ОБЕСПЕЧЕНИЕ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ В БИБЛИОТЕКЕ ОО

КОНОНОВА В.В. ДИРЕКТОР ИМБЦ АО ИОО

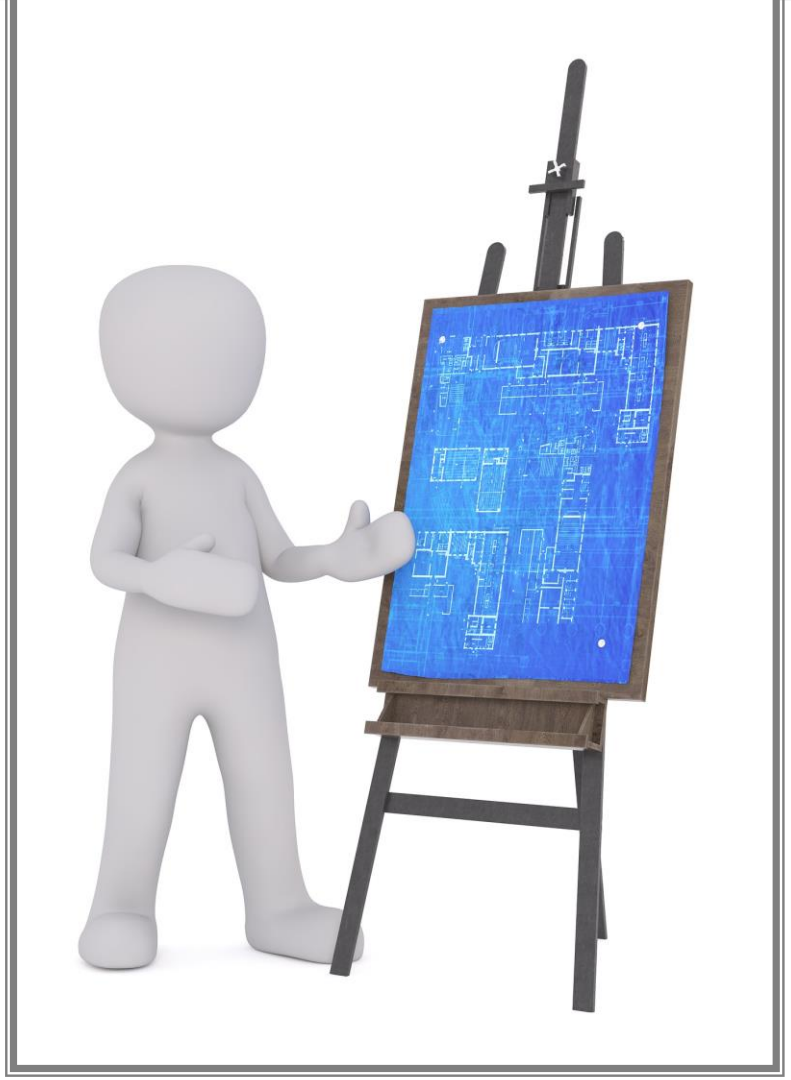
НОРМАТИВНОЕ СОПРОВОЖДЕНИЕ

ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ В БИБЛИОТЕКЕ ОО

БЕЗОПАСНОСТЬ И ДЕТИ

В настоящее время вопросам информационной безопасности уделяется большое внимание, особенно это касается безопасности детей.

Нам необходимо изучить и применять в своей работе три основополагающих документа на эту тему.



ДОКУМЕНТЫ И ССЫЛКИ

- О защите детей от информации, причиняющей вред их здоровью и развитию: федеральный закон от 29.12.2010 № 436-ФЗ: с изменениями и дополнениями
- Ссылка: http://www.Consultant.Ru/document/cons_doc_law_108808/

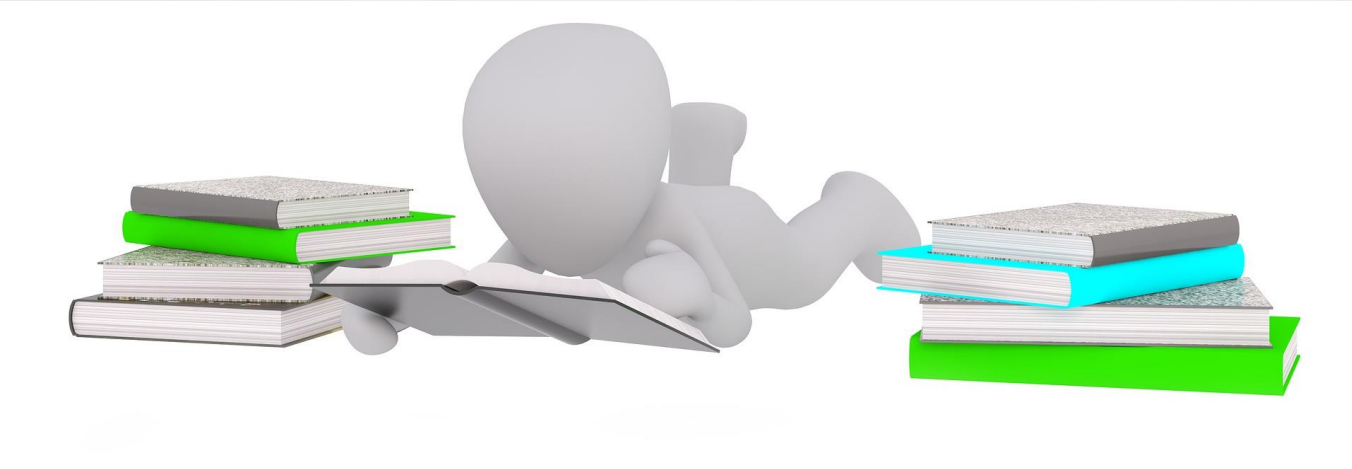
ДОКУМЕНТЫ И ССЫЛКИ

- О защите детей от информации, причиняющей вред их здоровью и развитию: федеральный закон от 29.12.2010 № 436-ФЗ: с изменениями и дополнениями
- Ссылка: http://www.Consultant.Ru/document/cons_doc_law_108808/

ДОКУМЕНТЫ И ССЫЛКИ

- Стратегия противодействия экстремизму в российской федерации до 2025 г.: Утв. Президентом РФ 28.11.2014 n пр-2753
- Доступна для скачивания по ссылке:
- Https://на.Мвд.Рф/upload/site128/document_file/strategiya_protivodeystviya_ekstremizmu_v_rossiyskoy_federaci.Pdf

- Вышеперечисленные документы изучаем самостоятельно и применяем в работе по мере необходимости.
- Особое внимание прошу уделить изучению следующего документа.



МЕТОДИЧЕСКИЕ РЕКОМЕНДАЦИИ ПО РАБОТЕ С ЛИТЕРАТУРОЙ ЭКСТРЕМИСТСКОГО ХАРАКТЕРА

- Рекомендации разработаны Минкультом РФ. Документ очень подробный и «рабочий». Несмотря на то, что разработан и рекомендован для библиотек, подведомственных министерству культуры РФ, нам следует работать с ним, поскольку министерство образования РФ подобные рекомендации для своих библиотек пока не разработало.
- Ссылка: https://legalacts.ru/doc/rekomendatsii-po-rabote-bibliotek-s-dokumentami-vkliuchennymi-v-federalnyi/

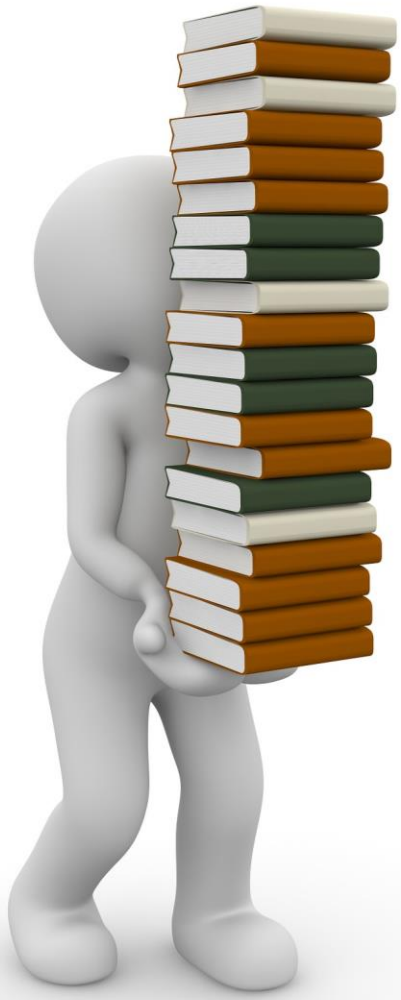
ВНИМАНИЕ!

На основе этих методических рекомендаций вам необходимо создать следующие локальные документы своей образовательной организации:

- Распоряжение о создании рабочей комиссии по сверке документов с федеральным списком экстремистских материалов
- Положение о работе рабочей комиссии по сверке документов с федеральным списком экстремистских материалов
- Журнал сверки актов наличия изданий, включенных в федеральный перечень экстремисткой литературы.
- Акты о наличии изданий, включенных в федеральный перечень экстремисткой литературы.

ВАЖНО

- Также необходимо иметь под рукой список экстремисткой литературы (его постоянное обновление происходит на Минюсте)
- Ссылка: https://minjust.Ru/ru/extremist-materials



БЕЗОПАСНОСТЬ В ИНТЕРНЕТЕ

ОСНОВНЫЕ ПРАВИЛА ЗАЩИТЫ
ОТ РАЗЛИЧНОГО ВИДА ОБМАНОВ И МОШЕННИЧЕСТВА
ПРИ РАБОТЕ В СЕТИ ИНТЕРНЕТ

РИСК №1: ПРОСТЫЕ ПАРОЛИ

Пользуйтесь паролями грамотно:

- У каждого аккаунта должен быть свой пароль;
- Он должен быть длинным (более 8 символов);
- Содержать строчные и заглавные буквы, цифры и символы;
- Его должно быть сложно подобрать (как следствие — взломать).

ХУДШИЕ ПАРОЛИ:

- Содержащие имя, фамилию, год рождения, имена детей и внуков и т.п.
- Qwerty, 123456 и им подобные
- Повторяющиеся на всех аккаунтах (тогда взлом одного аккаунта влечёт за собой цепную реакцию)
- Придуманные один раз и на всю жизнь
- Те, которые сохранили в браузере или записали на бумажке (а бумажку повесили на экран)
- **ВАЖНО!!!** Не ленитесь перелогиниваться. Нигде и никогда не ставьте галочку «сохранить пароль», тем более в общественном месте. Библиотека – тоже общественное место!

ЛУЧШИЕ ПАРОЛИ

- Те, что имеют сложную ассоциативную связь для вас лично
- Те, что не несут никакого смысла (например, thkfr#go)
  - Подобрать правильный пароль можно здесь:
  - Https://passgenerator.Ru/
  - Http://www.Onlinepasswordgenerator.Ru/
  - Https://randstuff.Ru/password/
- Часто изменяющиеся (не реже чем раз в полгода)

РИСК №2: КИБЕРБУЛЛИНГ

- **Кибербуллинг** — травля, оскорбления, угрозы от одного или нескольких агрессивно настроенных пользователей. 33% школьников либо знали о случаях кибертравли, с которым сталкивались их знакомые, либо сами становились жертвой.

КАК СЕБЯ ВЕСТИ?
(РЕКОМЕНДАЦИИ ЛАБОРАТОРИИ КАСПЕРСКОГО)

- Не реагировать ни на какие сообщения. Лучший способ свести травлю на нет — проявить безразличие к обидчикам;
- Добавить агрессоров в чёрный список в социальной сети или мессенджере;
- Сообщить о травле администратору социальной сети;
- Постараться переключиться на другие дела, пообщаться с близкими и отвлечься;
- Детям – обязательно рассказать о случившемся родителям;
- Если во время травли звучат реальные угрозы жизни и здоровью ребёнка, стоит напрямую сообщить об этом в правоохранительные органы.

РИСК №3: ОНЛАЙН-ГРУМИНГ

- Злоумышленники могут встретиться не только в тёмном переулке, но и в интернете. Больше половины школьников получают запросы в друзья от незнакомых людей в социальных сетях. При этом 34% из этих детей получают от взрослых незнакомцев предложения встретиться. А больше трети и вовсе признались, что встречались в офлайн с интернет-знакомыми. Далеко не всегда такие встречи могут закончиться дружбой.

ПРАВИЛА ПОВЕДЕНИЯ:

- Никогда не разговаривать с незнакомцами, особенно если они активно настаивают на встрече или пытаются узнать как можно больше конфиденциальной информации.
- Если решение о встрече принято, необходимо ввести правило – предупреждать о таких встречах того, кому доверяешь: друга, родителя, другого значимого взрослого
- Хорошее решение – установка приложения безопасности (такие есть у касперского, в дневнике онлайн есть и другие варианты). Важна простая мысль: это не слежка! Это – безопасность! Хороший пример могут подать родители, которые всегда предупреждают друг друга и детей о том, что задерживаются, куда идут и как скоро вернутся. Это – проявление заботы.

РИСК №4: ВРЕДОНОСНОЕ ПО

ВИРУС

- Это вредоносная программа, которая заражает компьютер или смартфон. Основная его цель — повредить, стереть информацию, или же извлечь из системы различные данные пользователя. Он попадает в систему вместе с заражённым файлом.

ЧЕРВЬ

- В отличие от вирусов, червям для распространения не требуются вмешательство человека. Заражённые червём устройства используются, например, для рассылки спама, проведения сетевых атак. Также некоторые черви могут содержать вредоносные «составляющие», предназначенные для кражи или удаления файлов.

ТРОЯН

- Вредоносная программа, которая незаметно под видом обычного софта (отсюда и название) получает доступ к информации на устройстве или его ресурсам, как в случае с троянами-майнерами криптовалют. После «установки» такой программы на устройстве злоумышленники могут шпионить за его владельцем, красть пароли или превращать компьютер в источник спама и многое другое.

КЕЙЛОГГЕР

- «Клавиатурный шпион», который собирает всю информацию, которую пользователь вводит при помощи клавиатуры. Таким образом легко увести всевозможные логины, пароли, номера и pin-коды банковских карт, серии и номера документов.

РЕКЛАМНОЕ ПО ИЛИ ADWARE

- Это программы, которые без согласия пользователя непрерывно открывают рекламные баннеры, изменяют настройки браузера, перенаправляют набранные url-адреса на рекламные страницы. Это не вредоносные программы, но весьма неприятные, поэтому относятся к категории нежелательного ПО.

РИСК № 5: МОШЕННИЧЕСТВО

- Видов мошенничества существует великое множество. Самые распространённые, к сожалению, наживаются на нашем желании помочь ближнему. Часты ложные сборы на оплату тяжёлых заболеваний, переводов на содержание приютов для бездомных животных, сбор денег на помощь погорельцам или жертвам стихийных бедствий и терактов. Какие же виды мошенничества самые «популярные»?

СОЦИАЛЬНАЯ ИНЖЕНЕРИЯ

- Злоумышленники получают доступ к аккаунту одного из ваших друзей в социальной сети. Далее они пишут жалостливое письмо всем адресатам: автокатастрофа с близкими, срочный платеж кредита, тяжелая болезнь и так далее, не брезгуя ничем. Цель одна – получить денег.
- Другой вариант: вам звонят из банка с сообщением о том, что по вашей карте проходит подозрительная транзакция и просят подтвердить все данные карты, включая cvv-код. Разумеется, если человек теряется и сообщает всю информацию, данные его карты оказываются у злоумышленников.

ФИШИНГ

- Вы получаете письмо, не вызывающее подозрений: знакомый интерфейс проверенного сайта, страницы оплаты надёжного банка, интернет-магазина, где вы уже совершали покупки. Например, крупный бренд предлагает принять участие в платном опросе — для этого надо лишь ввести все данные с банковской карты, чтобы они смогли перевести на неё деньги. В результате пользователь не только не получит обещанное вознаграждение, но и может лишиться оставшихся накоплений на карточке.

КРУПНЫЙ ВЫИГРЫШ В ОБМЕН НА «КОМИССИЮ»

- Сегодня популярны розыгрыши среди знаменитостей и крупных брендов. Бывает так, что пользователю обещают солидную сумму за участие в розыгрыше или за прохождение опроса. Тех, кто согласится поучаствовать, мошенники сначала попросят предоставить личную информацию, а затем предложат внести «комиссию» или «сервисный сбор» (обычно небольшой, чтобы не вызывать подозрений), чтобы получить деньги. Увы, после этого пользователь не только не получает выигрыш, но и прощается с «комиссией», или ещё хуже — его данные, в том числе платёжные, оказываются в руках злоумышленников.

КАК С ЭТИМ БОРОТЬСЯ?

- Не переходить по подозрительным ссылкам в почте, соцсетях, мессенджерах, даже если их прислали знакомые люди;
- Проверять информацию: если человек действительно ваш друг, у вас наверняка есть его номер телефона. Позвоните, поинтересуйтесь, всё ли у него в порядке. И пусть выяснится, что у него всего лишь взломали аккаунт, а с ним и его близкими всё хорошо;
- Проверять наличие замочка в адресной строке, если указываете конфиденциальные данные, в том числе от банковской карты;
- Не скачивать файлы, которые вам отправляют незнакомые адресаты;
- Избегать контента на пиратских сайтах: такой софт небезопасен;
- Помнить о том, что если что-то кажется слишком заманчивым, скорее всего — это обман.

БЕЗОПАСНЫЙ ИНТЕРНЕТ: РЕСУРСЫ

- Безопасность от МВД (короткий поиск: мвд.рф/безопасный-интернет-детям) https://мвд.Рф/%D0%B1%D0%B5%D0%B7%D0%BE%D0%BF%D0%B0%D1%81%D0%BD%D1%8B%D0%B9-%D0%B8%D0%BD%D1%82%D0%B5%D1%80%D0%BD%D0%B5%D1%82-%D0%B4%D0%B5%D1%82%D1%8F%D0%BC
- Безопасность от Яндекса https://yandex.Ru/support/common/security/

БЕЗОПАСНЫЙ ИНТЕРНЕТ: ЛИТЕРАТУРА

- Ефимова Л.Л. «Информационная безопасность детей»
- Цветкова М.С., Якушина Е.В. «Информационная безопасность/правила безопасного интернета». Пособие для 2-4 классов
- Цветкова М.С., Якушина Е.В. «Информационная безопасность/безопасное поведение в сети интернет». Пособие для 5-6 классов
- Цветкова М.С., Хлобыстова И.Ю. «Информационная безопасность/кибербезопасность». Пособие для 7-9 классов
- Министерство образования и науки РФ ФГБНУ «центр защиты прав и интересов детей». Памятка для родителей «родителям о психологической безопасности детей и подростков». Москва, 2018