных адресов;

8. 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.

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. Тестирование и поиск уязвимостей в них происходит не так интенсивно, как для ПК, то же самое касается и мобильных приложений.

Современные мобильные браузеры уже практически догнали настольные аналоги, однако расширение функционала влечет за собой большую сложность и меньшую защищенность.

Далеко не все производители выпускают обновления, закрывающие критические уязвимости для своих устройств.

Основные советы для безопасности мобильного телефона:

1. Будь осторожен, ведь когда тебе предлагают бесплатный контент, в нем могут быть скрыты какие-то платные услуги;

2. Думай, прежде чем отправить SMS, фото или видео. Ты точно знаешь, где они будут в конечном итоге?

3. Необходимо обновлять операционную систему твоего смартфона;

4. Используй антивирусные программы для мобильных телефонов;

5. Не загружай приложения от неизвестного источника, ведь они могут содержать вредоносное программное обеспечение;

6. После того как ты выйдешь с сайта, где вводил личную информацию, зайди в настройки браузера и удали cookies;

7. Периодически проверяй какие платные услуги активированы на твоем номере;

8. Давай свой номер мобильного телефона только людям, которых ты знаешь и кому доверяешь;

9. Bluetooth должен быть выключен, когда ты им не пользуешься. Не забывай иногда проверять это.

Фишинг или кража личных данных

Главная цель фишинг - вида Интернет-мошенничества, состоит в получении конфиденциальных данных пользователей — логинов и паролей. На английском языке phishing читается как фишинг (от fishing — рыбная ловля, password — пароль).

Основные советы по борьбе с фишингом:

1. 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;

2. Используй безопасные веб-сайты, в том числе, интернет-магазинов и поисковых систем;

3. 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;

4. 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;

5. Установи надежный пароль (PIN) на мобильный телефон;

6. Отключи сохранение пароля в браузере;

7. 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.

ФЕДЕРАЛЬНАЯ СЛУЖБА ПО НАДЗОРУ В СФЕРЕ СВЯЗИ, ИНФОРМАЦИОННЫХ ТЕХНОЛОГИЙ И МАССОВЫХ КОММУНИКАЦИЙ
(РОСКОМНАДЗОР)

УПРАВЛЕНИЕ ПО ЗАЩИТЕ ПРАВ СУБЪЕКТОВ ПЕРСОНАЛЬНЫХ ДАННЫХ

Инструкция деятельности рабочей группы Молодежной палаты Консультативного совета при Уполномоченном органе по защите прав субъектов персональных данных «Волонтерское движение Молодежной палаты по мониторингу интернет-ресурсов на предмет наличия на них контента буллингового содержания» по выявлению интернет-ресурсов с информацией буллингового содержания
(далее – Рабочая группа Молодежной палаты)

Москва 2018

Как известно, существует несколько видов осуществления деструктивного влияния на пользователя в сети «Интернет» с целью нанести ему психологический ущерб. Наиболее распространенными из них являются кибербуллинг, кибертроллинг, кибераутинг, киберсталкинг.

В настоящей Инструкции описан механизм реагирования членов Молодежной палаты Консультативного совета при Уполномоченном органе по защите прав субъектов персональных данных в случае обнаружении ими в сети «Интернет» информации, содержащей признаки буллинга.

ДЕСТРУКТИВНОЕ ВОЗДЕЙСТВИЕ НА ЛИЧНОСТЬ В СЕТИ «ИНТЕРНЕТ»: ВИДЫ И ОТЛИЧИЯ. КИБЕРБУЛЛИНГ: ХАРАКТЕРИСТИКИ И ОСНОВНЫЕ ТИПЫ

Кибербуллинг, кибертроллинг, кибераутинг, киберсталкинг: понятия и отличия.

Говоря о столь близких понятиях, как кибербуллинг, кибертроллинг, кибераутинг, киберсталкинг отметим, что ключевым отличием является определение цели, которая лежит в основе совершения таких психологических манипуляций.

Основной целью кибертроллинга является осуществление провокации пользователей, направленной на возникновение спора между пользователями, которые изначально придерживались одной позиции, или на эскалацию коммуникативного конфликта между пользователями.

Цели кибербуллинга и кибераутинга заключаются в осуществлении травли пользователя по разным основаниям.

Кибербуллинг предполагает осуществление группой лиц, ее представителями травли одного пользователя в различной форме и по любой причине: половозрастные характеристики, национальная, расовая, религиозная принадлежность и т.д.

Кибераутинг представляет собой вид кибербуллинга и предполагает собой разглашение информации о сексуальной ориентации и гендерной идентичности другого человека без его на то согласия, что в итоге может привести к травле пользователя с нетрадиционными взглядами.

Киберсталкинг представляет собой наиболее жесткую форму прессинга в Интернете, которая направлена на преследование, слежение за жертвой.

Киберсталкинг характеризуется активным забрасыванием жертвы информацией псевдопозитивного или компрометирующего содержания.

Таким образом, по своей сути киберсталкинг представляет собой наиболее агрессивный вариант психологического воздействия и, зачастую, становится следствием кибербуллинга.

Кибербуллинг: основные характеристики кибербуллинга и его типы

Основными характеристиками кибербуллинга являются:

- неоднократность и/или периодичность осуществления деструктивных действий в отношении жертвы;
- наличие умысла принести ущерб жертве, как психологический, моральный, так и физический;
- нанесение вреда;

- злоупотребление своей силой или влиянием, положением в интернет-сообществе.

Исследователи выделяют восемь типов кибербуллинга:

1. Флейминг представляет собой обмен короткими эмоциональными репликами между двумя и более людьми, который происходит на открытых площадках в сети «Интернет» и больше похоже на информационную войну пользователей, возникшей по причине, не имеющей отношения к первоначальному предмету обсуждения. На первый взгляд, флейминг — борьба между равными, но при определенных условиях она может превратиться в неравноправный психологический террор.

2. Нападки, постоянные изнурительные атаки (харассмент) представляют собой повторяющиеся оскорбительные сообщения, направленные на жертву (например, сотни смс-сообщений на мобильный телефон, постоянные звонки), с перегрузкой персональных каналов коммуникации. Встречаются также в чатах и форумах, в онлайн-играх эту технологию чаще всего используют гриферы — группа игроков, имеющих целью не победу, а разрушение игрового опыта других участников.

3. Клевета представляет собой распространение оскорбительной и неправдивой информации. Текстовые сообщения, фото, песни, которые часто имеют сексуальный характер. Жертвами могут быть не только отдельные лица, но и целый список лиц. Например, случаются рассылки таких списков, как: «кто есть кто в школе», «кто с кем спит», а также создаются специальные «книги для критики» с шутками про знакомых.

4. Самозванство, перевоплощение в определенное лицо заключается в позиционировании преследователя в лице жертвы, используя пароль доступа жертвы к аккаунту в социальных сетях, в блоге, почте, системе мгновенных сообщений, или самостоятельно создает поддельный аккаунт жертвы с аналогичным никнеймом и осуществляет от имени жертвы негативную коммуникацию. Организация «волны обратных связей» происходит, когда с адреса (аккаунта) жертвы, поддельного аккаунта без ее ведома отправляют друзьям провокационные письма.

5. Надувательство, выманивание конфиденциальной информации и ее распространение представляет собой получение персональной информации и ее публикация в Интернете или осуществление ее передачи тем лицам, для которых она не предназначалась.

6. Отчуждение (остракизм, изоляция) представляет собой осуществление преследователем (группой преследователей) действий, направленных на исключение жертвы из процесса социального взаимодействия, группы. Онлайн-отчуждение возможно в любых типах сред, где присутствует возможность создания приватных чатов, быть включенным в черный список, то есть возможность быть исключенным из онлайн-среды. Одной из форм

проявления кибер-остракизм является также отсутствие ответа на мгновенные сообщения или электронные письма.

7. Киберпреследование — скрытое выслеживание жертвы с целью организации нападения, избиения, изнасилования и т.д.

8. Хеппислепингом является публикация, распространение в сети Интернет видеороликов с записями реальных сцен насилия без согласия жертвы, которые размещают в Интернете. Начинаясь как шутка, хеппислепинг может закончиться трагически.

ВЫЯВЛЕНИЕ КОНТЕНТА БУЛЛИНГОВОГО СОДЕРЖАНИЯ: ГДЕ ВСТРЕЧАЕТСЯ, КАК РАСПОЗНАТЬ, ЧТО ДЕЛАТЬ ЧЛЕНУ МОЛОДЕЖНОЙ ПАЛАТЫ ПРИ ОБНАРУЖЕНИИ ПОДОБНОЙ ИНФОРМАЦИИ

Кибербуллинг: где встречается?

Для осуществления кибербуллинга используются следующие площадки и возможности:

- мобильная связь (смс-сообщения);
- мобильные приложения и мессенджеры (What's App, Viber, Instagram, Badoo и т.д.);
- чаты и форумы в сети «Интернет»;
- электронная почта (рассылка сообщений);
- социальные сети (ВКонтакте, Facebook и т.д.);
- сервисы видеохостинга;
- игровые сайты и виртуальные игровые миры.

Среди представленных площадок, по данным исследования 2014 года компании Pew Research Center в 2014 году наиболее часто кибербуллинг встречается на площадках:

- социальных сетей (66% опрошенных пользователей);
- раздел комментариев на сайтах (22% пользователей);
- онлайн-игры (16% пользователей);
- персональная e-mail рассылка (16% пользователей);
- онлайн-форумы (10%);
- сайты знакомств (6%).

При этом женщины и девушки чаще сталкиваются с кибербуллингом в социальных сетях, а мужчины, в особенности, молодые мужчины - чаще упоминают онлайн-игры в качестве площадки, на которой они сталкивались с кибербуллингом.

Как распознать кибербуллинг

Любое унизительное, оскорбительное, угрожающее безопасности человека сообщение, а также видеофрагменты, фотоизображения, размещенные в сети «Интернет» без согласия жертвы, по своей сути, можно отнести к кибербуллингу.

Также к явлению кибербуллинга относится создание поддельных профилей пользователя, интернет-ресурсов, деятельность которых направлена на очернение потенциальной жертвы.

Для понимания сути явления кибербуллинга отметим, что его участниками являются следующие лица, между которыми распределены ролевые позиции:

- агрессора (обидчика);
- жертвы (пассивной или агрессивной);
- свидетеля;
- защитника (необязательный элемент коммуникации).

Примеры ситуаций, описываемых жертвами кибербуллинга и демонстрирующих наличие в сообщениях (нереиске) информации буллингового содержания

-«Мои фотографии, которые я выкладывала в группу для похудения, когда мне было лет 13, всплыли, когда мне было 15, меня шантажировали этими фотографиями»;

- «Мой бывший парень угрожал выложить мои интим-фото в Интернет, и его друзья видели эти фото»;

-«Я сталкивался с оскорблениями в комментариях на разные темы в разных сообществах от совершенно незнакомых мне людей из-за того, что их точка зрения не совпадает с моей»;

-«Незнакомый человек стал писать мне в социальной сети «Вконтакте». Присылал фото убитых животных и инвалидов, говорил, что эти фото красивее меня»;

- «Больше года надо мной издевались одноклассники и мальчики на 2 года младше, они выкладывали в Сети унижающие видео, где публично обзывали и насмехались, писали в личные сообщения, что я проститутка и т.д., хотя это неправда»;

- «Двое одноклассников дочери оставили о ней комментарии, имеющие сексуальный характер. Они опубликовали их на ресурсе Nettby»;

- «Мальчик встречался с девочкой, и на Facebook его некоторое время поливали грязью».

Алгоритм действий членов Молодежной палаты при выявлении контента буллингового содержания

При выявлении информации, содержащей признаки буллинга в социальных сетях, члену Молодежной палаты необходимо:

1. изготовить скриншот интернет-страницы, на которой размещена информация такого содержания (на скриншоте должны быть указаны: URL-адрес интернетс-страницы, дата и время изготовления скриншота);

2. обратиться в адрес администрации социальной сети, на которой размещен подобный контент:

- ВКонтакте:

Инструкция: https://vk.com/support?act=faqs&c=3&id=8842,

Форма обращения: https://vk.com/support?act=new&from=h&id=8842;

- Facebook:

Инструкция: https://ru-ru.facebook.com/help/reportabuse,

Форма обращения:

https://ru-ru.facebook.com/help/contact/274459462613911

- Instagram

Инструкция:

https://ru-ru.facebook.com/help/instagram/192435014247952?helpref=faq_content, https://help.instagram.com/443165679053819?helpref=page_content, https://help.instagram.com/446663175382270?helpref=faq_content,

Форма обращения:

https://help.instagram.com/contact/383679321740945?helpref=faq_content,

https://help.instagram.com/contact/584460464982589?helpref=faq_content

- Twitter

Инструкция:

https://help.twitter.com/ru/rules-and-policies/twitter-report-violation,

Форма обращения:

https://help.twitter.com/forms/moment_reporting, https://help.twitter.com/ru/safety-and-security/report-a-tweet, https://help.twitter.com/ru/safety-and-security/report-abusive-behavior

3. провести анализ такого сообщения на предмет наличия в нем персональных данных и, в случае их наличия, направить информационное письмо в адрес Роскомнадзора (образец письма прилагается – Приложение 1).

При выявлении информации, содержащей признаки буллинга, на иных интернет-ресурсах, члену Молодежной палаты необходимо:

1. изготовить скриншот интернет-страницы, на которой размещена информация такого содержания (на скриншоте должны быть указаны: URL-адрес интернет-страницы, дата и время изготовления скриншота);

2. провести анализ такого сообщения на предмет наличия в нем персональных данных и, в случае их наличия, направить информационное письмо в адрес Роскомнадзора (образец письма прилагается – Приложение 2).

Приложение 1
Образец письма Рабочей группы Молодежной палаты в адрес Роскомнадзора

Врио заместителя руководителя Роскомнадзора
Ю.Е. Контемирову

Уважаемый Юрий Евгеньевич!

Рабочей группой Молодежной палаты в ходе мониторинга информационно-коммуникационной сети «Интернет» был выявлен факт размещения на интернет-странице _____ (указать URL-адрес интернет-страницы) информации, содержащей признаки интернет-травли (кибербуллинга) в отношении пользователя социальной сети _____ (указать название социальной сети).

Так, на указанной интернет-странице пользователем _____ (указать ник пользователя, ссылку на его аккаунт) размещено сообщение следующего содержания: _____(процитировать сообщение с буллингом). В указанном сообщении содержатся персональные данные гражданина в объеме _____ (перечислить перечень сведений, указанных в сообщении, о пользователе).

Администратором группы является _____ (ссылка на профиль администратора, указывается, в случае, когда сообщение распространено в группе в социальной сети).

Учитывая п. 1 Положения о Федеральной службе по надзору в сфере связи, информационных технологий и массовых коммуникаций, утвержденного постановлением Правительства Российской Федерации от 16.03.2009 № 228, направляем Вам указанную информацию в качестве информирования и для принятия, при наличии оснований, соответствующих мер реагирования, направленных на удаление буллингового контента.

Приложение: на ___ л., в 1 экз. (прикладываются скриншоты интернет-страницы, подтверждающие факт распространения буллинговой информации).

С уважением,

Председатель Рабочей группы Молодежной палаты _____

Приложение 2
Образец письма Рабочей группы Молодежной палаты в адрес Роскомнадзора

Врио заместителя руководителя Роскомнадзора
Ю.Е. Контемирову

Уважаемый Юрий Евгеньевич!

Рабочей группой Молодежной палаты в ходе мониторинга информационно-коммуникационной сети «Интернет» был выявлен факт размещения на интернет-странице _____ (указать URL-адрес интернет-страницы) информации, содержащей признаки интернет-травли (кибербуллинга) в отношении посетителя интернет-ресурса.

Так, на указанной интернет-странице пользователем _____ (указать ник пользователя) размещено сообщение следующего содержания: _____(процитировать сообщение с буллингом). В указанном сообщении содержатся персональные данные гражданина в объеме _____ (перечислить перечень сведений, указанных в сообщении, о пользователе).

Администратором интернет-ресурса является _____ (информация может быть получена, в том числе, из общедоступных интернет-ресурсов Whois).

Учитывая п. 1 Положения о Федеральной службе по надзору в сфере связи, информационных технологий и массовых коммуникаций, утвержденного постановлением Правительства Российской Федерации от 16.03.2009 № 228, направляем Вам указанную информацию в качестве информирования и для принятия, при наличии оснований, соответствующих мер реагирования, направленных на удаление буллингового контента.

Приложение: на ___ л., в 1 экз. (прикладываются скриншоты интернет-страницы, подтверждающие факт распространения буллинговой информации).

С уважением,

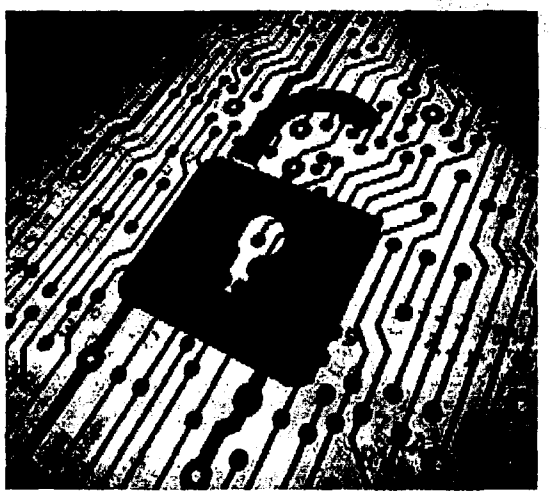
Председатель Рабочей группы Молодежной палаты _____

РОСКОМНАДЗОР

РОЛЬ И МЕСТО ЗАЩИТЫ ПРАВ СУБЪЕКТОВ ПЕРСОНАЛЬНЫХ ДАННЫХ В ОБЕСПЕЧЕНИИ КИБЕРБЕЗОПАСНОСТИ

КИБЕРУГРОЗЫ В СЕТИ ИНТЕРНЕТ

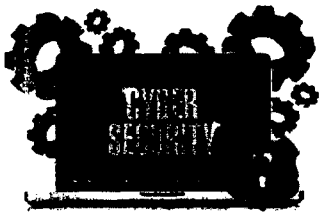
- ✓ МОШЕННИЧЕСТВО
- ✓ СЛЕЖКА
- ✓ КИБЕРБУЛЛИНГ, ТРОЛЛИНГ
- ✓ ШАНТАЖ
- ✓ ВЫМОГАТЕЛЬСТВО
- ✓ АГРЕССИВНЫЙ МАРКЕТИНГ



ИСТОЧНИКИ КИБЕРУГРОЗ

- **ПРАКТИКА ПРИНЯТИЯ** условий пользовательского соглашения по умолчанию
- **ХИЩЕНИЕ ПД**
- **ИСПОЛЬЗОВАНИЕ** «серых» мобильных приложений
- **ФИШИНГ**
- **ПОВСЕМЕСТНОЕ ИСПОЛЬЗОВАНИЕ** видеонаблюдения
- **ПЕРЕДАЧА** ПД по незащищенным каналам связи
- **ИСПОЛЬЗОВАНИЕ** геолокационных сервисов
- **РАСПРОСТРАНЕНИЕ** ПД в открытых источниках
- **ОБЩЕНИЕ** с виртуальными друзьями

ПОСЛЕДСТВИЯ КИБЕРУГРОЗ



- **ПРИСВОЕНИЕ ЛИЧНОГО ИМУЩЕСТВА ГРАЖДАН ОБМАННЫМ ПУТЁМ**
- Вред психическому, нравственному и духовному здоровью граждан
- Нарушение права на личную жизнь
- Принуждение к выполнению воли третьих лиц
- Монетизация пользователя сети Интернет, т.е. пользователь становится товаром

Манипулирование субъектом персональных данных

ПРАВОВОЕ РЕГУЛИРОВАНИЕ ЗАЩИТЫ ПРАВ СУБЪЕКТОВ ПЕРСОНАЛЬНЫХ ДАННЫХ

- **КОНВЕНЦИЯ СОВЕТА ЕВРОПЫ**
  О защите физических лиц при автоматизированной обработке персональных данных ETS № 108

- **ФЕДЕРАЛЬНЫЙ ЗАКОН РОССИЙСКОЙ ФЕДЕРАЦИИ**
  «О персональных данных»

- **ФЕДЕРАЛЬНЫЙ ЗАКОН РОССИЙСКОЙ ФЕДЕРАЦИИ**
  «Об информации, информационных технологиях и о защите информации»
  (в части порядка блокировки информации в сети Интернет)

- **ПОСТАНОВЛЕНИЕ ПРАВИТЕЛЬСТВА РОССИЙСКОЙ ФЕДЕРАЦИИ**
  «О Федеральной службе по надзору в сфере связи, информационных технологий и массовых коммуникаций»

НАРУШЕНИЯ ПОРЯДКА ОБРАБОТКИ ПЕРСОНАЛЬНЫХ ДАННЫХ В СЕТИ ИНТЕРНЕТ

- Нерегулируемый оборот информации, содержащей персональные данные
- Несоответствие обработки персональных данных декларируемым в пользовательских соглашениях Интернет-компаний целям обработки персональных данных
- Сбор и анализ персональной информации пользователей, в том числе, персонифицированной заинтересованности пользователя к определенным товарам
- Использование персональных данных пользователя сети Интернет с целью продвижения товаров, работ, услуг на рынке
- Создание фальшивых аккаунтов в социальных сетях
- Использование персональных данных в коммерческих целях
- Общедоступность личной информации

ПОЛНОМОЧИЯ РОСКОМНАДЗОРА ПО КОНТРОЛЮ ЗА СОБЛЮДЕНИЕМ ЗАКОНОДАТЕЛЬСТВА В ОБЛАСТИ ПЕРСОНАЛЬНЫХ ДАННЫХ

АИС «Реестр нарушителей прав субъектов персональных данных»

ЦЕЛЬ:

ОГРАНИЧЕНИЕ ДОСТУПА К ИНФОРМАЦИИ, ОБРАБАТЫВАЕМОЙ С НАРУШЕНИЕМ ЗАКОНОДАТЕЛЬСТВА РОССИЙСКОЙ ФЕДЕРАЦИИ В ОБЛАСТИ ПЕРСОНАЛЬНЫХ ДАННЫХ

НАЛИЧИЕ СИСТЕМЫ ПО ЗАЩИТЕ ПРАВ СУБЪЕКТОВ ПЕРСОНАЛЬНЫХ ДАННЫХ

СПОСОБСТВУЕТ

Достижению БАЛАНСА интересов
Личности, общества и государства

СОХРАНЕНИЮ

неприкосновенности ЧАСТНОЙ
ЖИЗНИ

Сохранению
психологического
Здоровья граждан