Изменились требования к сайту. Готовые памятки — берите и размещайте в новом разделе

Изменились требования к сайту школы. Теперь нужно добавить новый раздел, разместить в нем локальные акты, а также памятки по информационной безопасности. Воспользуйтесь готовыми памятками → 30. Они разработаны по рекомендациям Минобрнауки.

Виктория Ярцева,
юрист-редактор
Справочной Системы
«Образование»

Создать на сайте новый раздел школам рекомендует Минобрнауки. Если этого не сделать, школу могут обвинить в том, что она не приняла меры по защите детей от вредной информации, и оштрафовать на 50 тыс. руб. (ч. 2 6.17 КоАП РФ). Чтобы избежать штрафа, создайте на официальном сайте раздел «Информационная безопасность» и включите в него шесть подразделов.

Подраздел 1. Локальные акты. Нужно опубликовать план мероприятий по обеспечению информационной безопасности учащихся и копии документов, которые регламентируют работу школы с персональными данными. Копии размещают в формате PDF. Если копии уже опубликованы в другом разделе, можно дать на него гиперссылку. Дополнительно проверьте, опубликована ли на сайте политика обработки персональных данных. Штраф за ее отсутствие в свободном доступе – 30 тыс. руб. (ч. 3 ст. 13.11 КоАП РФ).

Подраздел 2. Нормативное регулирование. В подразделе публикуют федеральные и региональные законы, письма органов власти и другие нормативные документы, которые регламентируют информационную безопасность учеников.

Документы можно опубликовать в формате PDF или дать гиперссылки на сайты органов государственной власти. Для федеральных законов используйте сайт **pravo.gov.ru**.

Разместите гиперссылки на следующие законы:

- Федеральный закон от 29.12.2010 № 436-ФЗ «О защите детей от информации, причиняющей вред их здоровью и развитию»;
- Федеральный закон от 27.07.2006 № 152-ФЗ «О персональных данных».

Подраздел 3. Педагогам. В подразделе опубликуйте методические материалы, информацию о мероприятиях, проектах и программах, которые повышают информационную грамотность педагогов. Материалы и информацию можно публиковать как текст на сайте или разместить электронные копии документов в формате PDF.

Подраздел 4. Ученикам. В подразделе публикуют памятки для учеников → **30** и информацию о мероприятиях, проектах и программах по повышению их информационной грамотности.

Подраздел 5. Родителям. В этом подразделе должны быть опубликованы памятки для родителей. Их можно скачать в тексте этой статьи на **e.rukobr.ru**. Не все родители и старшие родственники учеников владеют компьютером так, чтобы защитить детей от вредной информации или действий мошенников, поэтому опубликуйте ссылку на учебник Ростелекома **azbukainterneta.ru**.

Подраздел 6. Детские безопасные сайты. Сформировать список безопасных сайтов школе придется самостоятельно. Нужно публиковать гиперссылки на проверенные сайты, которые не содержат запрещенную информацию, не занимаются незаконным сбором персональных данных и мошенничеством ■

Электронный журнал

Скачайте 15 памяток для учеников и их родителей на **e.rukobr.ru** в тексте этой статьи

e.rukobr.ru

Внимание! Скачайте дополнительные памятки

На **e.rukobr.ru** в тексте этой статьи можно скачать 15 памяток по информационной безопасности. Если вы подписаны только на бумажный журнал, возьмите бесплатный демодоступ на три дня. В этот период вы сможете читать и скачивать материалы из любых номеров журнала, а также пользоваться сервисами, которые есть только в электронных статьях.

ПАМЯТКА для школьников

СПРАВОЧНИК РУКОВОДИТЕЛЯ ОБРАЗОВАТЕЛЬНОГО УЧРЕЖДЕНИЯ

Как безопасно общаться в социальных сетях

Рекомендовано Минобрнауки

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 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 то, что ты загружаешь? Подумай, прежде чем что-то опубликовать, написать и загрузить.

4. **Не используй реальное имя.** Когда в сети разговариваешь с незнакомыми людьми, не называй и не используй реальное имя. Не раскрывай информацию о себе: место жительства, место учебы и прочее.

5. **Не сообщай свое местоположение.** Избегай размещения фотографий в интернете, где ты изображен на местности, по которой можно определить местоположение.

6. **Используй сложные пароли.** При регистрации пиши сложные пароли. Они должны содержать не менее восьми знаков и включать в себя строчные и прописные буквы, цифры и несколько символов, такие как знак доллара, фунта, восклицательный знак.

7. **Используй разные пароли.** Для социальной сети, почты и других сайтов создавай разные пароли. Тогда если тебя взломают, то злоумышленники получат доступ только к одному месту, а не ко всем сразу.

ПАМЯТКА для школьников

Справочник руководителя образовательного учреждения

Как безопасно пользоваться электронной почтой

1. **Выбери правильный почтовый сервис.** В интернете много бесплатных. Однако почту лучше заводить на популярном сервисе, которым уже пользуются твои знакомые.

2. **Не пиши о себе в адресе почты.** Не указывай в почтовом адресе личную информацию. Например, лучше выбрать «музыкальный_фанат@» или «рок2018@» вместо «андрей2005@».

3. **Используй двухэтапную авторизацию.** Для двухэтапной авторизации помимо пароля нужно вводить код, который присылают по СМС.

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

5. **Используй проверочный вопрос.** Придумай сам свой личный вопрос для идентификации, если сервис дает такую возможность.

6. **Заведи несколько почтовых ящиков.** Первый для частной переписки с адресатами, которым ты доверяешь. Этот электронный адрес не нужно использовать при регистрации на форумах и сайтах.

7. **Не открывай вложения писем.** Не открывай файлы и другие вложения в письмах, даже если они пришли от друзей. Уточни у них, отправляли ли они тебе эти файлы.

8. **Выходите из почты.** Не забывай нажимать «Выйти» после окончания работы на почтовом сервисе, перед тем как закрыть вкладку с сайтом.

ПАМЯТКА для школьников

СПРАВОЧНИК РУКОВОДИТЕЛЯ ОБРАЗОВАТЕЛЬНОГО УЧРЕЖДЕНИЯ

Как защититься от кибербуллинга

Рекомендовано Минобрнауки

КИБЕРБУЛЛИНГ - ситуация, когда человека в Сети преследуют сообщениями, которые содержат оскорбления, агрессию, запугивание; хулиганство; социальное бойкотирование.

1. **Не бросайся в бой.** Лучший способ: посоветоваться, как себя вести, и если нет того, к кому можно обратиться, то вначале нужно успокоиться. Если ты начнешь отвечать оскорблениями на оскорбления, то только еще больше разожжешь конфликт.

2. **Управляй своей киберрепутацией.** Ищи способы выяснить, кто стоит за анонимным аккаунтом обидчика. Анонимность в Сети мнимая.

3. **Береги виртуальную честь смолоду.** Не веди хулиганский образ виртуальной жизни. Интернет фиксирует все действия и сохраняет их. Удалить их будет сложно.

4. **Игнорируй единичный негатив.** Одноразовые оскорбительные сообщения лучше игнорировать. Обычно агрессия прекращается на начальной стадии.

5. **Блокируй агрессора.** В программах обмена мгновенными сообщениями, в социальных сетях можно запретить конкретным адресам присылать сообщения.

6. **Поддержи жертву кибербуллинга.** Покажи преследователю, что оцениваешь его действия негативно. Сообщи взрослым о факте агрессивного поведения в Сети.

ПАМЯТКА для школьников

СПРАВОЧНИК РУКОВОДИТЕЛЯ ОБРАЗОВАТЕЛЬНОГО УЧРЕЖДЕНИЯ

Как защититься от компьютерных вирусов

КОМПЬЮТЕРНЫЙ ВИРУС – это программа, которая может создавать свои копии. Вирусы повреждают или уничтожают файлы на зараженном компьютере и всю операционную систему в целом. Чаще всего распространяются вирусы через интернет.

1. **Загрузи современную операционную систему.** Используй современные операционные системы с высоким уровнем защиты от вредоносных программ.

2. **Обновляй операционную систему.** Включи режим автоматического обновления операционной системы. Если в системе нет такого режима, регулярно устанавливай обновления самостоятельно. Загружай их с официального сайта разработчика.

3. **Используй права пользователя.** Работай на компьютере под правами пользователя, а не администратора. Это не позволит большинству вредоносных программ автоматически установиться.

4. **Не рискуй.** Используй антивирусные программные продукты проверенных производителей с автоматическим обновлением баз.

5. **Ограничь доступ к своему компьютеру.** Не разрешай посторонним пользоваться своим компьютером.

6. **Выбирай тщательно источники.** Копируй и загружай файлы только с проверенных съемных носителей или интернет-ресурсов. Не открывай файлы, которые получил из ненадежных источников. Даже те, которые прислал твой знакомый. Уточни у него, отправлял ли он тебе их.