

БЕЗОПАСНОСТЬ В СЕТИ ИНТЕРНЕТ

К.ф.-м.н. Ткачев В.И.

ОСНОВНЫЕ НОРМАТИВНЫЕ ДОКУМЕНТЫ

- -Федеральный закон от 29 декабря 2010 г. № 436-ФЗ «О защите детей от информации, причиняющей вред их здоровью и развитию» (далее - Федеральный закон № 436-ФЗ).
- Федеральный закон от 28 июля 2012 г. N 139-ФЗ "О внесении изменений в Федеральный закон "О защите детей от информации, причиняющей вред их здоровью и развитию" и отдельные законодательные акты Российской Федерации"
- - Распоряжение Правительства РФ от 02.12.2015 N 2471-р «Об утверждении Концепции информационной безопасности детей»

ОСНОВНЫЕ ИНТЕРНЕТ УГРОЗЫ

- ⦿ **Контентные угрозы**
- ⦿ **Коммуникационные угрозы**
- ⦿ **Электронные угрозы**
- ⦿ **Потребительские угрозы**
- ⦿ **Возникновение интернет-зависимости**

ОСНОВНЫЕ ИНТЕРНЕТ УГРОЗЫ

Контентные угрозы

Контентные угрозы — это материалы, содержащие насилие, агрессию, эротику и порнографию, нецензурную лексику, информацию, разжигающую расовую ненависть, пропаганду анорексии и булимии, суицида, азартных игр, наркотических веществ и т.д.

ОСНОВНЫЕ ИНТЕРНЕТ УГРОЗЫ

Контентные незаконные угрозы

- ⦿ детская порнография (включая изготовление, распространение и хранение);
- ⦿ наркотические средства (изготовление, продажа, пропаганда употребления),
- ⦿ все материалы, имеющие отношение к расовой или религиозной ненависти (экстремизм, терроризм, национализм и др.), а также ненависти или агрессивного поведения по отношению к группе людей, отдельной личности или животным),
- ⦿ азартные игры и т.д.

ОСНОВНЫЕ ИНТЕРНЕТ УГРОЗЫ

Контентные неэтичные угрозы (*противоречащие принятым в обществе нормам морали и социальным нормам*)

- ⦿ широко распространенные в сети изображения сексуального характера, в том числе и порнография;
- ⦿ агрессивные онлайн игры;
- ⦿ азартные игры;
- ⦿ пропаганда нездорового образа жизни (употребление наркотиков, алкоголя, табака, анорексии, булимии);
- ⦿ принесение вреда здоровью и жизни (различных способов самоубийства, аудионаркотиков, курительных смесей);
- ⦿ нецензурная брань;
- ⦿ оскорбления, и др.

ОСНОВНЫЕ ИНТЕРНЕТ УГРОЗЫ

Коммуникационные угрозы

Коммуникационные угрозы связаны с межличностными отношениями интернет-пользователей с помощью различных чатов, онлайн-мессенджеров (ICQ, Gogletalk, Skype и др.), социальных сетей, сайтов знакомств, форумов, и т.п.

- ⦿ Киберпреследования - это преследование пользователя сообщениями, содержащими оскорбления, агрессию, сексуальные домогательства с помощью различных интернет-сервисов;
- ⦿ Незаконные контакты - это общение между взрослым и ребенком, при котором взрослый пытается установить более близкие отношения для сексуальной эксплуатации ребенка;
- ⦿ Груминг - установление дружеских отношений с ребенком с целью изнасилования;

ОСНОВНЫЕ ИНТЕРНЕТ УГРОЗЫ

Электронные угрозы

возможность хищения персональной информации, риск подвергнуться вирусной атаке, онлайн-мошенничеству, спам-атаке, шпионским программам и т.д

кибермошенничество — один из видов киберпреступления, целью этого преступления является обман пользователей. (хищение личных данных, номера банковских счетов, паспортные данные, коды, пароли и др.), для причинения материального и финансового ущерба.

ОСНОВНЫЕ ИНТЕРНЕТ УГРОЗЫ

Потребительские угрозы

Потребительские угрозы - злоупотребление в интернете правами потребителя.

- ⦿ угроза приобретения товара низкого качества;
- ⦿ контрафактная и фальсифицированная продукция, потеря денежных средств без приобретения товара или услуги;
- ⦿ хищение персональной информации с целью кибермошенничества.

ОСНОВНЫЕ ИНТЕРНЕТ УГРОЗЫ

Угроза возникновения интернет-зависимости

- ⦿ *неспособность и нежелание отвлечься даже на короткое время от интернета и, тем более, прекратить работу в нем;*
- ⦿ *досада и раздражение, возникающие при вынужденных отвлечениях, и навязчивые размышления об интернете в такие периоды;*
- ⦿ *стремление проводить за работой в интернете все увеличивающиеся отрезки времени и неспособность спланировать время окончания сеанса;*
- ⦿ *желание тратить на обеспечение работы в сети все больше денег;*
- ⦿ *готовность лгать друзьям/ членам семьи о времени работы в сети;*
- ⦿ *способность и склонность забывать при работе в интернете о домашних делах/учебе/служебных обязанностях и пр.;*
- ⦿ *стремление и способность освободиться на время работы в интернете от чувств вины, беспомощности, тревоги, обретение эмоционального подъема и т.д.*

МЕРЫ РЕГЛАМЕНТАЦИИ РАБОТЫ В СЕТИ ИНТЕРНЕТ С ЦЕЛЬЮ ОБЕСПЕЧЕНИЯ БЕЗОПАСНОСТИ. СИСТЕМЫ КОНТЕНТНОЙ ФИЛЬТРАЦИИ.

- ✓ Контентные фильтры на уровне провайдера (для образовательной организации);
- ✓ Включение функций родительского контроля для персонального компьютера в операционных системах Windows, iOS, Android;
- ✓ Специальное программное обеспечение для осуществления контентной фильтрации (SkyDNS, icensor, Kinder Gate);
- ✓ Применение функции блокировки нежелательного контента в антивирусном ПО (Антивирус Касперского, Dr.Web, InternetSecurity);
- ✓ Применение расширений для браузера (web-filter - Google Chrome, «Гогуль» Mozilla FireFox);
- ✓ Ограничения доступа к нежелательному контенту в поисковых системах с помощью функции безопасного поиска;
- ✓ Применение «Черного списка» в социальных сетях;
- ✓ Ограничение доступа средствами мобильного оператора;

МЕРЫ РЕГЛАМЕНТАЦИИ РАБОТЫ В СЕТИ ИНТЕРНЕТ С ЦЕЛЮ ОБЕСПЕЧЕНИЯ БЕЗОПАСНОСТИ. СИСТЕМЫ КОНТЕНТНОЙ ФИЛЬТРАЦИИ.

Настройки Фильтр Домены Статистика Аккаунт Поддержка

Разрешить все
Заблокировать все категории
Рекомендованные

Появилась идея?
Мы будем признательны за любые отзывы о работе сервиса. [Нажмите сюда](#) чтобы оставить отзыв.

Профиль Основной

Фильтр

Поставьте галочки на категориях сайтов, которые хотите заблокировать или выберите рекомендованные настройки в левой колонке. Нажмите кнопку "Сохранить" для применения настроек.

Сохранить

- Черные сайты
 - Агрессия, расизм, терроризм
 - Грубость, матерщина, непристойность
 - Наркотики
 - Прокси и анонимайзеры
 - Фишинг
 - Ботнеты
 - Запаркованные домены
 - Плагиат и рефераты
 - Сайты, распространяющие вирусы
- Информация для взрослых
 - Алкоголь и табак
 - Знакомства
 - Порнография и секс
 - Астрология
 - Казино, лотереи, тотализаторы
 - Сайты для взрослых
- Пожиратели трафика
 - Радио и музыка онлайн
 - Файловые архивы
 - Фотогалереи
 - Торренты и P2P-сети
 - Фильмы и видео онлайн

МЕРЫ РЕГЛАМЕНТАЦИИ РАБОТЫ В СЕТИ ИНТЕРНЕТ С ЦЕЛЬЮ ОБЕСПЕЧЕНИЯ БЕЗОПАСНОСТИ. СИСТЕМЫ КОНТЕНТНОЙ ФИЛЬТРАЦИИ.



The image shows the configuration interface for tinyFilter, a content filtering system. The interface is divided into four main sections:

- General Settings:** Features a shield icon and an option to "Enable Password Protection" with a "Set Password" button.
- Content Filter:** Includes a checked "Enable Content Filter" option, an "Advanced Settings" button, and dropdown menus for "Blocked Site", "Blocked Keyword", and "Trusted Sites". Below these are radio buttons for "Block Site", "Block Keyword", and "Trusted Site", along with an "Add" button.
- Profanity Filter:** Includes a checked "Enable Profanity Filter" option, a "Profanity Filter" dropdown menu, and an "Add" button.
- List Subscription:** Features an RSS icon, an unchecked "Enable List Subscription" option, and a "Generate Your List" button.

At the bottom of the interface, there are "Reset" and "Save" buttons.

РЕКОМЕНДАЦИИ ПО РАБОТЕ В СЕТИ ИНТЕРНЕТ

Общие рекомендации педагогам

- Проведение работ по формированию информационной культуры у детей и подростков как одной из составляющих духовной культуры общества.
- Проведение родительских собраний темы: «Компьютер: добро или зло», «Информационная компетентность: отбор компьютерных сайтов и программ для детей».
- Ознакомление родителей с видами информации, способной причинить вред здоровью и развитию несовершеннолетних, запрещенной или ограниченной для распространения на территории Российской Федерации, а также с негативными последствиями распространения такой информации.
- Проведение уроков по развитию навыков ответственного и безопасного поведения в современной информационно-телекоммуникационной среде у обучающихся («Защита прав детей в сети Интернет»).
- Формирование психологической, социальной, информационной грамотности детей для профилактики интернет-зависимости.
- Работа над собственной информационной культурой с целью осуществления компетентного диалогического общения с учащимися.
- Обучение родителей, детей и подростков правилам ответственного и безопасного пользования услугами Интернет и мобильной (сотовой) связи, другими электронными средствами связи и коммуникации, в том числе способам защиты от противоправных и иных общественно опасных посягательств в информационно-телекоммуникационных сетях.

РЕКОМЕНДАЦИИ ПО РАБОТЕ В СЕТИ ИНТЕРНЕТ

Рекомендации по работе с обучающимися

Для учащихся желание выяснить, что они могут себе позволить делать без разрешения взрослых, является абсолютно нормальным. Для обеспечения интернет-безопасности обучающихся педагогам важно:

- познакомить учащихся с ответственным, достойным поведением в Интернете;
- рассказать об основных опасностях и правилах безопасного использования сети Интернет;
- убедить никогда не выдавать личную информацию, в том числе фамилию, имя, домашний адрес, номера телефонов, название школы, адрес электронной почты, фамилии друзей или родственников, свои имена в программах мгновенного обмена сообщениями, возраст или дату рождения, по электронной почте, в чатах, системах мгновенного обмена сообщениями, регистрационных формах, личных профилях и при регистрации на конкурсы в Интернете;
- объяснить опасность личных встреч с друзьями по Интернету без присутствия взрослых;
- убедить сообщать вам, если что-либо или кто-либо в сети тревожит или угрожает им;
- ознакомить с правилами поведения на форумах и чатах, убедить их, что они не должны использовать сеть для хулиганства, распространения сплетен или угроз другим людям.

РЕКОМЕНДАЦИИ ПО РАБОТЕ В СЕТИ ИНТЕРНЕТ

Рекомендации по работе с родителями

Важной мерой для обеспечения безопасной работы в сети интернет является привлечение к этой работе родителей. Сетевая безопасность подростков - трудная задача, поскольку об Интернете они знают зачастую больше, чем их родители. Тем не менее, участие взрослых тоже необходимо:

- Необходимо помнить, что очень часто дети уходят в себя и, как следствие, уходят в виртуальный мир или попадают в сомнительную компанию, потому что не видят интереса к себе родных людей и считают, что родители не понимают их и не любят;
- Очень важно поддерживать доверительные отношения с детьми в семье;
- Беседуйте с подростками об их друзьях в Интернете и о том, чем они занимаются. Спрашивайте о людях, с которыми подростки общаются по мгновенному обмену сообщениями, и убедитесь, что эти люди им знакомы;
- Интересуйтесь, какими чатами и досками объявлений пользуются подростки, и с кем они общаются. Поощряйте использование модерируемых (контролируемых) чатов и настаивайте, чтобы они не общались с кем-то в приватном режиме;
- Настаивайте, чтобы подростки не соглашались на личные встречи с друзьями из Интернета. Напоминайте, какие опасности это может за собой повлечь;
- Убедите подростков никогда не выдавать личную информацию по электронной почте, в чатах, системах мгновенного обмена сообщениями, регистрационных формах, личных профилях и при регистрации на конкурсы в Интернете. Напоминайте, чем это может обернуться;
- Помогите подросткам защититься от спама. Научите их не выдавать в Интернете своего электронного адреса, не отвечать на нежелательные письма и использовать специальные почтовые фильтры;
- Обсудите с подростками азартные сетевые игры и связанный с ними риск.

ОБЕСПЕЧЕНИЕ
БЕЗОПАСНОСТИ В
ОБРАЗОВАТЕЛЬНОЙ
ОРГАНИЗАЦИИ

ОРГАНИЗАЦИОННО-АДМИНИСТРАТИВНЫЕ МЕРОПРИЯТИЯ

- обеспечение защиты детей от информации, причиняющей вред их здоровью и (или) развитию, посредством использования СКФ, а также путем осуществления педагогами визуального контроля работы детей в сети «Интернет»;
- - оказание организационной и методической поддержки работникам образовательной организации, в том числе путем их направления на повышение квалификации по вопросам защиты детей от информации, причиняющей вред их здоровью и (или) развитию, распространяемой посредством сети «Интернет»;
- - содействие проведению автоматизированного мониторинга использования в образовательных организациях СКФ и мониторинга организационно административных мероприятий;
- - проведение образовательных и консультационных мероприятий с родителями обучающихся с целью объяснения правил, рисков предоставления детям средств связи с выходом в сеть «Интернет», в частности, при посещении образовательного учреждения;
- - внесение отдельного положения в договор об оказании образовательных услуг, предусматривающего запрет использования личных средств связи с выходом в сеть «Интернет» или согласие родителей о снятии ответственности с руководителя образовательной организации в случае предоставления своему ребенку данного устройства при посещении образовательного учреждения.

ОРГАНИЗАЦИОННО-АДМИНИСТРАТИВНЫЕ МЕРОПРИЯТИЯ. ОТВЕТСТВЕННОСТЬ

- В соответствии со статьей 6.17 Кодекса Российской Федерации об административных правонарушениях от 30 декабря 2001 г. № 195-ФЗ руководитель образовательной организации несет ответственность за нарушение законодательства Российской Федерации о защите детей от информации, причиняющей вред их здоровью и (или) развитию.
- Вместе с тем Федеральный закон № 436-ФЗ не определяет ответственность поставщиков СКФ за ненадлежащее оказание услуги по ограничению доступа обучающихся к видам информации, распространяемой посредством сети «Интернет», причиняющей вред здоровью и (или) развитию детей, а также не соответствующей задачам образования (далее - услуга).

МЕТОДИЧЕСКИЕ РЕКОМЕНДАЦИИ

**МЕТОДИЧЕСКИЕ РЕКОМЕНДАЦИИ О РАЗМЕЩЕНИИ НА
ИНФОРМАЦИОННЫХ СТЕНДАХ, ОФИЦИАЛЬНЫХ
ИНТЕРНЕТ-САЙТАХ И ДРУГИХ ИНФОРМАЦИОННЫХ
РЕСУРСАХ ОБЩЕОБРАЗОВАТЕЛЬНЫХ ОРГАНИЗАЦИЙ И
ОРГАНОВ, ОСУЩЕСТВЛЯЮЩИХ УПРАВЛЕНИЕ В СФЕРЕ
ОБРАЗОВАНИЯ, ИНФОРМАЦИИ О БЕЗОПАСНОМ
ПОВЕДЕНИИ И ИСПОЛЬЗОВАНИИ СЕТИ "ИНТЕРНЕТ**

МЕТОДИЧЕСКИЕ РЕКОМЕНДАЦИИ

- Локальные нормативные акты в сфере обеспечения информационной безопасности обучающихся
- Нормативное регулирование
- Педагогическим работникам
- Обучающимся
- Родителям (законным представителям) Обучающихся
- Детские безопасные сайты

МЕТОДИЧЕСКИЕ РЕКОМЕНДАЦИИ

- Приложение N 1. Памятка для обучающихся об информационной безопасности детей
- Приложение №2. Информационная памятка для обучающихся для размещения на официальных интернет-ресурсах
- Приложение №3 Памятка для родителей об информационной безопасности детей