

ИНФОРМАТИКА

9

класс

ИНФОРМАЦИОННОЕ ОБЩЕСТВО: ВОЗМОЖНОСТИ И ПРОБЛЕМЫ

ИНФОРМАЦИОННО-КОММУНИКАЦИОННЫЕ
ТЕХНОЛОГИИ В СОВРЕМЕННОМ ОБЩЕСТВЕ

КЛЮЧЕВЫЕ СЛОВА

- ◆ информационное общество
- ◆ информационная этика
- ◆ информационное право
- ◆ информационная безопасность
- ◆ защита информации

ИНФОРМАЦИОННОЕ ОБЩЕСТВО

Информационное общество — современный этап развития цивилизации, когда главную роль играют информация и информационно-коммуникационные технологии (ИКТ).

- ◆ Возрастает роль информации
- ◆ Возрастает число людей, работающих в сфере ИКТ
- ◆ Разворачиваются процессы цифровой трансформации многих сфер нашей жизни



ИНФОРМАЦИОННОЕ ОБЩЕСТВО

Жизнь человека в обществе подчиняется нормам этики и права.

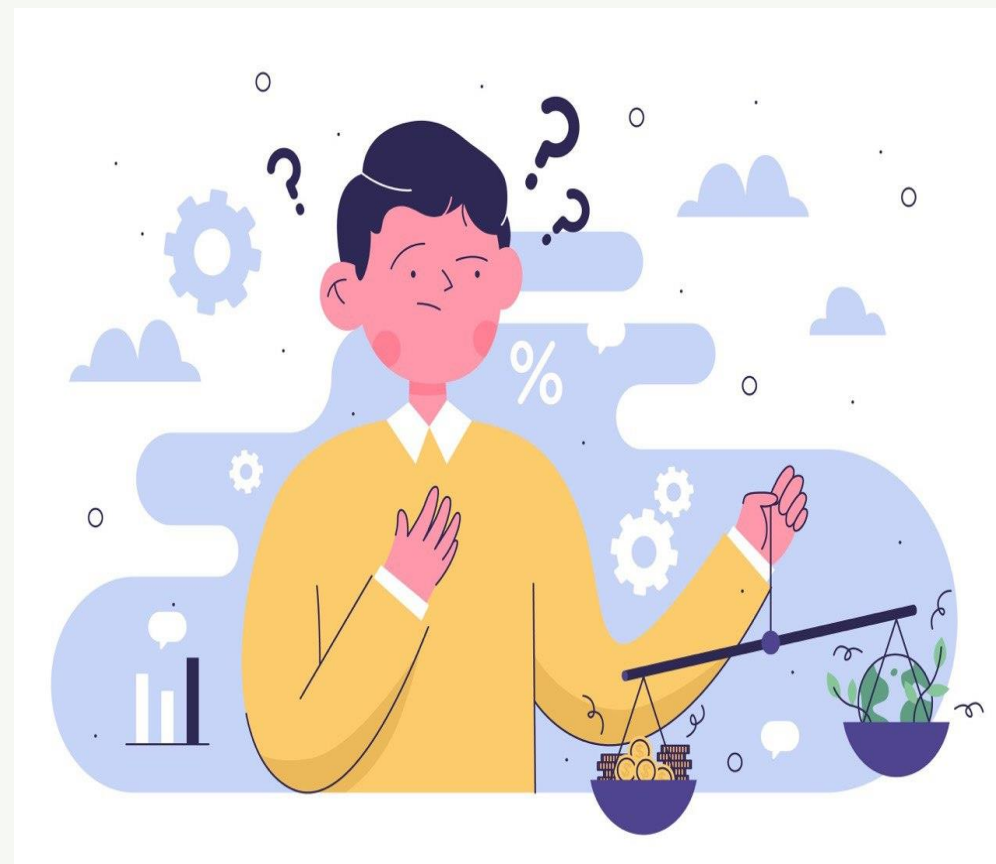
В условиях информационного общества особое значение приобретает соблюдение человеком норм информационной этики и информационного права.



ИНФОРМАЦИОННАЯ ЭТИКА

Этика — система моральных и нравственных норм, принятых в обществе; её важнейшими категориями являются «добро», «зло», «ответственность», «справедливость», «долг».

Информационная этика — область этики, которая рассматривает проблемы, возникающие в связи с развитием и использованием ИКТ, в том числе глобальной сети Интернет.



НОРМЫ ИНФОРМАЦИОННОЙ ЭТИКИ

1. Недопустимость несанкционированного открытия принадлежащих другим пользователям папок, файлов, почтовых ящиков, аккаунтов и просмотра их содержимого.
2. Недопустимость несанкционированного изменения настроек рабочего стола компьютера, не являющегося собственностью пользователя.
3. Недопустимость поиска, скачивания, создания и размещения в Сети контента, неэтичного по своему содержанию (например, содержащего жестокость, насилие, представляющего людей в неподобающем внешнем виде и т. д.).



НОРМЫ ИНФОРМАЦИОННОЙ ЭТИКИ

4. Недопустимость передачи содержания переписки по электронной почте, в мессенджерах и социальных сетях третьим лицам без предварительного согласия собеседника.
5. Недопустимость нарушения норм сетевого общения, использования в социальных сетях, мессенджерах и электронной почте: **компьютерных жаргонизмов, спама, оффтопика, кросспостинга, флуда, смайл-флуда, флейма, троллинга**



ИНФОРМАЦИОННОЕ ПРАВО

Информационное право — область права, регулирующая общественные отношения, связанные с созданием, хранением, обработкой, распространением, использованием информационных ресурсов.



НОРМЫ ИНФОРМАЦИОННОГО ПРАВА

На законодательном уровне запрещено:

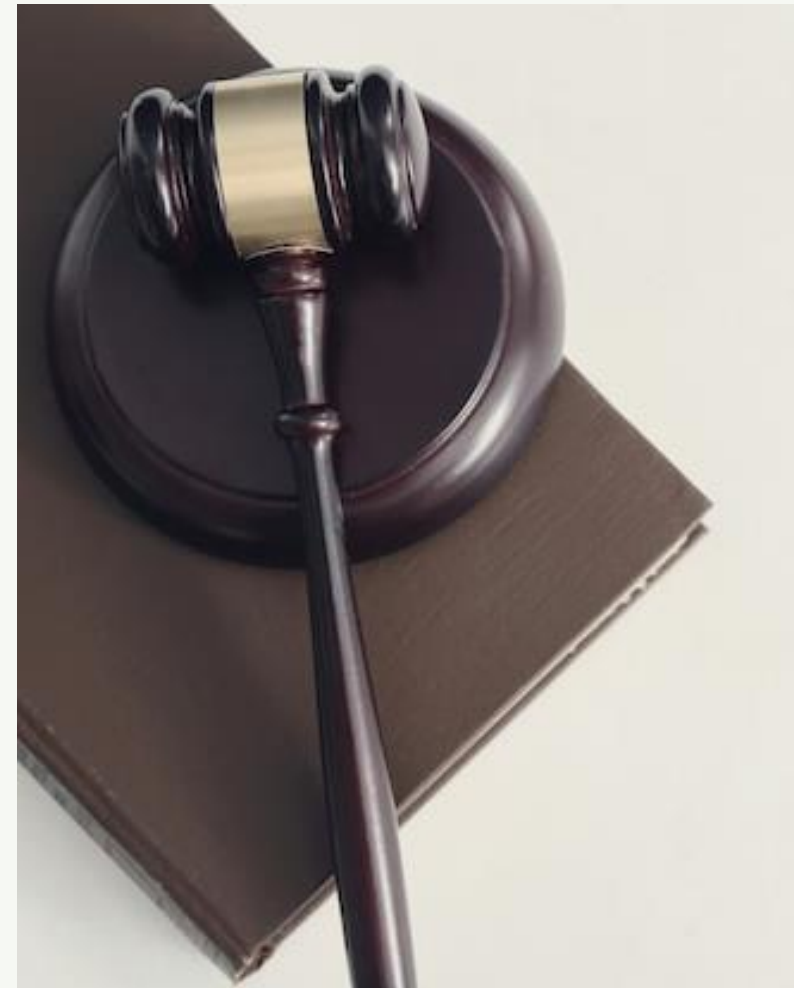
- распространять информацию, направленную на пропаганду войны, разжигание национальной, расовой или религиозной ненависти и вражды, а также иную информацию, за распространение которой предусмотрена уголовная или административная ответственность
- нарушать «неприкосновенность частной жизни, личную и семейную тайну», а также «право на тайну переписки, телефонных переговоров, почтовых, телеграфных и иных сообщений»
- передавать третьим лицам без предварительного согласия сетевых пользователей их личные данные — реальные имена, адреса, телефоны, фотографии



НОРМЫ ИНФОРМАЦИОННОГО ПРАВА

На законодательном уровне запрещено:

- нарушать авторские права и использовать нелицензионные материалы, в том числе программное обеспечение, являющиеся чужой интеллектуальной собственностью
- осуществлять несанкционированный доступ к чужому контенту, размещённому на ПК, носителях информации, сетевых сервисах, путём взлома аккаунтов других пользователей
- разрабатывать, распространять и использовать вредоносные программы и компьютерные вирусы



ИНФОРМАЦИОННАЯ БЕЗОПАСНОСТЬ

Информационная безопасность – защищённость информации и поддерживающей инфраструктуры информационной системы от случайных или преднамеренных воздействий естественного или искусственного характера, способных нанести ущерб субъектам информационных отношений (владельцам и пользователям информации) в рамках данной информационной системы.

ИНФОРМАЦИОННАЯ
БЕЗОПАСНОСТЬ



Обеспечение возможности работы с информацией

ДОСТУПНОСТЬ

Обеспечение защиты информации от удаления или искажения

ЦЕЛОСТНОСТЬ

Обеспечение защиты важной или личной информации

КОНФИДЕНЦИАЛЬНОСТЬ

ЗАЩИТА ИНФОРМАЦИИ

Защита информации — деятельность, направленная на предотвращение утечки защищаемой информации, несанкционированных и непреднамеренных воздействий на защищаемую информацию.

ВИДЫ ИНФОРМАЦИОННЫХ УГРОЗ

Несанкционированные (преднамеренные)

хищение информации

Вредоносные программы (вирусы)

Физическое воздействие на аппаратное обеспечение

Случайные (непреднамеренные)

Ошибки профессионалов

Ошибки пользователей

Отказы и сбои аппаратного обеспечения

Форс-мажорные обстоятельства



ЗАЩИТА ИНФОРМАЦИИ НА КОМПЬЮТЕРЕ

Каждый пользователь должен лично отвечать, обеспечивать и поддерживать защиту информационных ресурсов.

Защита информации подразумевает:

- использование антивирусной программы, регулярное обновление антивирусной базы и осуществление антивирусной проверки компьютера;
- периодическое резервное копирование файлов на внешние носители;
- использование блока бесперебойного питания;
- установку межсетевых экранов (Firewall);
- использование трудно определяемых паролей;
- физическую защиту информационных ресурсов



ПРАВИЛА ПОВЕДЕНИЯ В СЕТИ ИНТЕРНЕТ

Создавая свой профиль в социальных сетях, не указывайте свой адрес, дату рождения, школу, класс.

Придумывая себе логин (ник, имя пользователя), вместо имени используйте псевдоним; вы можете отразить в нём свои стремления, характер, интересы. При этом личную информацию, такую как ваша фамилия или дата рождения, включать в логин не рекомендуется.



ПРАВИЛА ПОВЕДЕНИЯ В СЕТИ ИНТЕРНЕТ

Пароли должны быть уникальными; цифры и спецсимволы значительно усложняют процесс их подбора злоумышленниками.

В социальные сети, мессенджеры и почту безопаснее входить через приложения; ввода паролей в браузерах следует избегать.

Не пользуйтесь сервисами, которые сохраняют пароли: онлайн-сервисы для хранения паролей ненадёжны; их часто взламывают.

Никому не сообщайте свои пароли.

При завершении работы с общедоступным компьютером корректно выходите из учётных записей, которые вы использовали.



ПРАВИЛА ПОВЕДЕНИЯ В СЕТИ ИНТЕРНЕТ



Будьте особенно бдительны при совершении интернет-покупок, согласовывайте все платежи с родителями.

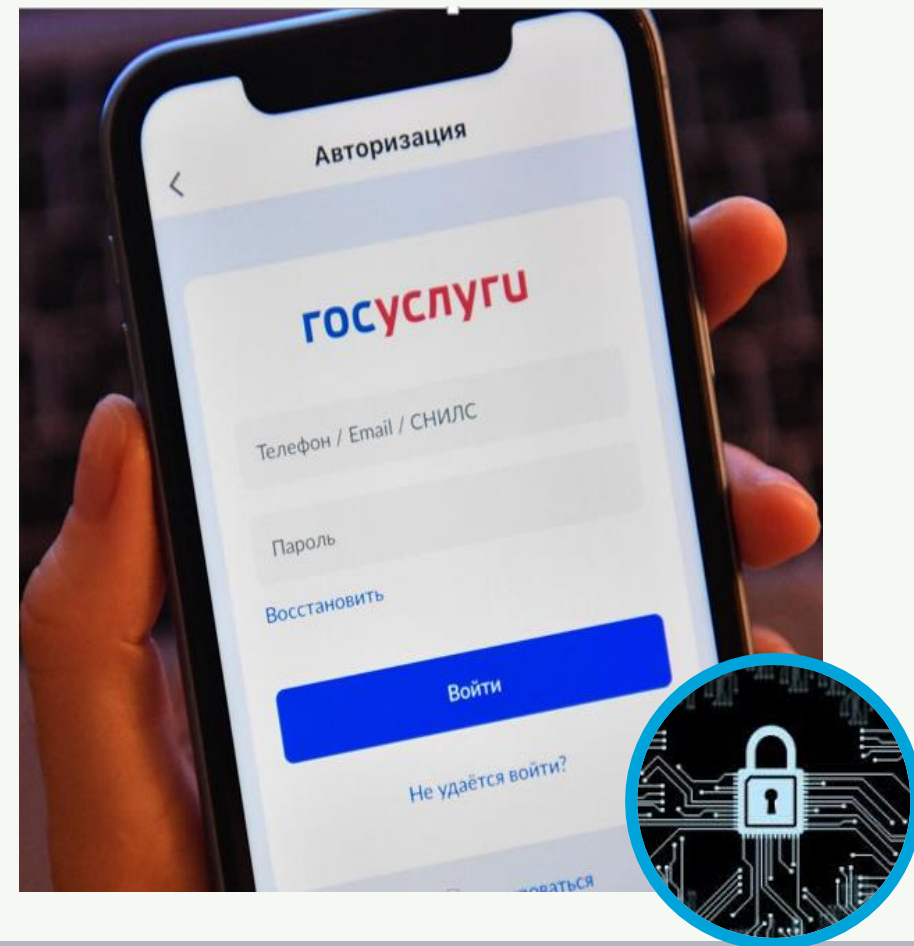
Обратите внимание на строку браузера на странице, на которой вводятся платёжные данные; проверьте, есть ли в строке браузера изображение закрытого навесного замочка — он означает безопасную передачу данных.

Когда замочек открыт, защита недостаточна. Если есть изображение восклицательного знака или перечёркнутого замка, на таком сайте не стоит вводить свои данные.



ПРАВИЛА ПОВЕДЕНИЯ В СЕТИ ИНТЕРНЕТ

Свои персональные данные (фамилию, домашний адрес, номер телефона, название школы, номера документов и т. д.) можно вводить только на государственных сайтах или на сайтах для покупки билетов. И только в том случае, если соединение устанавливается по протоколу HTTPS. Не оставляйте свои персональные данные на других сайтах.



ПРАВИЛА ПОВЕДЕНИЯ В СЕТИ ИНТЕРНЕТ

Старайтесь не выкладывать полную информацию (фотографии, видеозаписи) о себе и жизни своей семьи на всеобщее обозрение. Доступ к такой информации можно открывать только проверенным людям: родным, близким, друзьям и людям, с которыми вы знакомы в реальной жизни.

Помните: всё, что попало в Сеть, останется там навсегда. Как правило, стереть данные из Сети невозможно.

Единственный способ избежать утечки информации — не делиться ею без особой на то необходимости.

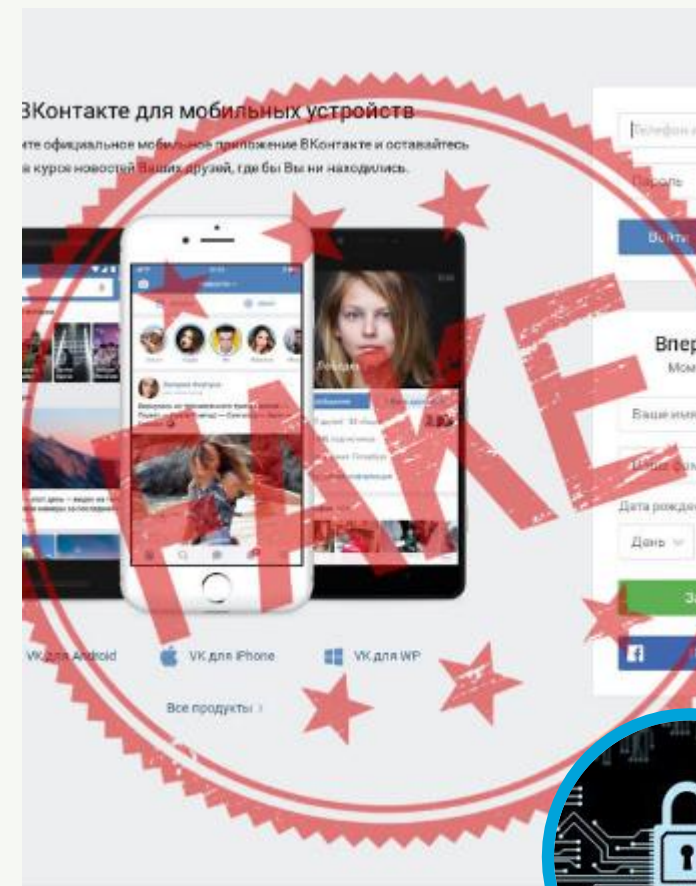


ПРАВИЛА ПОВЕДЕНИЯ В СЕТИ ИНТЕРНЕТ

Учитесь различать оригинальные и поддельные сайты.

Поддельные сайты могут иметь дизайн и адрес, напоминающие сайт-оригинал.

Злоумышленники ждут, когда человек введёт логин и пароль на поддельном сайте. Узнав эти данные, они используют их для входа в настоящий профиль своей жертвы.



ПРАВИЛА ПОВЕДЕНИЯ В СЕТИ ИНТЕРНЕТ



Будьте внимательны в онлайн-играх: игровые объекты, членство в командах, социальные связи внутри игры — всё это может стать механизмом манипуляции для мошенников и других злоумышленников.

В Интернете много сайтов, содержащих аркады, головоломки, другие игры с системой начисления очков; здесь деньги не тратятся.

Сайты с азартными играми, как правило, связаны с выигрышем или проигрышем денег.

Привычка к азартным играм приводит к формированию у человека психологической зависимости, представляющей серьёзную социальную и медицинскую проблему.



ПРАВИЛА ПОВЕДЕНИЯ В СЕТИ ИНТЕРНЕТ

Не всё, что вы видите в Сети, верно. Старайтесь мыслить критически, чтобы оценить достоверность материалов.

При поиске информации по интересующему вас вопросу обращайтесь внимание на источник информации, отдавая предпочтение официальным сайтам. Сверяйте найденную в Сети информацию по 2–3 источникам; проверяйте, есть ли в Сети другие мнения и факты, которые не противоречат ранее найденной информации



Не доверяйте безоговорочно сайтам с кричащими заголовками и обилием рекламы; следует насторожиться, если пользователя, щёлкнувшего на какой-либо новости, перекидывают куда-то дальше.

Не посещайте сайты расистского, дискриминационного, насильственного содержания — они способны поставить под угрозу ваше психологическое и физическое здоровье.



ПРАВИЛА ПОВЕДЕНИЯ В СЕТИ ИНТЕРНЕТ

Соблюдайте сетевой этикет.

Не старайтесь привлечь к себе внимание за счёт эпатажа.

Пишите грамотно.

Не оскорбляйте других, не будьте навязчивы, не позволяйте своим негативным эмоциям выходить из-под контроля.

Получив оскорбительное или иное сообщение, заставляющее вас чувствовать себя некомфортно, не отвечайте на него.

Никогда не участвуйте в травле: буллинг в Сети ничем не отличается от реального и одинаково опасен и для жертвы, и для агрессора.



ПРАВИЛА ПОВЕДЕНИЯ В СЕТИ ИНТЕРНЕТ

Онлайн-друг может быть совсем не тем человеком, за кого он себя выдаёт.

Злоумышленники, выдавая себя за вашего сверстника, могут пытаться выведать частную информацию о вас и членах вашей семьи. Затем, в зависимости от своих целей, они могут искать личной встречи, угрожать жертве.

Прежде чем вступить в диалог с незнакомцем, обратите внимание на его возраст и число друзей в Сети; следует насторожиться, если незнакомец старше вас, имеет очень мало друзей, просит вас выслать ему какие-нибудь фото или данные, — это явные приметы злоумышленника.



ПРАВИЛА ПОВЕДЕНИЯ В СЕТИ ИНТЕРНЕТ



Фишинг — вид интернет-мошенничества, целью которого является получение доступа к конфиденциальным данным пользователей.

Опасайтесь интернет-мошенничества: получив сообщение о выигрыше или возможности бесплатного получения какой-то вещи, не вводите пароли, номера телефонов, банковских карт или другую личную информацию.

Помните: подлинные интернет-сервисы не рассылают пользователям писем с просьбами сообщить свои учётные данные, пароль и прочее.



ПРАВИЛА ПОВЕДЕНИЯ В СЕТИ ИНТЕРНЕТ

Позаботьтесь о безопасности копий важных документов, которые вы решили хранить в облаке.

Отсканированные документы поместите в архив, при создании которого выберите опцию «непрерывный архив» (solid archive) и установите для этого архива пароль.

Не используйте один и тот же пароль для разных архивов.



ОТРАСЛЬ ИНФОРМАЦИОННЫХ ТЕХНОЛОГИЙ

ИТ-отрасль – стратегический сегмент экономики России. В национальной программе «Цифровая экономика Российской Федерации» определены научно-технические направления, имеющие ключевое значение для развития и процветания нашей страны.



КЛЮЧЕВЫЕ НАПРАВЛЕНИЯ

- ◆ большие данные
- ◆ нейротехнологии и искусственный интеллект
- ◆ промышленный Интернет
- ◆ компоненты робототехники и сенсорика
- ◆ технологии беспроводной связи
- ◆ технологии виртуальной и дополненной реальностей



ЧТО НУЖНО ДЛЯ УСПЕХА



Чтобы достигнуть успеха необходимо обладать:

- ◆ способностью ставить цели и достигать их
- ◆ способностью учиться, в том числе на своих ошибках
- ◆ способностью взаимодействовать с другими
- ◆ развитыми навыками чтения и письма, вычислительными навыками
- ◆ навыками тайм-менеджмента и др.

Способность к саморазвитию — главное условие успеха в современном стремительно изменяющемся мире!



Информационное общество — современный этап развития цивилизации, когда главную роль играют информация и информационно-коммуникационные технологии.

Информационная этика — это область этики, которая рассматривает проблемы, возникающие в связи с развитием и использованием ИКТ, в том числе глобальной сети Интернет.

Информационное право — область права, регулирующая общественные отношения, связанные с созданием, хранением, обработкой, распространением, использованием информационных ресурсов.

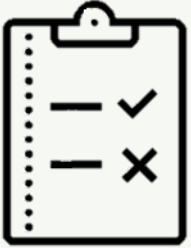
Информационная безопасность — это защищённость информации, которой обладает человек, исключение рисков её уничтожения, искажения и утечки, которые могут привести к невосполнимым потерям или ущербу для лица, обладающего этой информацией. Различают непреднамеренные и преднамеренные угрозы информационной безопасности.

Защита информации — деятельность, направленная на предотвращение утечки защищаемой информации, несанкционированных и непреднамеренных воздействий на защищаемую информацию.

Помните, защита вашей информации, ваша информационная безопасность — это прежде всего зона вашей ответственности.

Информатика и информационные технологии оказывают очень важное влияние на развитие экономики всего мира и каждой страны.

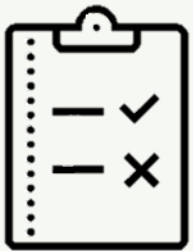
Способность к саморазвитию — главное условие успеха в современном стремительно изменяющемся мире!



ВОПРОСЫ И ЗАДАНИЯ

Какое общество называется информационным? Перечислите его основные черты.

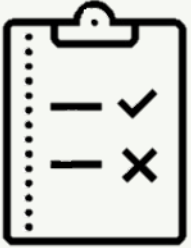




ВОПРОСЫ И ЗАДАНИЯ

Какую роль играют нормы этики и права в жизни общества?

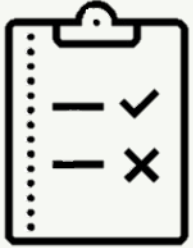




ВОПРОСЫ И ЗАДАНИЯ

С чем связано появление информационной этики и информационного права?

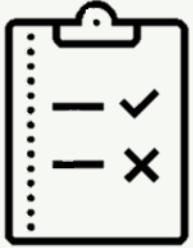




ВОПРОСЫ И ЗАДАНИЯ

Назовите основные нормы информационной этики.

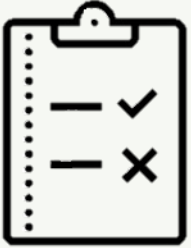




ВОПРОСЫ И ЗАДАНИЯ

Назовите основные нормы информационного права.

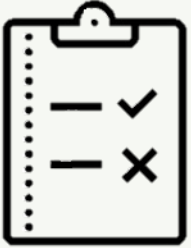




ВОПРОСЫ И ЗАДАНИЯ

Какие правовые нормы использования программного обеспечения вам известны?

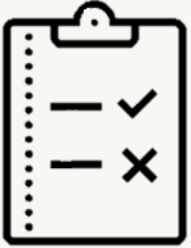




ВОПРОСЫ И ЗАДАНИЯ

Что такое информационная безопасность? Приведите примеры угроз информационной безопасности.

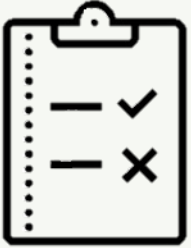




ВОПРОСЫ И ЗАДАНИЯ

Что такое защита информации? Кто несёт ответственность за защиту информации пользователя?

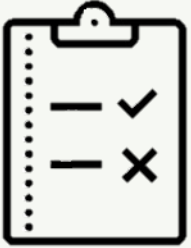




ВОПРОСЫ И ЗАДАНИЯ

Как пользователь может обеспечить защиту информации на своём компьютере?





ВОПРОСЫ И ЗАДАНИЯ

Какие возможности для защиты информации от случайной потери или удаления предусмотрены и в программном обеспечении компьютера?





ВОПРОСЫ И ЗАДАНИЯ

Какими приёмами фишинга пользуются интернет-мошенники?
Найдите соответствующие примеры в сети Интернет и
подготовьте презентацию на эту тему.

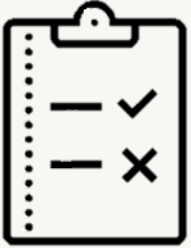




ВОПРОСЫ И ЗАДАНИЯ

Как вы считаете, можно ли похитить пароли, реквизиты банковских карт, списки контактов или другую конфиденциальную информацию со смартфонов? Что вам известно о вирусах и антивирусных программах для мобильных устройств?





ВОПРОСЫ И ЗАДАНИЯ

Какова основная идея правил (стратегий) безопасного поведения в сети Интернет?





ВОПРОСЫ И ЗАДАНИЯ

Распределите между учениками класса приведённые в учебнике правила безопасного поведения в сети Интернет. Совместными усилиями создайте презентацию «Безопасность в Интернете», разместив на её слайдах правила и соответствующие им визуальные образы — их вы можете подобрать в сети Интернет. Обязательно дайте ссылки на используемые источники информации.





ВОПРОСЫ И ЗАДАНИЯ

Одной из проблем информационного общества является социальная инженерия. Выясните, что это такое. Сталкивались ли вы, ваши родственники или знакомые с этим явлением?



ИНФОРМАЦИОННАЯ БЕЗОПАСНОСТЬ

ИНФОРМАЦИОННАЯ ЭТИКА

ИНФОРМАЦИОННОЕ ПРАВО

ИНФОРМАЦИОННОЕ ОБЩЕСТВО

ИНФОРМАЦИОННЫЕ ТЕХНОЛОГИИ:

- ◆ большие данные
- ◆ нейротехнологии и искусственный интеллект
- ◆ промышленный Интернет
- ◆ компоненты робототехники и сенсорика
- ◆ технологии беспроводной связи
- ◆ технологии виртуальной и дополненной реальностей

СОВРЕМЕННАЯ ЛИЧНОСТЬ:

- ◆ способностью ставить цели и достигать их
- ◆ способностью учиться, в том числе на своих ошибках
- ◆ способностью взаимодействовать с другими
- ◆ развитыми навыками чтения и письма, вычислительными навыками
- ◆ навыками тайм-менеджмента и др.