Сетевой этикет и меры безопасности в сети Интернет

Сегодня на уроке мы…

- изучим правила сетевого этикета, меры безопасности в сети Интернет;
- ознакомимся с ответственностью за совершение противоправных действий в сети Интернет;
- научимся использовать правила сетевого этикета при работе в сети Интернет, рекомендации для безопасной работы в сети Интернет.

Вспомним

Какие технологии называются облачными?

Облачные технологии — технологии обработки данных, в которых компьютерные ресурсы и мощности предоставляются пользователю как **Интернет-сервис.**

Вспомним

Какой облачный сервис является базовым?

Для того чтобы ваши данные были доступны вам (или вашим друзьям) на любом компьютере (где бы он ни находился), в том числе и на мобильном устройстве, используются **облачные хранилища данных**.

Этот сервис является базовым для других облачных сервисов, поскольку входит в состав почти каждого из них.

Вспомним

В чем суть совместной работы над документами? Какие сервисы предоставляют такие возможности?

Согласование изменений в документах может быть организовано более оперативно — через облачные сервисы, предназначенные для совместной работы над документами, например **Google Docs**.

Доступ к сервисам Google Docs можно получить прямо из окна браузера.

Вспомним

В каком случае пользователь получает доступ к облачным сервисам?

Чтобы пользоваться облачными сервисами, необходимо создать **аккаунт** — учетную запись, в которой хранится персональная информация.

Аккаунт может быть привязан к адресу электронной почты.

Основные правила сетевого этикета

Интернет — мир интересных и полезных возможностей, но в то же время это источник угроз, особенно для детей и молодежи. Агрессия, мошенничество, психологическое давление — опасности, которые могут поджидать в глобальной сети каждый день.

Работая с различными облачными сервисами или общаясь по сети, нужно соблюдать такие же правила, как и при работе с электронной почтой. Обезличенность при общении в Интернете заставляет пользователей забывать, что они имеют дело не с машиной, а с реальными людьми. Правила сетевого этикета помогают достичь взаимопонимания и обеспечивают безопасность общения.

Основные правила сетевого этикета

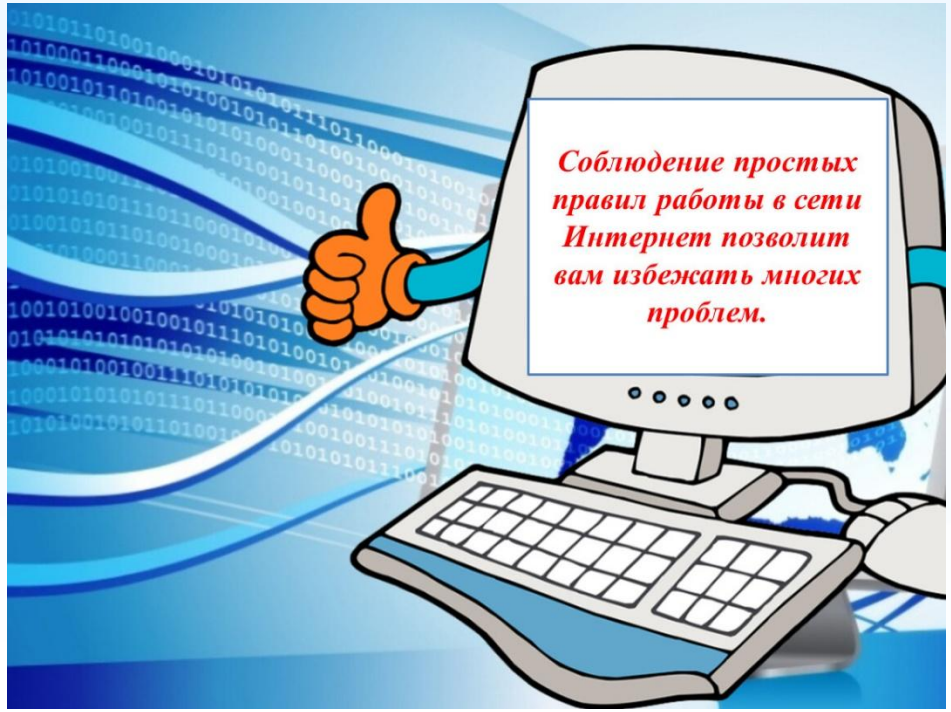
1. Будьте вежливы и не забывайте об обязательных формулах приветствия, обращения, благодарности.

Основные правила сетевого этикета

2. Избегайте бессодержательных бесед, чтобы не тратить свое время и время собеседника.

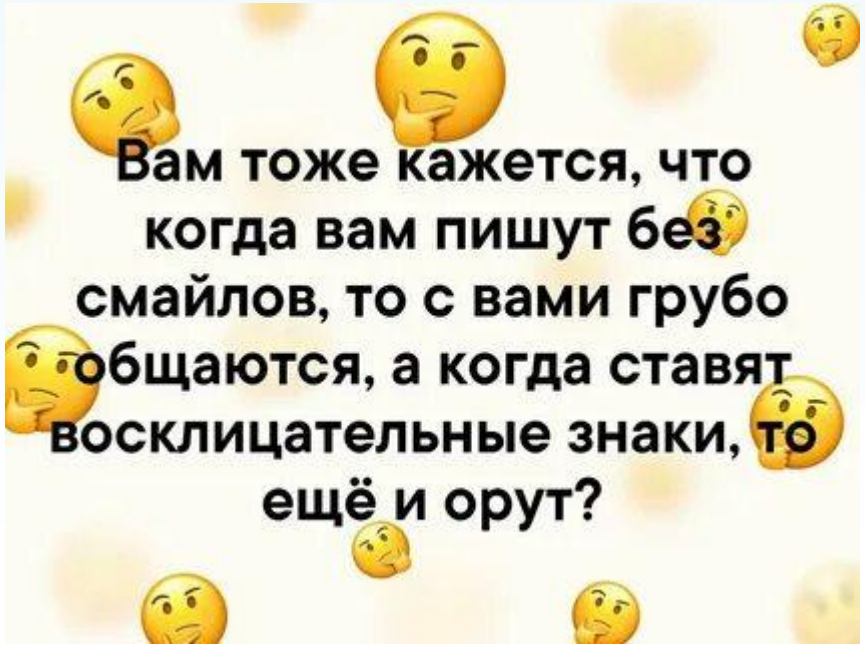
Основные правила сетевого этикета

3. Пишите грамотно. Используйте проверку орфографии. Перед отправкой сообщения перечитайте текст.



Основные правила сетевого этикета

4. Без необходимости не пишите на транслите (т. е. не злоупотребляйте использованием букв алфавита другого языка). Не набирайте текст заглавными буквами. Не перегружайте сообщение смайликами.



Основные правила сетевого этикета

5. Сохраняйте анонимность при общении с незнакомцами.

Рекомендации, которые помогут снизить вероятность совершения противоправных действий в Интернете

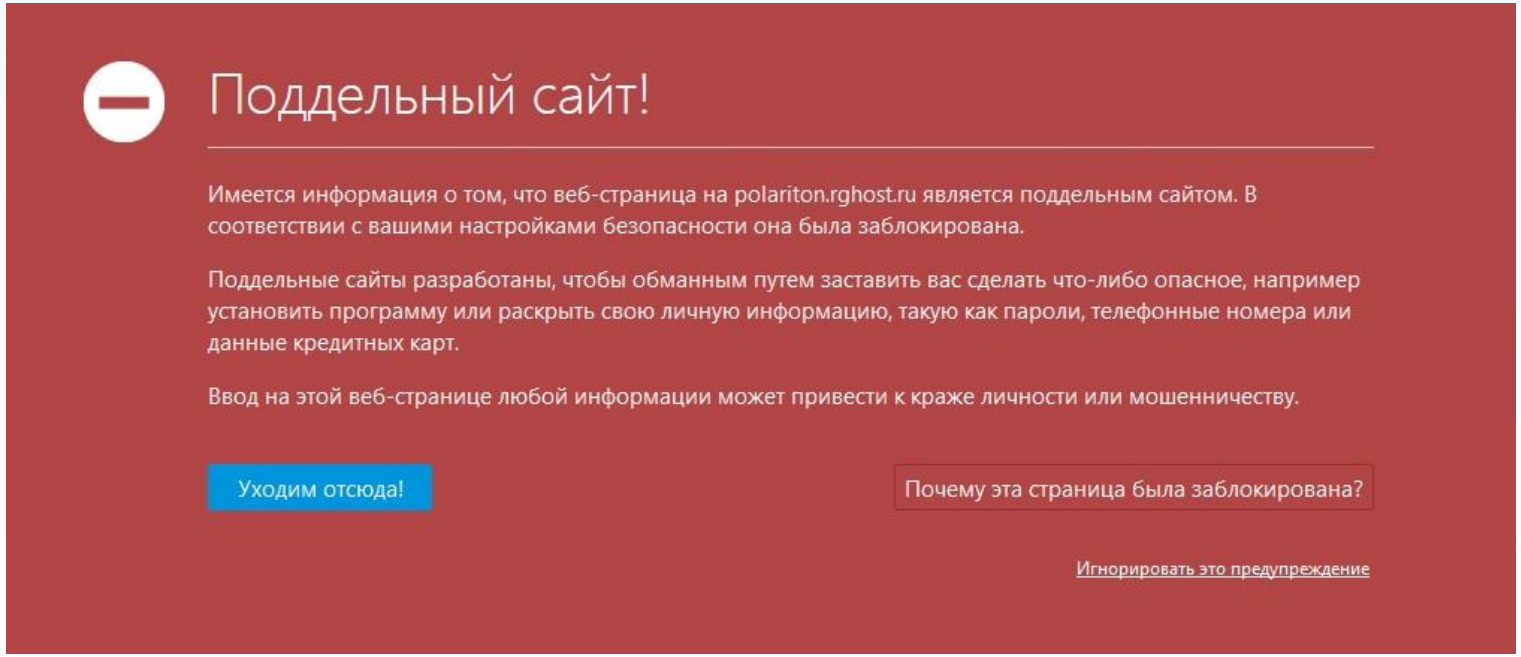
Неосмотрительность и халатный подход к обеспечению безопасности в Интернете могут дать возможность преступникам совершить противоправные действия. Сначала преступник получает несанкционированный доступ к учетным записям в социальных сетях, к электронному почтовому ящику, к аккаунтам и др. Получив реквизиты, злоумышленник заходит в учетную запись и осуществляет рассылку контактам владельца взломанной учетной записи сообщения мошеннического характера.

Рекомендации, которые помогут снизить вероятность совершения противоправных действий в Интернете:

1. Для выхода в сеть Интернет используйте устройства, на которых установлены и постоянно обновляются антивирусные программы.

Рекомендации, которые помогут снизить вероятность совершения противоправных действий в Интернете:

2. При посещении известных сайтов обращайте внимание на их внешний вид: возможно, это поддельная копия.

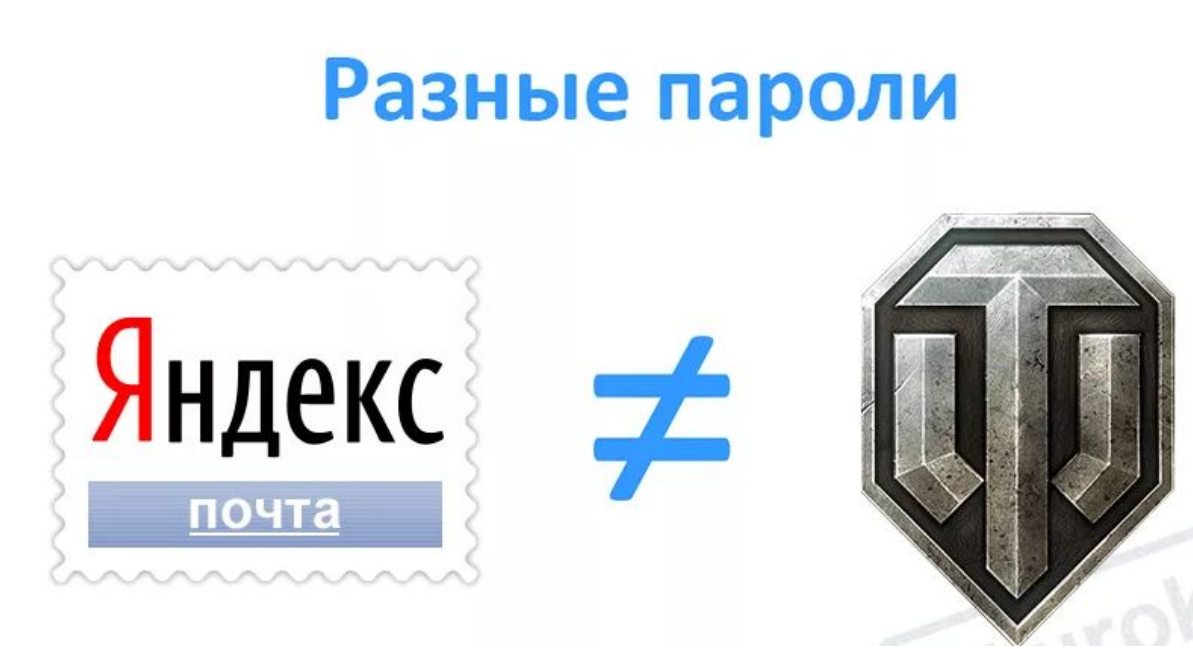


Рекомендации, которые помогут снизить вероятность совершения противоправных действий в Интернете:

3. Вводите личную информацию только на веб-сайтах, которые работают с использованием защищенных протоколов (в браузере рядом с адресом такого сайта отображается значок замка).

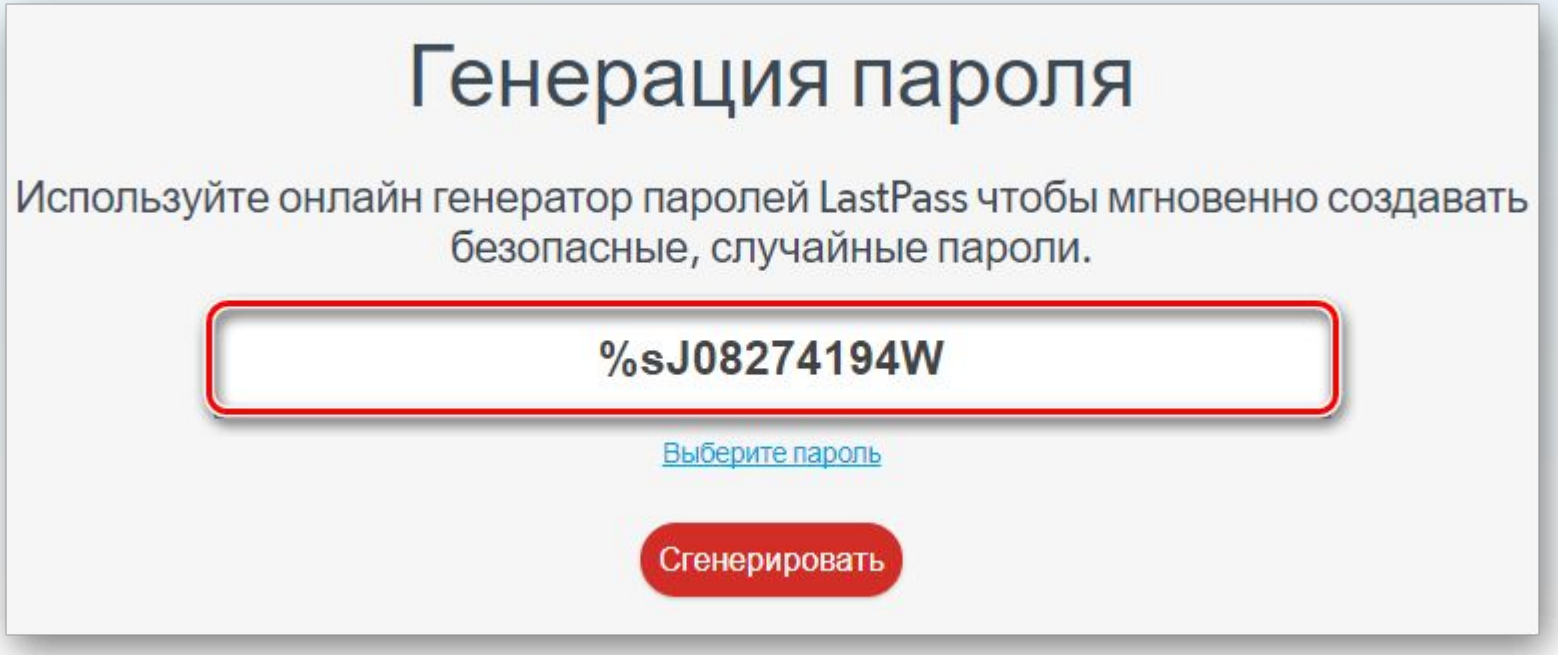
Рекомендации, которые помогут снизить вероятность совершения противоправных действий в Интернете:

4. Не используйте одинаковые логины и пароли на различных сайтах.



Рекомендации, которые помогут снизить вероятность совершения противоправных действий в Интернете:

5. Не используйте легкие пароли (даты рождения, номера телефонов и т. д.).



Рекомендации, которые помогут снизить вероятность совершения противоправных действий в Интернете:

6. Остерегайтесь неожиданных или необычных электронных сообщений, даже если вам знаком отправитель; не открывайте вложения и не переходите по ссылкам в таких сообщениях.

Рекомендации, которые помогут снизить вероятность совершения противоправных действий в Интернете:

7. При поступлении сообщений от знакомых, содержащих просьбы о финансовых операциях или о передаче финансовых реквизитов, обязательно проверяйте данную информацию по другим каналам связи (личная встреча, телефонный звонок, голосовая связь). Постарайтесь установить личность собеседника с помощью контрольных вопросов, ответы на которые могут быть известны только вам двоим.

Примеры мошенничества в Интернете

Примеры мошенничества в Интернете:

1. Производится вирусная атака на компьютерные устройства, блокируется браузер или операционная система, а на экране монитора появляется требование оплатить крупный штраф.

2. На электронный почтовый ящик приходит письмо, которое обещает: после покупки обучающего курса можно уже завтра начинать зарабатывать огромные деньги. Помните, что никто не будет рассказывать совершенно незнакомым людям, как заработать огромные деньги, мошенники просто зарабатывают деньги на продаже этих обучающих курсов.

Ответственность за преступления в сети Интернет

Законодательством Республики Беларусь определена мера ответственности за следующие преступления в сети Интернет:

1. Несанкционированный доступ к данным.

Законодательством Республики Беларусь определена мера ответственности за следующие преступления в сети Интернет:

2. Модификация (изменение) данных без разрешения владельца.

Законодательством Республики Беларусь определена мера ответственности за следующие преступления в сети Интернет:

3. Умышленное уничтожение данных, приведение их в непригодное состояние.

Законодательством Республики Беларусь определена мера ответственности за следующие преступления в сети Интернет:

4. Разработка, использование и распространение вредоносных программ.

Законодательством Республики Беларусь определена мера ответственности за следующие преступления в сети Интернет:

5. Нарушение авторского права.

Статьи Уголовного кодекса Республики Беларусь, определяющие ответственность за преступления в сети Интернет (http://kodeksy.by).

Статья 212. Хищение путем использования компьютерной техники.

Статья 349. Несанкционированный доступ к компьютерной информации.

Статья 350. Модификация компьютерной информации.

Статья 351. Компьютерный саботаж.

Статья 352. Неправомерное завладение компьютерной информацией.

Статья 353. Изготовление либо сбыт специальных средств для получения неправомерного доступа к компьютерной системе или сети.

Статья 354. Разработка, использование либо распространение вредоносных программ.

Статья 355. Нарушение правил эксплуатации компьютерной системы или сети.

Специальные слова (сленг) в Интернете

1. Для обозначения нарушений правил сетевого этикета:

Флейм (англ. flame — пламя) — неожиданно возникшее активное обсуждение, при развитии которого участники обычно забывают о первоначальной теме, переходят на личности и не могут остановиться.

1. Для обозначения нарушений правил сетевого этикета:

Флуд (англ. flood — наводнение) — сообщения, не несущие никакой полезной информации. Флуд может распространяться с целью троллинга, т. е. из желания кому-либо досадить. Технический флуд представляет собой хакерскую атаку с большим количеством запросов, приводящую к отказу работы сервиса (DDoS-атака).

1. Для обозначения нарушений правил сетевого этикета:

Спам (англ. spam) — сообщения, присылаемые от неизвестных людей или организаций без разрешения. Часто термин спам употребляется в значении почтовый спам — рассылка электронных писем, содержащих рекламу.

1. Для обозначения нарушений правил сетевого этикета:

Оффтоп (англ. off topic — вне темы) — сетевое сообщение, не имеющее отношения к заранее установленной теме общения. Наиболее неодобряемой формой оффтопа являются рекламные сообщения.

1. Для обозначения нарушений правил сетевого этикета:

Хотлинк (англ. hotlink) — включение в веб-страницу файлов-изображений или других ресурсов с чужого сервера. Этот прием используется недобросовестными веб-мастерами. При этом расходуются чужие ресурсы и трафик.

1. Для обозначения нарушений правил сетевого этикета:

Оверквотинг (англ. overquoting) — избыточное цитирование.

2. Для обозначения противоправных действий в Интернете:

Фишинг (англ. phishing — password + fishing выуживание паролей) — вид мошенничества с целью получения доступа к логинам и паролям пользователей.

2. Для обозначения противоправных действий в Интернете:

Киберсквоттинг (англ. cybersquatting) — регистрация доменных имен, содержащих торговую марку, принадлежащую другому лицу, с целью их дальнейшей перепродажи или недобросовестного использования.

2. Для обозначения противоправных действий в Интернете:

Брутфорс (от англ. brute force — полный перебор) — метод атаки или взлома путем перебора всех возможных вариантов пароля.

2. Для обозначения противоправных действий в Интернете:

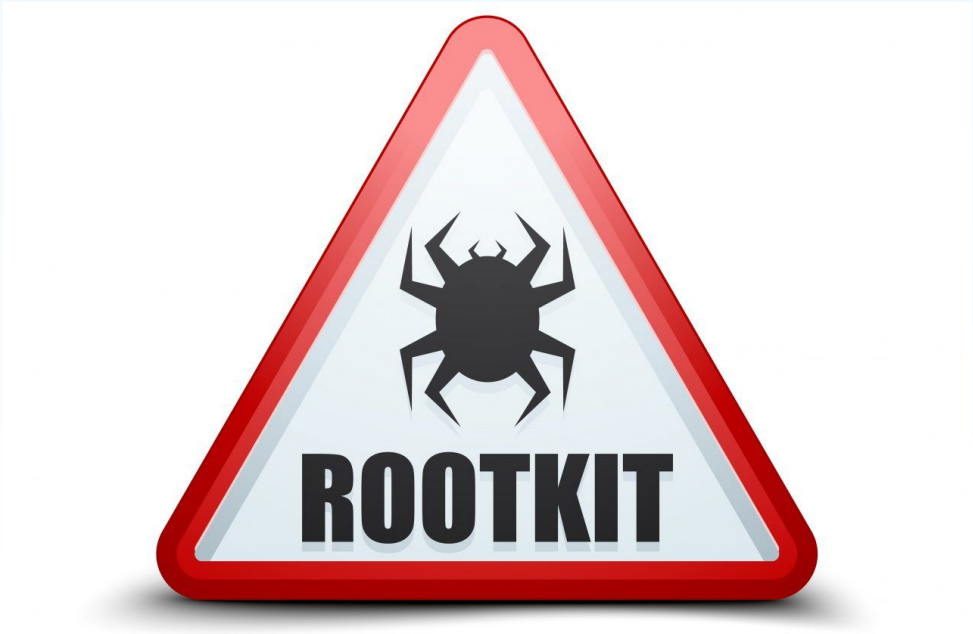
Кардинг (от англ. carding) — вид мошенничества с использованием чужой платежной карты или ее реквизитов.

2. Для обозначения противоправных действий в Интернете:

Кликджекинг (англ. clickjacking) — механизм обмана пользователей Интернета, позволяющий узнать контакты посетителей сайта еще до того, как они сами разместили их на сайте.

2. Для обозначения противоправных действий в Интернете:

Руткит (англ. rootkit) — программа или набор программ для скрытия следов присутствия злоумышленника или вредоносной программы в системе.



2. Для обозначения противоправных действий в Интернете:

Фарминг (англ. pharming) — скрытое перенаправление на ложный IP-адрес.

Повторим

Почему нужно соблюдать правила этикета при общении в сети Интернет?

Правила сетевого этикета помогают достичь взаимопонимания и обеспечивают безопасность общения.

Повторим

Какие правила сетевого этикета не соблюдаются в приведенных ниже сообщениях?

Сегодня четверг. Это хуже, чем суббота, но гораздо лучше, чем понедельник... Но немного хуже, чем пятница. Зато четверг лучше, чем среда. Четверг даже лучше, чем воскресенье, потому что в воскресенье завтра понедельник, а в четверг завтра пятница...

Бессодержательные беседы

Повторим

Какие правила сетевого этикета не соблюдаются в приведенных ниже сообщениях?

Смайлы  — это очень удобно  . Но в то же время у них есть обратная сторона  . Они берегут эту тайну  . И никто не должен знать о ней  . НИКТО! 

Перегрузка сообщения смайликами

Повторим

Какие правила сетевого этикета не соблюдаются в приведенных ниже сообщениях?

нАриСуй Мне:
1) УвАжАеШь — рОзоВыЙ фОн;
2) ОбИдЕлся — КоричНевЫй фОн;
3) дружИшЬ — бЕлЫй фОн.
рАзошлИ Это Всем СвОим дРуЗьяМ, И тВоя СтЕнА бУдЕт СупеРКрАсИвая.

Набор текста заглавными буквами

Повторим

Какие меры необходимо предпринять, чтобы обезопасить свои учетные записи от действий мошенников?

Не используйте одинаковые логины и пароли на различных сайтах.

Не используйте легкие пароли (даты рождения, номера телефонов и т. д.).

Повторим

Каким должен быть безопасный пароль?

Хороший пароль – всегда комбинированный. В нем используются символы, буквы и цифры разного регистра. Длина пароля – желательно не менее 8 символов, а лучше не менее 12. Избегайте смысловых паролей: не используйте распространенные фразы или слова.

Повторим

Какие действия в сети Интернет определены законодательством Республики Беларусь как противоправные?

1. Несанкционированный доступ к данным.
2. Модификация (изменение) данных без разрешения владельца.
3. Умышленное уничтожение данных, приведение их в непригодное состояние.
4. Разработка, использование и распространение вредоносных программ.
5. Нарушение авторского права.

Домашнее задание

§ 5