ГОСУДАРСТВЕННОЕ УЧРЕЖДЕНИЕ
ДОПОЛНИТЕЛЬНОГО ОБРАЗОВАНИЯ ВЗРОСЛЫХ
«ВИТЕБСКИЙ ОБЛАСТНОЙ ИНСТИТУТ РАЗВИТИЯ ОБРАЗОВАНИЯ»

Мониторинг социальных сетей обучающихся

Методические рекомендации

Витебск
Витебский областной институт развития образования
2025

Введение

В современном цифровом мире необходимо предусмотреть защиту обучающихся учреждений образования от негативной информации, которая может быть доступной через сеть Интернет, с целью обеспечения их защиты от различных видов насилия. Профилактическая работа в этом направлении должна иметь целью понимание обучающимися сути информационного насилия и информационной зависимости, знание методов защиты от негативного информационного воздействия, формирование у детей соответствующих установок, минимизацию рисков от пагубного влияния.

Социальные сети в Республике Беларусь

Среди используемых социальных сетей в Республике Беларусь следует назвать Вконтакте, Instagram, TikTok, Facebook, Одноклассники. Также широко распространено общение в мессенджерах Telegram, Viber, WhatsApp. В каждой социальной сети действуют свои правила регистрации и использования, с которыми необходимо ознакомиться перед созданием аккаунта. Во всех социальных сетях предусмотрена возможность жалобы администрации на публикацию, которая включает информацию, пропагандирующую различные формы насилия и противоправное поведение, а также блокировка личных сообщений от пользователей, блокировка страниц пользователей, распространяющих подобную информацию.

Общая безопасность в интернете

В первую очередь это действия мошенников, которые хотят получить финансовую или иную выгоду. Мошенники могут быть хорошо оснащены и использовать самые разные инструменты и методы – например, вирусное программное обеспечение (далее – вирусы), поддельные сайты (далее – сайт-зеркало), мошеннические письма, перехват и подбор паролей к учетным записям в социальных сетях и почтовых сервисах.

Вирусы

Вирусы могут распространяться с помощью вложенных файлов и ссылок в электронных письмах, в сообщениях в социальных сетях, на съемных носителях, через зараженные сайты. При этом сообщение с вирусом может быть получено как от постороннего человека, так и от знакомого, но уже зараженного участника социальной сети или почтовой переписки. Зараженными могут быть сайты, как специально созданные в целях мошенничества, так и обычные, но имеющие уязвимости информационной безопасности.

Вредоносные программы (вирусы, черви, «троянские кони», шпионские программы, боты и др.) могут нанести вред компьютеру и хранящимся на нем

данным. Они также могут снижать скорость обмена данными и даже использовать ваш компьютер для распространения вируса, рассылать от вашего имени спам с адреса электронной почты или профиля какой-либо социальной сети.

Рекомендации

Использовать антивирусное программное обеспечение с постоянно обновляемыми базами вирусных сигнатур.

Не открывать вложенные файлы или ссылки, полученные по электронной почте, через социальную сеть или другие средства коммуникаций в интернете, не удостоверившись, что файл или ссылка не содержит вирус.

Внимательно проверять доменное имя сайта, так как злоумышленники часто используют похожие имена сайтов, чтобы ввести жертву в заблуждение (например, www.yandex.ru – истинный сайт, www.yadndex.ru – сайт-зеркало).

Обращать внимание на предупреждения браузера о том, что сайт может угрожать безопасности компьютера.

Не подключать к своему компьютеру непроверенные съемные носители либо пользоваться антивирусным программным обеспечением, которое в принудительном порядке проверяет все съемные носители.

Не поддаваться на провокации злоумышленников, например, с требованием перевести деньги или отправить SMS, чтобы снять блокировку компьютера.

Мошеннические письма

Злоумышленники могут использовать различные методы социальной инженерии (угрозы, шантаж, игру на чувствах жертвы – например, жадности или сочувствии), чтобы выманить деньги. В таких случаях они пишут письма определенного сценария. Один из примеров – так называемые «нигерийские письма», в которых автор обещает жертве огромную прибыль взамен на небольшие накладные расходы.

Рекомендации

Внимательно изучить информацию из письма, обращая внимание на орфографическую грамотность письма. Если в письме предлагается большая выгода за незначительное вознаграждение, скорее всего, оно мошенническое.

Не открывать вложенные сообщения в таких письмах.

Игнорировать такие письма.

Получение доступа к аккаунтам в социальных сетях и других сервисах

Злоумышленники часто стремятся получить доступ к аккаунтам жертвы, например, в социальных сетях, почтовых и других сервисах. Украденные аккаунты они используют, например, для распространения спам-писем и вирусов.

Мошенники могут получить доступ к учётной записи следующими способами:

Заставить ввести свои данные на поддельном сайте.

Подобрать пароль, если он не является сложным.

Восстановить пароль с использованием «секретного вопроса» или

введенного ящика электронной почты.

Перехватить пароль при передаче по незащищенным каналам связи.

Как правило, для кражи данных об аккаунтах используются фишинговые сайты. **Фишинг** (англ, phishing, от fishing – рыбная ловля, выуживание) – вид интернет-мошенничества, целью которого является получение доступа к конфиденциальным данным пользователей – логинам и паролям. Злоумышленники создают фишинговые сайты, копирующие интерфейс известных ресурсов, а жертвы вводят на них свои логины и пароли, не понимая, что это сайты-зеркала.

Рекомендации

Использовать сложные пароли (сложные пароли состоят как минимум из 10 символов, включают буквы верхнего и нижнего регистра, цифры и специальные символы, не содержат имя пользователя и известные факты о нем).

Никому не сообщать свой пароль.

Для восстановления пароля использовать привязанный к аккаунту мобильный номер, а не секретный вопрос или почтовый ящик.

Не передавать учетные данные – логины и пароли – по незащищенным каналам связи (незащищенными, как правило, являются открытые и общедоступные Wi-Fi сети).

Внимательно проверять доменные имена сайтов, на которых вводятся учетные данные.

Обеспечение безопасности учащихся в сети Интернет

Правило 1. Установите четкие правила посещения сайтов. Определите, какие сайты они могут посещать, какие посещать нельзя. Заблокируйте доступ к неподходящим материалам. Настройте параметры безопасности вашего компьютера.

Правило 2. Помогите выбрать правильное регистрационное имя и пароль. Убедитесь в том, что они не содержат никакой личной информации. Напомните, что пароли никому нельзя передавать, за исключением лиц, которым можно доверять, например, родителям. Убедитесь, что у детей вошло в привычку выходить из своих аккаунтов, когда они используют общественные компьютеры в школе, кафе или библиотеке.

Правило 3. Объясните детям необходимость защиты их конфиденциальности в сети Интернет. Настаивайте на том, чтобы они никогда не выдавали своего адреса, номера телефона или другой личной информации; например, места учебы или любимого места для прогулки. Научите детей не выкладывать в сеть Интернет фото и видео, которые им могут навредить.

В Интернете немало сайтов, на которых можно публиковать свои комментарии, фото и видео, рассказывать о том, что с вами произошло, как вы живете и т. д. Обычно такие сервисы позволяют определить уровень доступа к вашей информации ещё до ее публикации.

Правило 4. Проверьте возрастные ограничения. Многие онлайн-

сервисы, в том числе Google, предоставляют доступ ко всем функциям только совершеннолетним. А создавать аккаунты Google могут только пользователи не моложе 13 лет.

Правило 5. Не позволяйте ребенку встречаться с онлайн-знакомыми без разрешения. Если ребенок желает встретиться с новым интернет-другом, следует настоять на сопровождении ребенка на эту встречу.

Правило 6. Научите детей ответственному поведению в Интернете. Помните золотое правило: *то, что вы не сказали бы человеку в личном общении, не стоит отправлять ему по SMS, электронной почте, в чате или комментариях на его странице*. Поговорите с детьми о том, как другие могут воспринимать их слова, и разработайте для своей семьи правила общения.

Правило 7. Настаивайте, чтобы дети уважали собственность других в Интернете. Объясните, что незаконное копирование и использование чужой работы – текста, музыки, компьютерных игр и других программ – является кражей.

Правило 8. Защитите свой компьютер и личные данные. Используйте антивирусное программное обеспечение и регулярно его обновляйте. Номер домашнего и мобильного телефона, домашний адрес не должны быть размещены в Интернете. Научите обучающихся не принимать файлы или открывать вложения в электронной почте от неизвестных людей.

Правило 9. Объясните детям, что пользователей с агрессивными проявлениями можно заблокировать в любой социальной сети, оставив жалобу администрации.

Правило 10. Помогите детям обеспечить безопасность своего игрового аккаунта. Если игрок ведет себя плохо или создает неприятности, его можно заблокировать в списке игроков и от него перестанут поступать сообщения.

Объясните, что нельзя привязывать свои личные карты для оплаты покупок в игре, отключать антивирус во время игры (если «игрушка» требует отключить антивирус, добавьте ее в исключения и играйте не отключая антивирус).

Правило 11. Напомните учащимся, что в социальной сети Вконтакте.ру функционирует 24/7 группа «Анти-КиберМоббинг», в которой можно получить консультацию в реальном времени.

Не останавливайтесь на достигнутом. Безопасность в сети Интернет требует постоянного внимания, поскольку технологии непрерывно совершенствуются. Старайтесь всё время держать руку на пульсе.

Правила пользования Wi-Fi в общественных местах

1. Для начала убедитесь, что вы подключаетесь к официальной сети того учреждения (заведения), в котором находитесь. Такие сети обычно имеют пароль или требуют минимальную авторизацию.

2. Старайтесь не посещать сайты, требующие авторизации. Оставить комментарии на форуме можно только в том случае, если вы уверены в безопасности подключения.

3. Не проводите через публичную сеть на сайтах или приложениях никаких финансовых операций.

4. После окончания работы убедитесь в том, что администратор учреждения удалил все ваши данные из своей базы данных.

Предупреждение столкновения с вредоносными программами

• Установите специальные почтовые фильтры и антивирусные системы для предотвращения заражения программного обеспечения и потери данных. Такие приложения наблюдают за трафиком и могут предотвратить как прямые атаки злоумышленников, так и атаки, использующие вредоносные приложения.

• Используйте только лицензионные программы и данные, полученные из надежных источников. Чаще всего вирусами бывают заражены пиратские копии программ, особенно игр.

• Объясните обучающимся, как важно использовать только проверенные информационные ресурсы и не скачивать нелицензионный контент.

• Периодически старайтесь полностью проверять компьютеры.

• Делайте резервную копию важных данных.

• Старайтесь периодически менять пароли от социальных сетей, электронной почты и не используйте слишком простые пароли.

Алгоритм работы учреждений образования для мониторинга социальных сетей учащихся, фиксации и реализации его результатов

Целью мониторинга социальных сетей обучающихся является выявление информации, которая может причинить вред развитию и здоровью ребёнка.

Рекомендуется на постоянной основе принимать следующие меры.

1. Изучить материалы по обеспечению безопасности при использовании сети Интернет:

- общая безопасность в Интернете;
- настройка родительского контроля;
- регистрация в социальных сетях, создание группы в социальных сетях, Google-сервисах;
- специализированные программы для осуществления контентной фильтрации и др.

2. Организовать разъяснительную работу с родителями и учащимися по безопасной работе с интернет-ресурсами, созданию форумов, блогов, групп, использованию специализированных программ.

3. Зарегистрироваться в социальных сетях, в которых присутствуют обучающиеся класса (группы), добавить их в друзья.

4. Войти в группы (сообщества), где зарегистрированы учащиеся.

5. Просматривать страницы обучающихся, обращая внимание на то, с кем они общаются, кто у них в друзьях, в каких группах (сообществах) состоят, каковы тематики этих групп, на записи на «стене» (в аккаунте).

Педагога должна насторожить:

- информация с суицидальным подтекстом, депрессивного содержания;
- пропаганда насилия;
- порнографическая и эротическая информация;
- информация агрессивного характера;
- информация наркотической тематики (изображения конопли и др.);
- информация экстремистского содержания (нацистская символика, обоснование национального или расового превосходства, призывы к уничтожению какой-либо нации, расы, религии).

7. Мониторинг социальных сетей в учреждении образования проводится 1 раз в месяц назначенными администрацией ответственными с целью выявления несовершеннолетних, вовлеченных в активные деструктивные сообщества.

8. Мониторинг социальных сетей несовершеннолетних, состоящих в банке данных подростков, требующих повышенного педагогического внимания (СОП, ИПР, относящихся к различным субкультурам, проявляющим девиантное поведение или агрессию, находящимся в трудной жизненной ситуации, и иные), проводится 2 раза в месяц.

9. Создавать группы совместно с учениками, наполняя их интересным содержанием, вовлекая учащихся в полезное для их развития общение.

10. При выявлении деструктивных проявлений, склонности к суицидальному поведению среди учащихся (наличие на странице подозрительных групп, лайки на деструктивных форумах, фотографиях и др.):

- обратить внимание на поведение ребенка в учреждении образования;
- информировать педагога-психолога, педагога социального, заместителя директора по воспитательной работе;
- осуществлять индивидуальные разъяснительные беседы с учащимися, их родителями (законными представителями).

11. Результаты мониторинга социальных сетей вносятся в журнал (форма приведена в приложении 1).

12. Рассмотреть результаты мониторинга социальных сетей в учреждениях образования на педагогических советах, совещаниях при директоре, родительских собраниях.

Работа с родителями (законными представителями) несовершеннолетних

Работа с родителями (законными представителями) включает содействие им в построении такого взаимодействия с несовершеннолетними, которое способствует управлению интернет-рисками и развитию у детей и подростков устойчивости к воздействию угроз.

Для организации работы могут быть использованы различные формы: родительские собрания, тематические встречи с участием представителей правоохранительных органов, здравоохранения и других заинтересованных, мероприятия в рамках проекта «Родительский университет», групповые и индивидуальные консультации и т.п.

Следует организовать информирование родителей (законных представителей) обучающихся по безопасному медиапотреблению, в частности, по контролю за безопасным поведением детей и подростков в сети Интернет **(Приложение).**

Важно, чтобы родители на таких мероприятиях были не просто пассивными слушателями, но и получили возможность активного участия, выработки собственной позиции и демонстрации собственного опыта решения проблемы.

Просветительская работа может быть организована и через информационные ресурсы учреждения образования, школьные СМИ, информационные бюллетени, выпуск брошюр, информационные письма родителям и т.п.

Анализ аккаунтов несовершеннолетних

Перечень социальных сетей для проведения анализа контента: Instagram, TikTok. Приоритет в анализе социальных сетей определяется возрастом ребенка. Instagram более популярен у подростков, сеть TikTok – у детей младшего школьного возраста. Несмотря на возрастные предпочтения, необходимо анализировать все доступные аккаунты несовершеннолетних в социальных сетях.

Instagram (Инстаграм) – приложение для обмена фотографиями и видеозаписями с элементами социальной сети, позволяющее снимать фотографии и видео, применять к ним фильтры, а также распространять их через свой сервис и ряд других социальных сетей. Ссылка на профиль подростка в Instagram может быть указана в другой социальной сети.

TikTok — платформа для создания и публикации коротких оригинальных видео с музыкальным сопровождением, напоминают смесь Instagram и YouTube. Общение в данных социальных сетях развито слабо. Количество подписчиков, специфика публикуемых видео и комментарии к ним могут предоставить дополнительную информацию об интересах обучающегося.

Алгоритм анализа профиля несовершеннолетнего в **Instagram**

(Инстаграм) и TikTok.

• Никнейм (имя), аватар (главное фото), информация, указанная в профиле;

• специфика сторис, сохранение сторис в актуальном состоянии;

• активность на странице, специфика публикаций (наличие или отсутствие лайков, комментариев, наличие отметок в публикациях других людей), наличие отметок обучающегося в публикациях других пользователей;

• подписки/подписчики – тематика интересов.

Приложение 1

Примерные вопросы для обсуждения на родительских собраниях по безопасному поведению детей и подростков в Интернете

I-IV классы

1. **Безопасное использование гаджетов**. Использование гаджетов в соответствии с возрастом – обучение способам поиска информации, ограничение по времени, настройки безопасности («Родительский контроль»), контроль соответствия потребляемого контента возрасту ребенка. Влияние чрезмерного использования гаджетов на психическое развитие ребенка.

2. **Опасность чрезмерной вовлеченности ребенка в информационное пространство**. Влияние киберпространства на внутрисемейные отношения. Проблема киберсоциализации. Вероятность усвоения моделей деструктивного поведения. Влияние чрезмерного медиапотребления на психическое и физическое здоровье и развитие детей.

3. **Права и обязанности родителей в контроле медиапотребления детей.** Ответственность родителей за воспитание и образование несовершеннолетних в рамках законодательства Республики Беларусь.

4. **Противоправные действия в отношении несовершеннолетних в сети Интернет.** Информирование родителей о преступлениях сексуального характера в отношении детей, вовлечении детей в деструктивные сообщества в социальных сетях, подстрекательстве к совершению противоправных действий.

V-VIII классы

1. **Деструктивные группы и сообщества социальных сетей**. Обзор деструктивных сообществ экстремистского, суицидального,

наркогенного содержания, криминально-асоциальных сообществ и других групп, содержащих информацию о немедицинском употреблении лекарственных препаратов, ПАВ, самоповреждениях и пр.

2. **Права и обязанности родителей в контроле медиапотребления детей.** Уголовная и административная ответственность родителей (законных представителей) за нарушение несовершеннолетними

детьми законодательства Республики Беларусь. Механизм привлечения родителей к ответственности.

3. **Оказание помощи подростку в кризисной ситуации.** Информирование родительской общественности об оказании социально-педагогической поддержки и психологической помощи в учреждении образования, социально-педагогических центрах, телефонах доверия.

4. **Особенности взаимоотношений со сверстниками в социальных сетях как фактор риска отклоняющегося поведения**. Кибербуллинг. Особенности общения подростков в сети Интернет. Обзор популярных социальных сетей и мессенджеров.

5. **Пусковые механизмы деструктивного поведения подростка.** Причины и факторы чрезмерной вовлеченности подростков в информационное пространство. Психологическая зрелость и персональный уровень жизнестойкости подростка, способность противостоять жизненным трудностям.

6. **Противоправные действия в отношении несовершеннолетних в сети Интернет.** Риски вовлечения подростков в преступные сообщества. Финансовые преступления в отношении несовершеннолетних. Маркеры поведения подростков, провоцирующих совершение противоправных действий в их отношении.

7. **Семейные традиции цифрового общества.** Культура потребления медиаинформации в семье. Важность живого общения членов семьи. Информационная гигиена членов семьи.

X- XI классы

1. **Самореализация старшеклассников как инструмент профилактики риска аутоагрессивного поведения.** Возможности самореализации в современном информационном обществе.

2. **Развитие осознанного медиапотребления**. Средства и приемы формирования индивидуальной культуры медиапотребления. Осознанность и контроль эмоциональной вовлеченности обучающихся в медиапотребление.

3. **Образовательный потенциал информационного пространства**. Цифровая образовательная среда и электронные базы знаний. Возможности современных информационных технологий в подготовке к прохождению итоговых испытаний, в выборе профессии и проектировании образовательной траектории.

4. **Права и обязанности родителей в контроле медиапотребления детей.** Необходимость оказания несовершеннолетним поддержки в подготовке к прохождению итоговых испытаний, в выборе профессии и проектировании образовательной траектории. Помощь родителей в выборе организации профессионального образования и прохождении процедуры поступления.

Приложение 2

Журнал учета мониторинга социальных сетей

класс _____

Классный руководитель _____

ГУО «_____»

20____ /20_____ учебный год

Журнал учёта работы по мониторингу аккаунтов обучающихся в социальных сетях

Дата мониторинга	Ф.И.О. проводившего мониторинг	Фамилия, имя обучающегося	Ссылка на аккаунт	Результат	Подпись проводившего мониторинг	Подпись представителя администрации