практика

административной работы в школе

ВЫПУСК №3
2021

ISSN 1726-0167

direktoria.org

практика
административной работы в школе

СОДЕРЖАНИЕ

3 (154), 2021

Колонка редактора

Функционирование школы

Развитие школы

Образовательный процесс

Работа с кадрами

Информатизация

Воспитательная работа

Адрес для писем:
115280, Москва, а/я 99

Адрес редакции: Москва,
1-й Автозаводский проезд, д. 4,
стр. 1, 5-й этаж.
Телефон / факс: (495) 710-30-01
http://www.praktika.direktor.ru
E-mail: praktika@direktor.ru

Современные дети рождаются, что называется, с гаджетами в руках. С раннего возраста они знакомы со Всемирной паутиной, умеют «бродить по Интернету». Когда в марте 2020 года школьники перешли на дистанционное обучение, время, которое они стали проводить в виртуальном пространстве, еще увеличилось. В связи с этим участились и случаи столкновения обучающихся с различными угрозами, которые несет Интернет. Поэтому актуализировалась проблема обеспечения информационной безопасности детства. Формирование кибербезопасности учащихся стало важной задачей не только родителей, но и школы.

Формирование основ кибербезопасности в образовательной организации

Е.Е. Ильина, учитель МКОУ «Михеевская основная общеобразовательная школа» Медынского района Калужской области

Понятие информационной безопасности детей определяется как состояние их защищенности, при котором отсутствует риск, связанный с причинением информацией вреда их здоровью и/или физическому, психическому, духовному и нравственному развитию.

Немного статистики:

- ежедневно в России в Интернет заходит более 80% всех детей, 90% от этого количества сталкивались с различными проблемами в Сети;
- за последние несколько лет средний возраст лиц, начинающих самостоятельно работать в Сети, снизился с 7 до 5 лет;
- более 50% детей, пользующихся Интернетом, посещают сайты с нежелательным контентом, а более 60% используют Сеть в развлекательных целях.

Исходя из вышесказанного, можно сделать вывод, что вопрос обеспечения информационной безопасности детей является весьма актуальным.

Нормативное регулирование информационной безопасности

Важность формирования основ кибербезопасности у школьников неоднократно подчеркивалась во многих официальных документах и в выступлениях специалистов. Формирование законодательного пространства в части обеспечения информационной безопасности обучающихся началось с 2010 года. 29 декабря 2010 года был принят Федеральный закон № 436-ФЗ «О защите детей от информации, причиняющей вред их здоровью и развитию», изменения в этот закон были внесены в мае 2017 года.

Вопросы информационной безопасности являлись приоритетными направлениями государственной политики в Национальной стратегии действий в интересах детей. Правительством РФ 2 декабря 2015 года была принята Концепция информационной безопасности детей. Во время слушаний в Совете Федерации на тему «Актуальные вопросы обеспечения информационной безопасности детей при использовании ресурсов сети Интернет» 14 марта 2014 года было принято решение о проведении ежегодного Единого урока по безопасности в сети Интернет

в образовательных организациях. В субъекты Российской Федерации направлено письмо Минобрнауки России от 28.04.2014 № ДЛ-115/03 «О направлении методических материалов для обеспечения информационной безопасности детей при использовании ресурсов сети Интернет». Нормативное регулирование информационной безопасности в образовательной организации осуществляется в соответствии со следующими документами:

- Федеральный закон от 27.07.2006 № 152 «О персональных данных»;
- Федеральный закон от 27.07.2006 № 149 «Об информации, информационных технологиях и о защите информации»;
- Федеральный закон от 28.12.2010 № 390 «О безопасности»;
- Федеральный закон от 29.12.2010 № 436 «О защите детей от информации, причиняющей вред их здоровью и развитию»;
- Федеральный закон от 02.07.2013 № 187 «О внесении изменений в отдельные законодательные акты Российской Федерации по вопросам защиты интеллектуальных прав в информационно-телекоммуникационных сетях»;
- Указ Президента РФ от 04.03.2013 № 183 «О рассмотрении общественных инициатив, направленных гражданами Российской Федерации с использованием интернет-ресурса “Российская общественная инициатива”»;
- Письмо Министерства образования и науки РФ от 03.10.2017 № 09-1995 «Методические рекомендации по проведению мероприятий по повышению правовой грамотности детей, родителей (законных представителей) и педагогических работников, участвующих в воспитании детей»;
- Письмо Министерства образования и науки РФ от 14.05.2018 № 08-1184 «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».

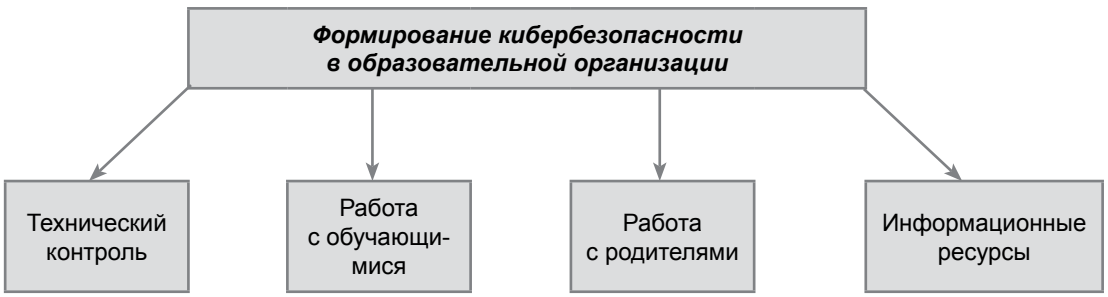
На уровне образовательного учреждения с целью организации информационной безопасности обучающихся разрабатываются и принимаются следующие локальные нормативные акты:

- программа информационной безопасности;
- инструкция по организации антивирусной защиты;
- положение о ведении электронного журнала;
- регламент работы с электронной почтой;
- классификатор интернет-безопасности;
- порядок доступа педагогов к информационно-телекоммуникационным сетям;
- инструкция для педагогических работников о порядке контроля использования обучающимися сети Интернет;
- положение об информационной открытости;
- положение об использовании сети Интернет;
- регламент работы в Интернете.

Направления работы по обеспечению кибербезопасности

Обеспечение кибербезопасности в школе проводится по нескольким направлениям (рис. 1).

Рис. 1. Обеспечение кибербезопасности в школе



Технический контроль

Технический контроль включает в себя контентную фильтрацию и антивирусные программы.

Контент-фильтр (программа ограничения веб-контента) — устройство или программное обеспечение для фильтрации сайтов по их содержимому, не позволяющее получить доступ к определенным сайтам или услугам сети Интернет. Система позволяет блокировать веб-сайты с содержимым, не предназначенным для просмотра.

Антивирусная программа — специализированная программа для обнаружения компьютерных вирусов, нежелательных программ и восстановления зараженных файлов, а также для предотвращения заражения файлов или операционной системы вредоносным кодом.

Рис. 2. Антивирусное ПО

Работа с обучающимися

Работу с обучающимися по формированию у них навыков кибербезопасности необходимо проводить на уроках информатики, классных часах и других внеклассных мероприятиях.

Примерные темы классных часов (занятий) по основам кибербезопасности

Класс	*Тема занятия*	*Содержание занятий*
2-й	Работа с файлами	1. Определение понятия «файл». 2. Перенос файла с компьютера на любой носитель информации. 3. Использование антивирусной программы для проверки файла на вирусы
3-й	Гигиена компьютера	1. Устройство компьютера. 2. Влияние пыли и влаги на функционирование компьютера. 3. Правила обращения с компьютерной техникой
4-й	Общение в сети Интернет	1. Основные программы, используемые для общения в сети Интернет. 2. Правила общения в Сети. 3. Практическая работа в одной из программ для онлайн-общения
5-й	Компьютерная зависимость. Интернет-зависимость	1. Основные приемы работы с компьютером. 2. Виды компьютерных зависимостей. 3. Инструкция «Как не попасть в компьютерную зависимость?»
6-й	Распространение компьютерных вирусов	1. Понятие «компьютерные вирусы». 2. Практические приемы работы с антивирусными программами

С 7-го класса обучающиеся начинают изучать информатику, поэтому целесообразно на некоторых уроках затрагивать тему кибербезопасности.

Рассмотрение темы кибербезопасности в курсе информатики

Класс	*Основная тема*	*Тема, касающаяся кибербезопасности*	*Задачи для учащихся на уроках*
7-й	Поиск информации. Обработка информации	Предотвращение утечки личных данных	1. Ознакомиться с каналами утечки личных данных в Интернете. 2. Изучить правила защиты личных данных. 3. Освоить основные приемы работы с ресурсами Интернета. 4. Научиться настраивать браузер
8-й	WWW-технология	Виды мошеннических действий в Сети	1. Ознакомиться с видами мошеннических действий в Интернете. 2. Освоить основные правила безопасной работы в Сети. 3. Научиться настраивать параметры безопасности своего компьютера
9-й	Локальные и глобальные компьютерные сети	Защита от вирусов, полученных из Сети	1. Ознакомиться с классификацией вирусов и другого вредоносного ПО. 2. Освоить приемы безопасной работы с ресурсами Интернета и ПК
10-й	Базы данных	Правовая охрана баз данных	1. Познакомиться с понятием авторского права и правовой защиты программ. 2. Ознакомиться с основами правовой охраны программ для компьютера и баз данных
11-й	Всемирная паутина	Настройки безопасности	1. Ознакомиться с приемами защиты в поисковых системах. 2. Научиться находить сведения о настройках безопасности веб-браузеров

Темы внеклассных мероприятий

1. Общие сведения о безопасности персонального компьютера и сети Интернет.
2. Техника безопасности и экология.
3. Интернет-зависимость — это проблема?
4. Методы обеспечения безопасности персонального компьютера. Вирусы и антивирусные программы.
5. Мошеннические действия в Сети. Киберпреступления.
6. Сетевой этикет. Интернет и психология.
7. Правовые аспекты защиты киберпространства.
8. Государственная политика в области кибербезопасности.

При проведении мероприятий в начальной и основной школе могут быть задействованы учащиеся старшего звена.

Работа с родителями (законными представителями) обучающихся

Работа с родителями (законными представителями) обучающихся включает в себя проведение родительских собраний и индивидуальное консультирование.

Тематика родительских собраний по вопросам кибербезопасности

1. Информационная безопасность детства.
2. Дети и социальные интернет-сети.
3. Опасности, подстерегающие ребенка в Сети.
4. Киберэтикет и правила поведения школьников в Интернете.
5. Виртуальные друзья. Друзья ли они?
6. О роли гаджетов в жизни ребенка.
7. Осторожно, кибершарентинг!
8. Осторожно, «группы смерти»!
9. Профилактика кибераддикции у школьников.
10. Инновации на страже безопасности ребенка.

Информационные ресурсы

К информационным ресурсам относятся:

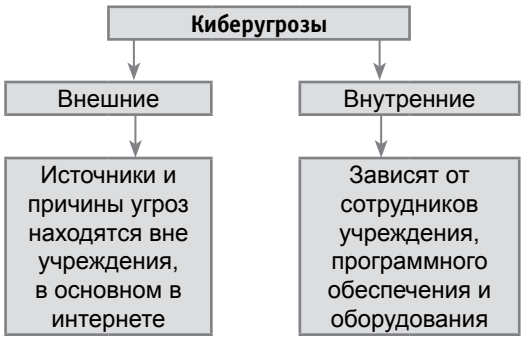
- памятки и листовки;
- классные уголки и тематические стенды;
- школьный сайт;
- специализированные сайты.

На тематических стендах и в классных уголках разме-

щается информация, посвященная вопросам кибербезопасности обучающихся. После проведения классных часов, тематических уроков или родительских собраний ученикам и их родителям (законным представителям) целесообразно раздавать листовки или памятки.
На сайте образовательной организации периодически необходимо размещать информацию о безопасном поведении в сети Интернет и ссылки на сайты, где можно узнать дополнительную информацию по теме.

Информация для оформления тематических стендов

Схема. Классификация киберугроз



Внешние угрозы:

- вирусы;
- спамовые письма;
- фишинг;
- удаленный взлом;
- кибербулинг.

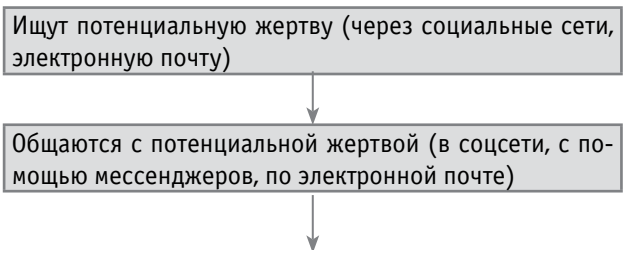
Вирусы проникают в компьютерные системы, и без эффективной защиты с ними бороться невозможно. Для распространения вирусов достаточно, чтобы ваш компьютер подключился к локальной сети, в которой есть зараженный компьютер. Вирусы могут проникать также через вложенные файлы, прикрепленные к электронному письму.
Спам способен забить каналы связи, он расходует трафик, отвлекает пользователей от работы и вынуждает искать важную и необходимую информацию среди рекламы. Спам — это один из каналов внедрения вредоносных троянских программ.
Фишинг — угроза, нацеленная на узкие группы пользователей, содержащая сообщения с социальным контекстом, которые призывают потенциальную жертву открыть исполняемый файл или перейти на сайт, содержащий вредоносный код.
За счет ***удаленного взлома*** злоумышленники получают возможность читать и редактировать документы, которые хранятся на чужих файл-серверах и компьютерах, по собственному желанию уничтожать их, внедрять собственные программы, следящие за всеми действиями пользователей и собирающие определенную информацию, вплоть до незаметного видео- и аудионаблюдения через штатные веб-камеры и микрофоны ноутбуков.
Кибербулинг — форма запугивания, насилия и травли детей с помощью телефона или сети Интернет. Жертва кибербулинга, как правило, находится в большом психологическом напряжении. Кибербулинг включает в себя:

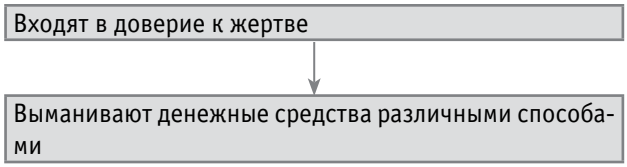
- анонимные угрозы — пересылка писем (сообщений) без указания подписи отправителя. Письма (сообщения) содержат угрозы и оскорбления, ненормативную лексику;
- преследование — рассылка писем (сообщений) продолжительное время, шантаж;
- использование личной информации — взлом страниц в социальных сетях или ящиков электронной почты с целью получения личной информации для дальнейшего шантажа или издевательства;
- флейминг — обмен эмоциональными репликами (сообщениями) между агрессором и жертвой с целью получения удовольствия от нанесения оскорблений;
- хипплейпинг — видеозаписи с издевательствами, которые в дальнейшем загружают на различные ресурсы, где их могут просматривать различные категории пользователей. Подобные видеоролики выгружаются в сеть без согласия жертвы.

Интернет-аферы

Цель интернет-аферы — выманивание денег у пользователей. Практически все злоумышленники действуют по одной схеме.

Схема действия злоумышленников





Виды интернет-афер

1. ***«Нигерийская афера»***. Пользователь получает письмо (сообщение) от незнакомца, которому необходимо перевести деньги из одной страны в другую. Потенциальной жертве обещают вознаграждение за помощь в переводе денег. После оплаты жертвой банковских расходов злоумышленник исчезает.

2. ***Лотерея***. Потенциальная жертва получает письмо (сообщение), в котором ее информируют о внушительном выигрыше. Для получения выигрыша необходимо прислать свои личные данные и оплатить банковские расходы. После оплаты банковских расходов злоумышленники исчезают.

3. ***Подружка (друг)***. Жертве приходит письмо с предложением познакомиться. Далее собеседник рассказывает, что он хотел бы побывать в вашей стране (городе). Злоумышленник договаривается с потенциальной жертвой о встрече, но в последний момент у него (нее) «внезапно» возникают финансовые трудности. Потенциальную жертву просят перевести деньги, после перевода общение прекращается, и «друг» исчезает.

4. ***Личные страницы.*** Злоумышленники похищают данные для входа на личные страницы пользователей социальных сетей, меняют логины и пароли для входа на страницу. От имени владельца страницы мошенники рассылают друзьям жертвы письма с просьбой перевести деньги. Причины для подобной просьбы могут быть самые разные (украли карту, на лечение и т.п.).

5. ***Компенсационные выплаты.*** Потенциальная жертва получает письмо (сообщение), в котором рассказывают, что можно получить какую-то компенсационную выплату (ребенку, студенту, пенсионеру, пользователю какой-то бонусной программы и т.д.). Для получения выплаты необходимо отправить свои персональные данные, в том числе и банковские реквизиты для перевода денег. Далее с личных счетов жертв списываются все денежные средства.

6. ***Ошибка.*** Пользователю, который разместил в Интернете объявление о продаже чего-либо, звонит злоумышленник и предлагает сразу перевести деньги за товар. «Покупатель» отправляет жертве копию документа о переводе денежных средств. Переведенная сумма «случайно» оказывается больше той суммы, которую необходимо было перевести. Злоумышленник просит жертву вернуть разницу. После того как жертва переводит деньги, злоумышленник исчезает. Позже обнаруживается, что перевод от «покупателя» был фиктивным, то есть разница идет в доход афериста.

Информация для оформления родительских уголков

1. ***Признаки***, на которые родителям школьника необходимо обратить внимание:
   - настроение ребенка изменилось в худшую сторону;
   - начал избегать общественных мероприятий;
   - изменилось отношение к сети Интернет;
   - изменилась реакция на приходящие сообщения;
   - удалены страницы в социальных сетях.

2. ***Советы для родителей*** о том, как обезопасить ребенка от негативного воздействия Интернета:
   - на домашнем компьютере, которым пользуется ребенок, необходимо создать отдельную учетную запись с ограниченными правами пользователя. У ребенка не должно быть возможности устанавливать и удалять программы без ведома родителей (законных представителей). Учетная запись родителя должна быть защищена паролем;
   - необходимо активировать функцию родительского контроля, включить безопасный поиск в браузерах, заблокировать нежелательные сайты (интернет-аукционы, порносайты, ряд онлайн-игр и т.д.);
   - для детей младшего школьного возраста установить специальный детский поисковик («Гогуль» или «Спутник.дети»).

3. ***О чем рассказать ребенку?***

Следует объяснить ребенку, что не всей информации, размещенной в Сети, можно доверять. Нельзя публиковать в Сети свой домашний адрес, личные данные и данные родителей, рассказывать незнакомцам о себе и своей семье, хвастаться дорогими вещами, игрушками, гаджетами.

4. ***Предупредите об опасностях***

Объясните, что нельзя общаться с посторонними людьми, сообщать им личные данные, отправлять свои фото- и видеоматериалы. Ни в коем случае нельзя ходить на встречи с незнакомцами. Научите ребенка пользоваться настройками конфиденциальности, посоветуйте закрыть профили в социальных сетях от посторонних и незнакомых пользователей. Объясните, что нужно не обращать внимания и не реагировать на киберагрессии.

Если ребенку начали писать оскорбительные письма (сообщения) с угрозами, он в первую очередь должен сказать

об этом родителям, а оппонента стоит игнорировать. Объясните, что не следует скачивать файлы с подозрительных сайтов, открывать письма (сообщения) от неизвестных отправителей, присланные ссылки. Нельзя отключать антивирусные программы. При использовании чужого устройства стоит всегда выходить из своих аккаунтов.

Памятки для обучающихся

Компьютерные вирусы

Компьютерный вирус — это **компьютерная программа.** Вирус может повредить или уничтожить файлы и данные, подконтрольные пользователю, от имени которого была запущена зараженная программа. Вирус способен уничтожить операционную систему со всеми файлами целиком.

Защита от вирусов:

- использовать современные операционные системы;
- устанавливать патчи (цифровые заплатки, устанавливающиеся с целью доработки программ);
- производить своевременное обновление операционной системы;
- использовать антивирусные программы известных производителей;
- работать на компьютере под правами пользователя, а не администратора, это не позволит большинству вредоносных программ инсталлироваться на персональном компьютере;
- ограничить физический доступ к своему компьютеру для посторонних людей;
- использовать внешние носители информации только из проверенных источников;
- не открывать файлы, полученные из ненадежных источников.

Сети Wi-Fi

Из истории: Wi-Fi не является видом передачи данных и технологией. Wi-Fi — это бренд, марка. В 1991 году нидерландская компания зарегистрировала бренд WECA, что обозначало словосочетание WirelessFidelity («беспроводная точность»).

Общедоступные сети Wi-Fi не являются безопасными.

Правила работы при использовании Wi-Fi:

- работая в общедоступных сетях, избегать ввода паролей доступа, логинов и других персональных данных;
- использовать антивирусные программы и брандмауэры, периодически обновлять программы;
- отключить функцию «общий доступ к файлам и принтерам»;
- не пользоваться публичными сетями для передачи личных данных (выход в социальные сети, использование электронной почты);
- использовать только защищенное соединение через https (при наборе веб-адреса вводите https://...);
- используя мобильные устройства, отключите функцию «Подключение к Wi-Fi автоматически».

Социальные сети

Социальные сети активно вошли в нашу жизнь, многие школьники буквально живут там. Зачастую пользователи не понимают, что информация, которая была размещена в социальных сетях, может быть найдена любым пользователем и использована кем угодно, в том числе необязательно с благими намерениями.

Советы по безопасности в социальных сетях:

- ограничьте список друзей в социальных сетях (общение только с родственниками, давними знакомыми, реальными друзьями);
- защитите свою частную жизнь: не указывайте на личной странице телефон, адрес, дату рождения и иную личную информацию;
- в переписке с незнакомыми людьми не сообщайте свое место жительства, паспортные данные и другие личные данные;
- ограничьте доступ к своей странице, в том числе к фото- и видеоматериалам. По ним можно определить ваше местоположение, уровень достатка вашей семьи, другую личную информацию;
- пользуйтесь только надежными паролями, которые состоят из букв, цифр и других знаков. Пароль для электронной почты и странички в социальных сетях должны быть различными.

Использованная литература

1. Вангородский С.Н. Основы кибербезопасности, 5–11-е классы: учебно-методическое пособие. — М.: Дрофа, 2019.

2. Поляков В.В., Кузнецов М.И., Марков В.В., Латчук В.Н. Основы безопасности жизнедеятельности. 5-й класс: учебник. — М.: Дрофа, 2019.

3. Тонких И.М., Комаров М.М., Ледовской В.И., Михайлов А.В. Основы кибербезопасности. — М.: Дрофа, 2016.

4. Учебные материалы Региональной общественной организации «Центр интернет-технологий» (РОЦИТ), 1996–2019.