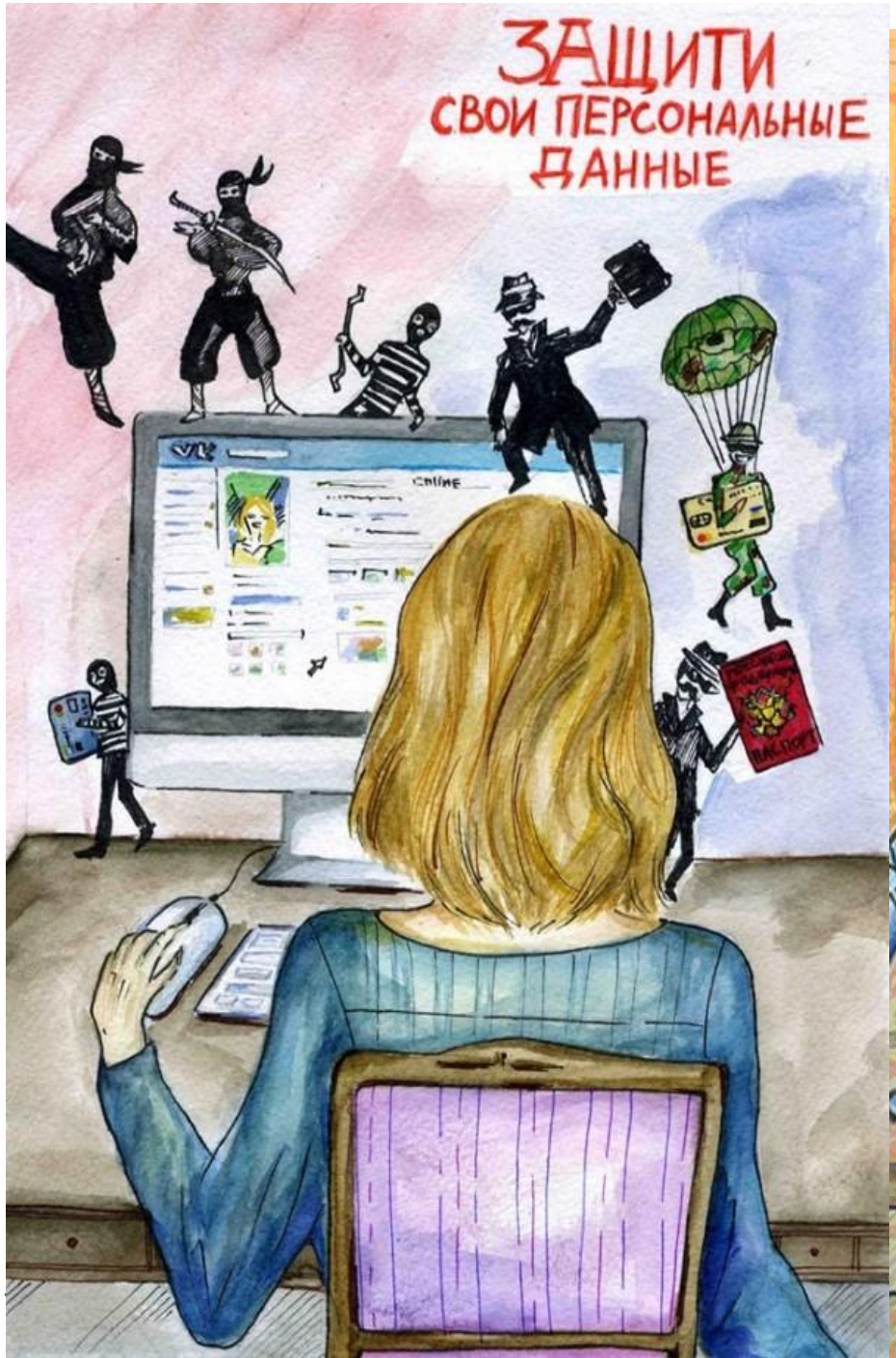
Безопасность в глобальной Сети. Защити свои персональные данные

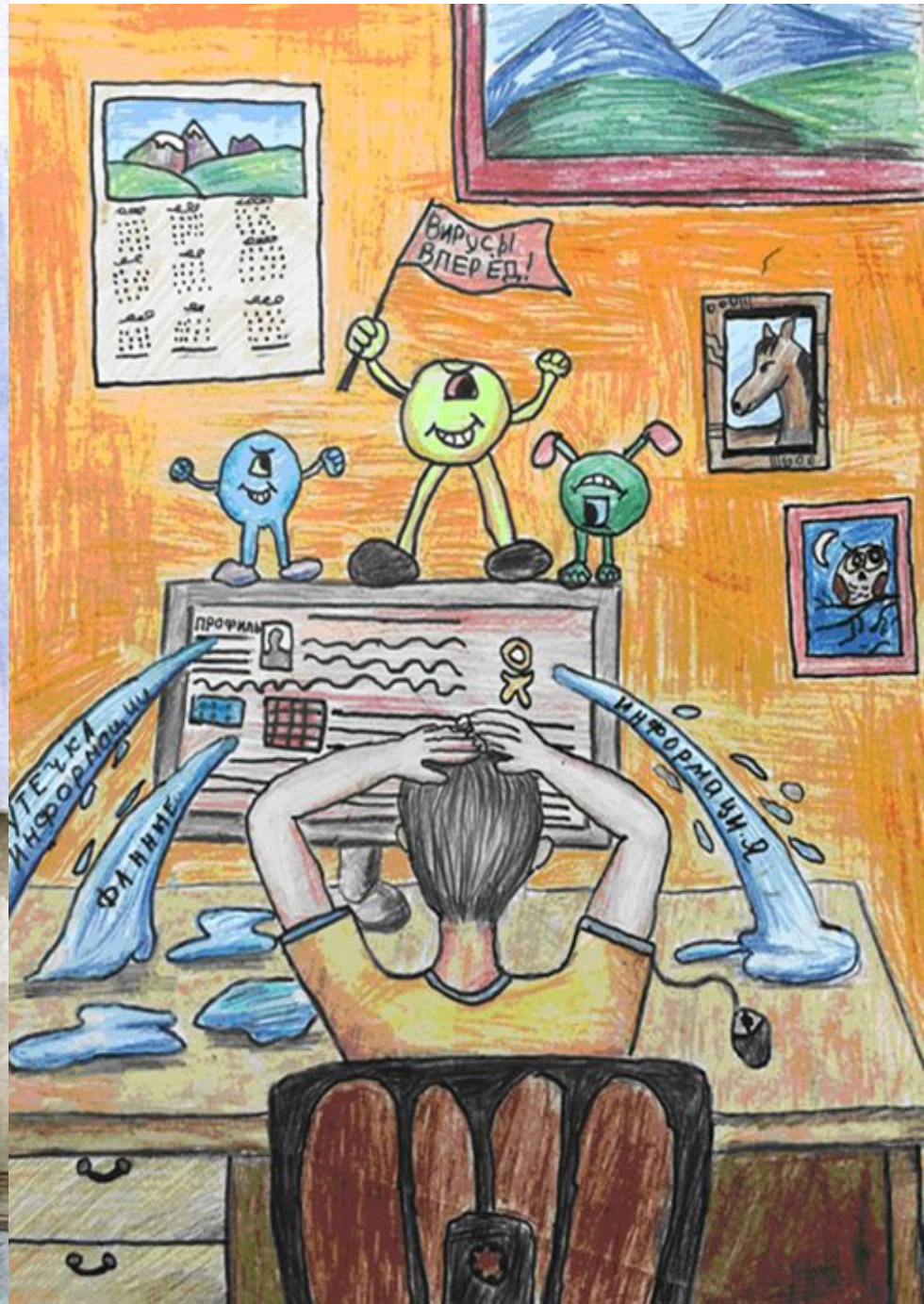
Классные часы(5-6 классы)

Октябрь 2021 года

СПАМ
Кибермошенники
СИНИЙ КИТ
Вирусы
БЕЗОПАСНОСТЬ
В СЕТИ ИНТЕРНЕТ

✓ Пользуйся аватаром и ником
✓ Установи антивирус
✓ Регулярно проверяй программное обеспечение
✓ Не запускай незнакомые программы
Запомни правила защиты персональных данных!
✓ Не используй один пароль на все ресурсы
«Защити свои персональные данные»

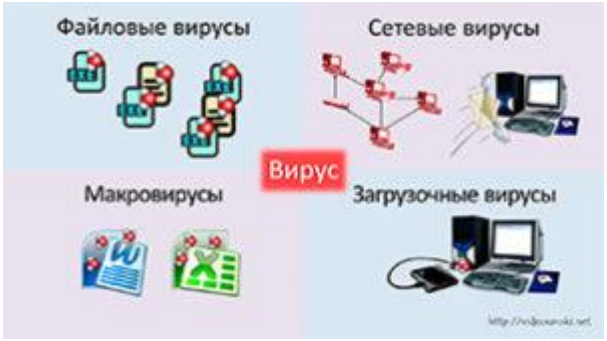

ЗАЩИТИ
СВОИ ПЕРСОНАЛЬНЫЕ
ДАННЫЕ


ВИРУСЫ ВПЕРЕД!
ПРОФИЛЬ
ОК
ТЕЧЬКА ИНФОРМАЦИИ
ФАЙЛЫ
ИНФОРМАЦИЯ

Защити свои данные
от супостата
в киеве
используй
аватарку
и придумай
ник
никому
не сообщай
личные данные
придумай
сложный
пароль
)Y>XSsj,+g~*
используй
защищенный
браузер
при
совершении
покупок
в интернете
установи
анти
вирус

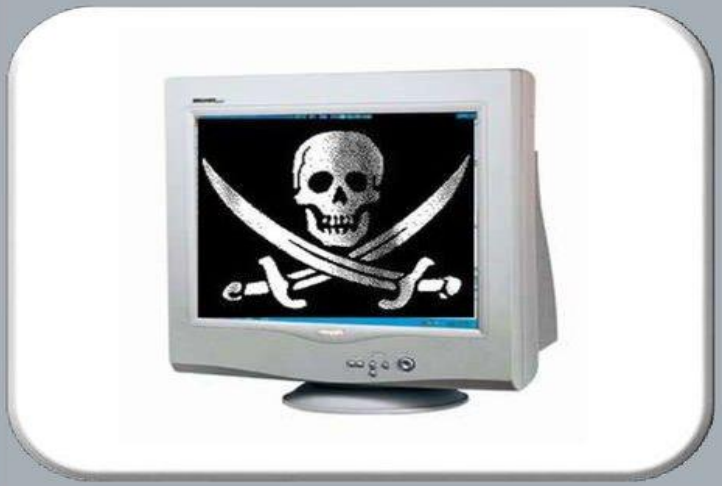
Вредоносная программа (другие термины: **зловредная программа**, **вредонос, зловред**; англ. *malware* — контаминация слов ***mal****icious* и *soft****ware***) — любое программное обеспечение, предназначенное для получения несанкционированного доступа к вычислительным ресурсам самой ЭВМ или к информации, хранимой на ЭВМ, с целью несанкционированного использования ресурсов ЭВМ или причинения вреда (нанесения ущерба) владельцу информации, и/или владельцу ЭВМ, и/или владельцу сети ЭВМ, путём копирования, искажения, удаления или подмены информации. Многие антивирусы считают крэки (кряки), кейгены и прочие программы для взлома приложений вредоносными программами, или потенциально опасными.

На жаргоне некоторых специалистов вредоносные программы называются также термином «*вирус*».



Фи́шинг (англ. *phishing* от *fishing* «рыбная ловля, выуживание») — вид интернет-мошенничества, целью которого является получение доступа к конфиденциальным данным пользователей — логинам и паролям. Это достигается путём проведения массовых рассылок электронных писем от имени популярных брендов, а также личных сообщений внутри различных сервисов, например, от имени банков или внутри социальных сетей. В письме часто содержится прямая ссылка на сайт, внешне неотличимый от настоящего, либо на сайт с редиректом. После того как пользователь попадает на поддельную страницу, мошенники пытаются различными психологическими приёмами побудить пользователя ввести на поддельной странице свои логин и пароль, которые он использует для доступа к определённому сайту, что позволяет мошенникам получить доступ к аккаунтам и банковским счетам.

Онлайн-пиратство



- незаконное копирование музыки, видео и игр – это кража, уважайте чужую собственность

Интернет-хулиганство

- нельзя использовать сеть для хулиганства, распространения сплетен или угроз другим людям, уважайте других пользователей

Персональные данные – это любая информация, относящаяся к прямо или косвенно определенному или определяемому физическому лицу (субъекту персональных данных).

Это та информация, которая позволяет нам узнать человека в толпе, идентифицировать и определить как конкретную личность. Идентифицирующих данных огромное множество, к ним относятся:

1. Фамилия, имя, отчество
2. Дата и место рождения
3. Адрес места жительства и номер телефона
4. Адрес электронной почты
5. Фотографии и многое другое

ПОМНИТЕ!

● После публикации информации в Интернете ее больше НЕВОЗМОЖНО будет контролировать и удалять каждую ее копию

ПРОВЕРЯЙТЕ!

● Всегда удостоверяйтесь в том, что Вам известно, кому предоставляется информация, и Вы понимаете, в каких целях она будет использоваться

ДУМАЙТЕ!

● Благоразумно ли размещать личную информацию на собственном веб-сайте, если невозможно быть уверенным в целях ее использования?

ОБРАЩАЙТЕ ВНИМАНИЕ!

● Имена студентов, их фотографии и другая личная информация с классного журнала может публиковаться на веб-сайте техникума только с согласия студентов и их родителей

Как защитить персональные данные в Сети:

- Ограничьте объем информации о себе, находящейся в Интернете. Удалите лишние фотографии, видео, адреса, номера телефонов, дату рождения, сведения о родных и близких и иную личную информацию
- Не отправляйте видео и фотографии людям, с которыми вы познакомились в Интернете и не знаете их в реальной жизни
- Отправляя кому-либо свои персональные данные или конфиденциальную информацию, убедитесь в том, что адресат – действительно тот, за кого себя выдает

Как защитить персональные данные в Сети:

- Если в сети Интернет кто-то просит предоставить Ваши персональные данные, например, место жительства или наименование техникума, группы, иные данные, посоветуйтесь с родителями, педагогом или взрослым человеком, которому Вы доверяете
- Используйте только сложные пароли, разные для разных учетных записей и сервисов. Старайтесь периодически их менять
- Заведите себе два адреса электронной почты – частный, для переписки (приватный и малоизвестный, который Вы никогда не публикуете в общедоступных источниках), и публичный – для открытой деятельности (форумов, чатов и т.д.)

Что делать, если вы обнаружили в Интернете оскорбительные тексты о себе или о своих фотографиях

- Сохраните все страницы, на которых найден это материал, для последующих действий
- Если по сайту или его адресу можно определить поставщика услуг, необходимо связаться с ним. Поставщик услуг может удалить текст и, вероятно, раскрыть личность автора. Кроме того, можно попросить собственного оператора Интернета связаться с администратором данного сайта и запросить удаление материалов
- Если администратор сайта отказался вам помочь, прекратите пользоваться таким ресурсом и удалите оттуда свои данные
- Если оскорбление очень серьезное и является преступлением, обратитесь в полицию

- Кроме того, можно настроить параметры программы работы с электронной почтой так, чтобы сообщения от определенного отправителя поступали в отдельную папку (спам). В этом случае их можно не читать
- Если известен адрес электронной почты отправителя, оскорбившего Вас, можно отправить копию злонамеренного сообщения поставщику услуг Интернета и попросить его удалить этот адрес электронной почты
- Если адрес электронной почты отправителя неизвестен, обратитесь за помощью к поставщику услуг Интернета.

- http://персональныеданные.дети/ - здесь вы найдете различные материалы, которые были разработаны специалистами Роскомнадзора, не только для педагогов и родителей, которые хотят помочь детям понять важность конфиденциальности личной жизни при использовании цифровых технологий, но также для молодых людей, которые с легкостью и энтузиазмом использую сеть Интернет

КАК ОБЕСПЕЧИТЬ СОБСТВЕННУЮ
БЕЗОПАСНОСТЬ В ИНТЕРНЕТЕ

Общаетесь в социальных сетях Facebook, Twitter, Instagram, Вконтакте или других

	Никогда не выкладывайте в общем доступе:		Не стоит размещать на своей страничке:
	дату и место рождения — эти данные могут сделать доступным номер Вашей карты социального страхования		откровенные признания и фотографии — работодатели и кадровые агентства часто интересуются личными данными соискателей
	планы на отпуск — можно спровоцировать ограбление		рассказы о своем рискованном поведении или хобби — страховые компании могут отказать Вам в страховке или повысить оплату за нее
	домашний адрес и номер мобильного телефона — гость или собеседник могут оказаться незванными		жалобы на работодателя или коллег по работе — за резкие высказывания могут уволить
	девичью фамилию Вашей мамы или название любимой песни — эти данные часто служат «ключом» при получении банковской карточки или подсказкой к паролю в аккаунте		грубости, оскорбления, матерные слова—читать такие высказывания так же неприятно, как и слышать

Сетевой этикет, ***сетикет***, ***нетикет***
(от англ. *net* «сеть» + фр. *etiquette* «этикет») — неологизм правил поведения, общения в Сети, традиции и культуры интернет-сообщества, которых придерживается большинство.

Дополнительные пожелания

- Обсудите со взрослыми и друзьями опасные последствия предоставления личной информации
- Пользователям НИКОГДА не следует сообщать пароли НИКОМУ, даже давним друзьям, и периодически пароль менять
- Интернет является общественным местом. Перед публикацией любой информации или фотографий следует помнить, что любой сможет получить к ним доступ. Чтобы выяснить, какая информация о Вас доступна в Сети, используйте поисковый модуль и в качестве поискового слова введите собственное имя
- Если вы получили отрицательный опыт размещения информации в сети Интернет, поговорите об этом со взрослыми