РОСКОМНАДЗОР

УПРАВЛЕНИЕ ФЕДЕРАЛЬНОЙ СЛУЖБЫ ПО НАДЗОРУ В СФЕРЕ СВЯЗИ, ИНФОРМАЦИОННЫХ ТЕХНОЛОГИЙ И МАССОВЫХ КОММУНИКАЦИЙ ПО ВОЛГОГРАДСКОЙ ОБЛАСТИ И РЕСПУБЛИКЕ КАЛМЫКИЯ
(Управление Роскомнадзора по Волгоградской области и Республике Калмыкия)

ул. Мира, д. 9, Волгоград, 400131
Телефон: (8442) 96-88-77; факс (8442) 96-88-76
E-mail: rsockanc34@rkn.gov.ru

15.10.2019 № 18479-08/34

На

Об оказании содействия

Министру образования и науки Республики Калмыкия

Н.Г. Манцаеву

А.С. Пушкина ул., д. 18,
г. Элиста, 358009

Уважаемый Николай Гаряевич!

В соответствии с ч. 1 ст. 23 Федерального закона от 27.07.2006 № 152-ФЗ «О персональных данных» и п. 1 Положения о Федеральной службе по надзору в сфере связи, информационных технологий и массовых коммуникаций (далее – Роскомнадзор), утвержденного постановлением Правительства РФ от 16.03.2009 № 228, уполномоченным органом по защите прав субъектов персональных данных является Роскомнадзор, на который возлагается осуществление функций по контролю и надзору за соответствием обработки персональных данных требованиям законодательства Российской Федерации в области персональных данных. На территории Республики Калмыкия таким органом является Управление Роскомнадзора по Волгоградской области и Республике Калмыкия.

В целях информирования несовершеннолетних о правилах защиты своих персональных данных, Роскомнадзором подготовлены информационно-методические материалы для несовершеннолетних по вопросам кибербезопасности в сети "Интернет".

Просим Вас рассмотреть возможность размещения на Вашем официальном сайте информационно-методических материалов, а также оказать содействие по размещению данных материалов на сайтах образовательных учреждений.

Просим сообщить в адрес Управления Роскомнадзора по Волгоградской области и Республике Калмыкия информацию о принятом решении.

Приложение: информационно-методические материалы на 12 л. в 1 экз.

Руководитель

В. С. Михайлов

Исполнитель: Козлова Л. В.
Тел.: (84722) 50002 доб. 806

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.

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.

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;

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.

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.

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.

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;

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.

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;

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.

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

Примеры ситуаций, описываемых жертвами кибербуллинга и демонстрирующих наличие в сообщениях (переписке) 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».

РОСКОМНАДЗОР

РОЛЬ И МЕСТО ЗАЩИТЫ ПРАВ СУБЪЕКТОВ ПЕРСОНАЛЬНЫХ ДАННЫХ В ОБЕСПЕЧЕНИИ КИБЕРБЕЗОПАСНОСТИ

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

РОСКОМНАДЗОР

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»

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